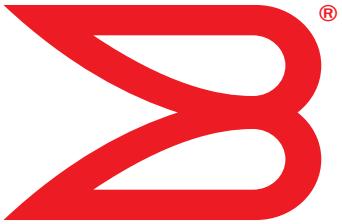
53-1003056-01
14 February 2014



Brocade Network Advisor

IP User Manual

Supporting Network Advisor 12.2.0

BROCADE

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
Brocade Network Advisor IP User Manual	53-1002045-01	New document	November 2010
Brocade Network Advisor IP User Manual	53-1002168-01	Updated for Network Advisor 11.1.	May 2011
Brocade Network Advisor IP User Manual	53-1002356-01	Updated for Network Advisor 11.2.	September 2011
Brocade Network Advisor IP User Manual	53-1002531-01	Updated for Network Advisor 11.2.1.	March 2012

Title	Publication number	Summary of changes	Date
Brocade Network Advisor IP User Manual	53-1002569-01	Updated for Network Advisor 11.3.0.	August 2012
Brocade Network Advisor IP User Manual	53-1002695-01	Updated for Network Advisor 12.0.0.	December 2012
Brocade Network Advisor IP User Manual	53-1002947-01	Updated for Network Advisor 12.1.0.	August 2012
Brocade Network Advisor IP User Manual	53-1003056-01	Updated for Network Advisor 12.2.0.	February 2014

Contents

Chapter 12 Server Management Console

Chapter 13 Wireless Management

Chapter 28 MPLS Management

Chapter 40 Reports

About This Document

In this chapter

How this document is organized

This document is organized to help you find the information that you want as quickly and easily as possible. This document supports Network Advisor 12.2.0 and later.

The document contains the following components:

- Chapter 1, "Getting Started," provides a high-level overview of the user interface.
- Chapter 2, "Patches," provides information about installing patches.
- Chapter 3, "Discovery," describes how to discover IP devices.
- Chapter 4, "Management Groups," describes how to create product and port management groups.
- Chapter 5, "Application Configuration," provides Management application configuration instructions.
- Chapter 6, "User Account Management," provides information on how to manage users.
- Chapter 7, "Dashboard Management,"provides details about the Dashboard tab.
- Chapter 8, "View Management," provides view and topology configuration instructions.
- Chapter 9, "MRP Topology," provides details about MRP topology.
- Chapter 10, "Call Home," provides call home configuration instructions.
- Chapter 11, "Third-party tools," provides instructions for adding and launching third-party tools.
- Chapter 12, "Server Management Console," provides information on using the Server Management Console to stop and start the Management application services, back up the Management application database, and capture technical support information.
- Chapter 13, "Wireless Management," provides information about wireless devices.
- Chapter 14, "VCS Management," provides information on VCS fabrics. This chapter is for Network OS devices only.

- Chapter 15, “Host Management,” provides information on how to configure an HBA. This chapter is for Fabric OS devices only.
- Chapter 16, “Fibre Channel over Ethernet,” provides information on how to configure FCoE. This chapter is for Fabric OS devices only.
- Chapter 17, “Telemetry,” provides instructions for you to monitor, report, and analyze traffic information and data on your network.
- Chapter 18, “Security Management,” provides security configuration instructions.
- Chapter 19, “Zoning,” provides zoning configuration instructions.
- Chapter 20, “Port Fencing,” provides information on how to configure port fencing. This chapter is for Fabric OS devices only.
- Chapter 21, “FICON Environments,” provides information on how to manage FICON. This chapter is for Fabric OS devices only.
- Chapter 22, “IP Element Manager,” provides instructions for accessing a device by connecting to its command line interface (CLI) or Web Management interface.
- Chapter 23, “Configuration Repository and Backup,” provides information on saving and backing up configurations.
- Chapter 24, “IP Configuration Wizard,” provides information on creating and deploying configuration payloads.
- Chapter 25, “CLI Configuration Management,” provides information on creating configurations and reports using command line interface commands.
- Chapter 26, “Image Repository for IP Products,” provides information for importing and deploying boot, monitor, software, and unified images.
- Chapter 27, “VLAN Management,” provides information on how to manage Virtual Local Area Networks (VLANs).
- Chapter 28, “MPLS Management,” provides information on how to configure Multi-protocol Label Switching (MPLS).
- Chapter 29, “VIP Servers,” provides information on how to manage virtual IP servers.
- Chapter 30, “Global Server Load Balancing,” provides information on how to configure Global Server Load Balancing policies.
- Chapter 31, “SSL Certificates for ServerIron Products,” provides information on how to import and deploy SSL certificates and keys.
- Chapter 32, “Deployment Manager,” provides information about how to view, deploy, and manage deployment configurations.
- Chapter 33, “Performance Data,” provides information on how to manage performance.
- Chapter 34, “Frame Monitor,” provides information on how to monitor frames. This chapter is for Fabric OS devices only.
- Chapter 35, “Power Center,” provides information on how to monitor power on Power over Ethernet (PoE) products.
- Chapter 36, “Policy Monitor,” provides information on how to configure best practice guidelines.
- Chapter 37, “Fault Management,” provides event management instructions.
- Chapter 38, “Packet Capture (Pcap),” provides information on how to configure switches as sensors to capture packets.
- Chapter 39, “Technical Support,” provides server, client, and device supportSave instructions.

- Chapter 40, “Reports,” provides instructions for generating reports.
- Appendix A, “Application menus,” provides information about the main and shortcut menus.
- Appendix B, “Call Home Event Tables,” provides supplemental information about call home event tables.
- Appendix C, “Event Categories,” provides information about events.
- Appendix D, “User Privileges,” provides supplemental information about user privileges and access levels.
- Appendix E, “Device Properties,” provides reference information related to fabric, product, and port properties.
- Appendix F, “Regular Expressions,” provides a summary of Unicode regular expression constructs that you can use in the Management application.
- Appendix G, “CLI Templates,” provides information about preconfigured CLI templates.
- Appendix H, “Troubleshooting,” provides general troubleshooting details.
- Appendix I, “Database Fields,” provides reference information related to databases.

Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some devices but not to others, this guide identifies exactly which devices are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for Network Advisor 12.2.0, documenting all possible configurations and scenarios is beyond the scope of this document.

Fabric OS hardware and software support

The following firmware platforms are supported by this release of Network Advisor 12.2.0:

- Fabric OS 5.0 or later in a pure Fabric OS fabric
- Fabric OS 6.0 or later in a mixed fabric

NOTE
Discovery of a Secure Fabric OS fabric in strict mode is not supported.

The hardware platforms in the following table are supported by this release of Network Advisor 12.2.0.

TABLE 1 Fabric OS-supported hardware

Device name	Terminology used in documentation	Firmware level required
Brocade 6505 switch	24-port, 16 Gbps Edge switch	Fabric OS v7.0.1 or later
Brocade M6505 embedded switch	24-port, 16 Gbps embedded switch	Fabric OS v7.2.0 or later
Brocade 6510 switch	48-port, 16 Gbps switch	Fabric OS v7.0.0 or later
Brocade 6520 switch	96-port, 16 Gbps switch	Fabric OS v7.1.0 or later
Brocade 6547 embedded switch	48-port, 16 Gbps embedded switch	Fabric OS v7.2.0 or later

TABLE 1 Fabric OS-supported hardware (Continued)

Device name	Terminology used in documentation	Firmware level required
Brocade 415 Host Bus Adapter	4 Gbps 1-port HBA	
Brocade 425 Host Bus Adapter	4 Gbps 2-port HBA	
Brocade 815 Host Bus Adapter	8 Gbps 1-port HBA	
Brocade 825 Host Bus Adapter	8 Gbps 2-port HBA	
Brocade 1860 Fabric Adapter	16 Gbps FC HBA mode 10 Gbps CNA mode 10 Gbps NIC mode	Adapter Software 3.0.0.0 or later
Brocade 1867 HBA	16 Gbps Mezzanine HBA	Adapter Software 3.0.3.0 or later
Brocade DCX 8510-4	16 Gbps 4-slot Backbone Chassis	Fabric OS v7.0.0 or later
Brocade DCX 8510-8[1, 2]	16 Gbps 8-slot Backbone Chassis	Fabric OS v7.0.0 or later
FC16-32 Blade	16 Gbps 32-port blade	Fabric OS v7.0.0 or later
FC16-48 Blade	16 Gbps 48-port blade	Fabric OS v7.0.0 or later

IronWare hardware and software support

The following firmware platforms are supported by this release of Network Advisor 12.2.0:

- BigIron 2.7.02e (sustaining mode) or later
- FastIron 7.2.0 or later
- NetIron 5.1.0 or later
- ServerIron (JetCore) 11.0 or later
- ServerIron ADX 12.2.0 or later
- TurboIron 4.2.0 or later

For platform-specific firmware requirements, refer to Table 2.

Table 2 lists the hardware platforms supported by this release of Network Advisor 12.2.0, the terminology used in the documentation, as well as any specific firmware requirements.

TABLE 2 IronWare-supported hardware

Device name	Terminology used in documentation	Firmware level required
BigIron family	Ethernet Chassis	BigIron 2.7.02e or 2.7.01b
BigIron RX-4 (BI-RX-4-AC)	Ethernet Chassis, 4 interface slots	BigIron 2.7.02e or 2.7.01b
BigIron RX-8 (BI-RX-8-AC)	Ethernet Chassis, 8 interface slots	BigIron 2.7.02e or 2.7.01b
BigIron RX-16 (BI-RX-16-AC-A)	Ethernet Chassis, 16 interface slots	BigIron 2.7.02e or 2.7.01b
Brocade 6910 Ethernet Access Switch	Ethernet Access Switch	release 2.0.2.7, loader version 1.0.1.3
FastIron family	Ethernet switch	See individual device.
FastIron CX 624S (FCX624S)	Ethernet L2/L3 Edge switch, 24 1GbE RJ45 ports	FastIron 06.0.00 and later
FastIron CX 648S (FCX648S)	Ethernet L2/L3 Edge switch, 48 1GbE RJ45 ports	FastIron 06.0.00 and later

TABLE 2 IronWare-supported hardware (Continued)

Device name	Terminology used in documentation	Firmware level required
FastIron CX 624S-HPOE (FCX624S-HPOE)	Ethernet L2/L3 Edge switch, 24 1GbE RJ45 ports, 24 POE+ ports	FastIron 06.0.00 and later
FastIron CX 648S-HPOE (FCX648S-HPOE)	Ethernet L2/L3 Edge switch, 48 1GbE RJ45 ports, 48 POE+ ports	FastIron 06.0.00 and later
FastIron CX 624S-F (FCX624S-F)	Ethernet L2/L3 Edge switch, 20 SFP ports	FastIron 06.0.00 and later
FastIron CX 624-E (FCX624-E)	Ethernet L2/L3 Edge switch, 24 1GbE RJ45 ports	FastIron 06.0.00 and later
FastIron CX 624-I (FCX624-I)	Ethernet L2/L3 Edge switch, 24 1GbE RJ45 ports	FastIron 06.0.00 and later
FastIron CX 648-E (FCX648-E)	Ethernet L2/L3 Edge switch, 48 1GbE RJ45 ports	FastIron 06.0.00 and later
FastIron CX 648-I (FCX648-I)	Ethernet L2/L3 Edge switch, 48 1GbE RJ45 ports	FastIron 06.0.00 and later
ICX 6610 Stackable switch family	Campus LAN Edge stackable switch	FastIron 07.0.3 and later Hyper Edge stacking requires FastIron 8.0 or later
ICX 6610-24 Stackable switch	24 RJ-45 ports Campus LAN Edge stackable switch	FastIron 07.0.3 and later Hyper Edge stacking requires FastIron 8.0 or later
ICX 6610-48 Stackable switch	48 RJ-45 ports Campus LAN Edge stackable switch	FastIron 07.0.3 and later Hyper Edge stacking requires FastIron 8.0 or later
ICX 6610-24F Stackable switch	24 SFP ports Campus LAN Edge stackable switch	FastIron 07.0.3 and later Hyper Edge stacking requires FastIron 8.0 or later
ICX 6610-24P Stackable switch	24 PoE ports Campus LAN Edge stackable switch	FastIron 07.0.3 and later Hyper Edge stacking requires FastIron 8.0 or later
ICX 6610-48P Stackable switch	48 PoE ports Campus LAN Edge stackable switch	FastIron 07.0.3 and later Hyper Edge stacking requires FastIron 8.0 or later
ICX 6430-24 switch	24-port Campus LAN switch	FastIron 07.4.00 and later
ICX 6430-24-HPOE switch	24-port Campus LAN HPOE switch	FastIron 07.4.00 and later
ICX 6430-48 switch	48-port Campus LAN switch	FastIron 07.4.00 and later
ICX 6430-48-HPOE switch	48-port Campus LAN HPOE switch	FastIron 07.4.00 and later
ICX 6450 stacking switch	Campus LAN stacking switch	FastIron 8.0 or later
ICX 6450-24 switch	24-port Campus LAN switch	FastIron 07.4.00 and later
ICX 6450-24 Base L3 router	24-port Campus LAN Base L3 router	FastIron 07.4.00 and later
ICX 6450-24 Base router	24-port Campus LAN Base router	FastIron 07.4.00 and later
ICX 6450-24 Premium router	24-port Campus LAN Premium router	FastIron 07.4.00 and later
ICX 6450-24-HPOE switch	24-port Campus LAN HPOE switch	FastIron 07.4.00 and later
ICX 6450-24-HPOE Base L3 router	24-port Campus LAN HPOE Base L3 router	FastIron 07.4.00 and later

TABLE 2 IronWare-supported hardware (Continued)

Device name	Terminology used in documentation	Firmware level required
ICX 6450-24-HPOE Base router	24-port Campus LAN HPOE Base router	FastIron 07.4.00 and later
ICX 6450-24-HPOE Premium router	24-port Campus LAN HPOE Premium router	FastIron 07.4.00 and later
ICX 6450-48 switch	48-port Campus LAN switch	FastIron 07.4.00 and later
ICX 6450-48 Base L3 router	48-port Campus LAN Base L3 router	FastIron 07.4.00 and later
ICX 6450-48 Base router	48-port Campus LAN Base router	FastIron 07.4.00 and later
ICX 6450-48 Premium router	48-port Campus LAN Premium router	FastIron 07.4.00 and later
ICX 6450-48-HPOE switch	48-port Campus LAN HPOE switch	FastIron 07.4.00 and later
ICX 6450-48-HPOE Base L3 router	48-port Campus LAN HPOE Base L3 router	FastIron 07.4.00 and later
ICX 6450-48-HPOE Base router	48-port Campus LAN HPOE Base router	FastIron 07.4.00 and later
ICX 6450-48-HPOE Premium router	48-port Campus LAN HPOE Premium router	FastIron 07.4.00 and later
ICX 6430 IronStack switch	24-port Campus LAN stackable switch	FastIron 07.4.00 and later
ICX 6430 IronStack Base L3 router	Campus LAN Base L3 stackable router	FastIron 07.4.00 and later
ICX 6430 IronStack Base router	Campus LAN Base stackable router	FastIron 07.4.00 and later
ICX 6430 IronStack Premium router	Campus LAN Premium stackable router	FastIron 07.4.00 and later
ICX 6450 IronStack switch	48-port Campus LAN stackable switch	FastIron 07.4.00 and later Hyper Edge stacking requires FastIron 8.0 or later
ICX7750-26Q switch	26 fixed 40 GbE and six 40 GbE slot module	FastIron 08.0.10 and later
ICX7750-48F switch	48 fixed 10 GbE and six fixed 40 GbE + 6×40 GbE slot	FastIron 08.0.10 and later
ICX7750-48C switch	48 10GBase-T and six fixed 40 GbE +6×40 GbE slot	FastIron 08.0.10 and later
FastIron GS	Ethernet L2/L3 Access switch	
FastIron GS-STK	Ethernet L2/L3 Access switch, stackable	
FastIron LS	Enterprise LAN switch	
FastIron LS-STK	Enterprise LAN switch, stackable	
FastIron SuperX/SX	Enterprise LAN chassis	FSX 02.4.00 and later
FastIron SX 800 and FastIron SX 1600	SX-FI2XGMRXL6 two port 10G management module supported	FastIron 08.0.10 and later
FastIron 8-port 10 GbE SFP Blade	8-port 10 GbE SFP Blade	
FastIron 24-port Fiber SFP GbE Blade	24-port Fiber SFP GbE Blade	
FastIron 24-port GbE Cu Blade	24-port GbE Cu Blade	
FastIron 2-port 10GbE SFP+ Blade	2-port 10GbE SFP+ Blade	
FastIron Edge Switch X-Series	Enterprise LAN Edge switch	
FastIron Edge X 424	Enterprise LAN Edge switch, 24 10/100/1000 Mbps ports	

TABLE 2 IronWare-supported hardware (Continued)

Device name	Terminology used in documentation	Firmware level required
FastIron Edge X 624	Enterprise LAN Edge switch, 24 10/100/1000 Mbps ports	
FastIron Edge X 448	Enterprise LAN Edge switch, 48 10/100/1000 Mbps ports	
FastIron Edge X 648	Enterprise LAN Edge switch, 48 10/100/1000 Mbps ports	
FastIron Edge X 424HF	Enterprise LAN Edge switch, 20 100/1000 Mbps SFP ports	
FastIron Edge X 624HF	Enterprise LAN Edge switch, 20 100/1000 Mbps SFP ports	
FastIron WS devices	Enterprise Campus switch	
Motorola Controllers RFS4000 series	Wireless controller	Mobility 5.1
Motorola Controllers RFS6000 series	Wireless controller	Mobility 5.1
Motorola Controllers RFS7000 series	Wireless controller	Mobility 5.1
Motorola Access Point 7131	Wireless access point	Mobility 4.1.1 (standalone mode) Mobility 5.1 [1] (adaptive mode)
Motorola Access Point 7131N	Wireless access point	Mobility 4.1.1 (standalone mode) Mobility 5.1 [1] (adaptive mode)
Motorola Access Point 5181	Wireless access point	Mobility 2.5.X (standalone mode) Mobility 5.1 [1] (adaptive mode)
Motorola Access Point 6511	Wireless access point	Mobility 5.1 [1] (adaptive mode)
NetIron family	Ethernet routers	NetIron 5.0.0 or 5.0.1
NetIron MLX (Supported regardless of license configuration)	Ethernet router	NetIron 5.0.0 or 5.0.1
NetIron MLXe (Supported regardless of license configuration)	Ethernet Core router	NetIron 5.0.0 or 5.0.1
NetIron XMR (Supported regardless of license configuration)	Ethernet Backbone router	NetIron 5.0.0 or 5.0.1
NetIron CES 2048CX (NI-CES-2048CX-AC) (Supported regardless of license configuration)	Ethernet Carrier router	NetIron 5.0.0 or 5.0.1
NetIron CER (Supported regardless of license configuration)	Ethernet Edge router	NetIron 5.0.0 or 5.0.1
ServerIron family	Application product	
ServerIron ADX 1000	Application switch	
ServerIron ADX 1000F	Application Fiber switch	ADX 12.3.03 or later
ServerIron ADX 4000	4U Application Delivery chassis	ADX 12.1.00 or later
ServerIron ADX 10000	10U Application Delivery chassis	ADX 12.1.00 or later

TABLE 2 IronWare-supported hardware (Continued)

Device name	Terminology used in documentation	Firmware level required
TurboIron Family	Data Center switch	4.1.00d or 4.2.00 or later
TurboIron 24X (T1-24X-AC)	Data Center switch	4.1.00d or 4.2.00 or later
Brocade 6650 Switch	Data Center switch	FastIron 7.5 and later
Brocade 6650 Base L3 Router	Data Center base L3 router	FastIron 7.5 and later
Brocade 6650 Router	Data Center router	FastIron 7.5 and later

1 The Management application cannot discover or manage wireless access points running Mobility 5.1.

Network OS hardware and software support

Network Advisor 12.2.0 supports the Network OS 4.1.0 firmware platform. For platform-specific firmware requirements, if any, refer to Table 3.

Table 3 lists the hardware platforms supported by this release of Network Advisor 12.2.0, the terminology used in the documentation, as well as any specific firmware requirements.

TABLE 3 Network OS-supported hardware

Device name	Terminology used in documentation	Firmware level required
Brocade VDX 2730 10 Gbps connection blade	VDX 2730 10 Gbps connection blade	2.1.1_fuj
Brocade VDX 2740 switch	VDX 2740 switch	4.0.0_bbd
Brocade VDX 6710 switch	VDX 6710 switch	2.1 or later
Brocade VDX 6720-24 switch	VDX 6720-24 switch	2.1 or later
Brocade VDX 6710T-1G switch	VDX 6710T-1G switch	4.1 or later
Brocade VDX 6720-60 switch	VDX 6720-60 switch	2.1 or later
Brocade VDX 6730-32 switch	VDX 6730-32 switch	2.1 or later
Brocade VDX 6730-76 switch	VDX 6730-76 switch	2.1 or later
Brocade VDX 6740 switch	VDX 6740 switch	4.0 or later
Brocade VDX 6740-T switch	VDX 6740-T switch	4.0 or later
Brocade VDX 8770-4 switch	VDX 8770-4 switch	3.0 or later
Brocade VDX 8770-8 switch	VDX 8770-8 switch	3.0 or later
Brocade VDX 8770 with 40G/10G Base-T/100G by line card	VDX 8770 switch with 40G/10G Base-T/100G by line card	4.1 or later

What's new in this document

The following changes have been made since this document was last released:

- Information that was added:
  - Troubleshooting
    - Element Manager troubleshooting
  - IP Element Manager
    - Configure dialog box
  - Dashboard Management
    - Top Port Traffic monitor
- Information that was changed:
  - CLI Configuration Management
    - Product configuration templates
  - Dashboard
    - Monitoring and Alerting Policy Suite/Fabric Watch widgets
    - Out of Range violations widget
    - Port Health violations widget
  - VCS Management
    - Tracing Ethernet fabric routes
  - Device Properties
    - Viewing VCS fabric properties
    - Viewing IP device and port properties
  - Database tables
  - IP Element Manager
    - Element Manager interface overview
    - Displaying port properties
    - Element Manager toolbar
    - Performance data
  - Performance Data
    - Configuring a monitor from a performance graph
    - IP real-time performance monitoring
    - Traffic flow dashboard monitors
  - VLAN Management
    - VLAN Manager
    - Port VLAN
- Information that was deleted:
  - License support for Ethernet fabrics

For further information about new features and documentation updates for this release, refer to the release notes.

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names Identifies the names of user-manipulated GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI
italic text	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles
`code` text	Identifies CLI output Identifies command syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, **switchShow**. In actual examples, command lettercase is all lowercase.

Notes, cautions, and warnings

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE
A note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates potential damage to hardware or data.

Key terms

For definitions specific to Brocade and Fibre Channel, see the *Brocade Glossary*.

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at:

http://www.snia.org/education/dictionary

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced trademarks and products
Linus Torvalds	Linux
Microsoft Corporation	Windows, Windows NT, Internet Explorer
Netscape Communications Corporation	Netscape
Red Hat, Inc.	Red Hat, Red Hat Network, Maximum RPM, Linux Undercover
Oracle	Solaris, Java Plug-in
The Open Group	UNIX
VMware, Inc.	VMware

Additional information

This section lists additional Brocade and industry-specific documentation that you might find helpful.

Brocade resources

To get up-to-the-minute information, go to *http://my.brocade.com* to register at no cost for a user ID and password.

White papers, online demonstrations, and data sheets are available through the Brocade website at:

http://www.brocade.com/products-solutions/products/index.page

For additional Brocade documentation, visit the Brocade website:

http://www.brocade.com

Release notes are available on the MyBrocade website and are also bundled with the Fabric OS firmware.

Other industry resources

For additional resource information, visit the Technical Committee T11 website. This website provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, and other applications:

http://www.t11.org

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association website:

http://www.fibrechannel.org

Getting technical help

Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

1. Management Application Serial Number

   To obtain the Management application serial number, select **Help > License**. The **License** dialog box displays.

2. General Information

   - Switch model
   - Switch operating system version
   - Error numbers and messages received
   - **supportSave** command output
   - Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions
   - Description of any troubleshooting steps already performed and the results
   - Serial console and Telnet session logs
   - syslog message logs

3. World Wide Name (WWN)

   Use the **licenseIdShow** command to display the WWN of the chassis.

   If you cannot use the **licenseIdShow** command because the switch is inoperable, you can get the WWN from the same place as the serial number, except for the Brocade DCX. For the Brocade DCX, access the numbers on the WWN cards by removing the Brocade logo plate at the top of the nonport side of the chassis.

Document feedback

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to:

documentation@brocade.com

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

Chapter

1 Getting Started

In this chapter

User interface components

The Management application provides easy, centralized management of the network, as well as quick access to all product configuration applications. Using this application, you can configure, manage, and monitor your networks with ease.

The Management application's main window contains a number of areas. The following graphic illustrates the various areas, and descriptions of them are listed below.

NOTE
Some widgets may be hidden. To display a widget to the **Dashboard** tab, click the Customize Dashboard icon ("Customizing the dashboard widgets and monitors" on page 217).

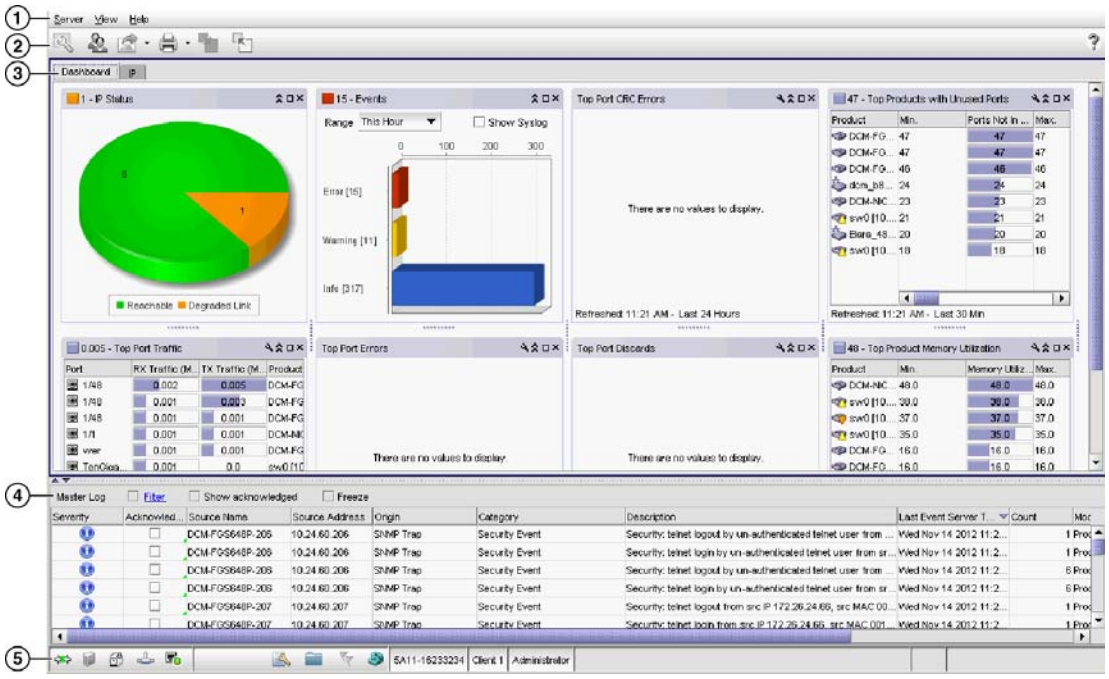


FIGURE 1 Main window

1. **Menu bar —** Lists commands you can perform on the Management application. The available commands vary depending on which tab (IP or Dashboard) you select. For a list of available commands, refer to Appendix A, "Application menus".
2. **Toolbar —** Provides buttons that enable quick access to dialog boxes and functions. The available buttons vary depending on which tab (IP or Dashboard) you select. For a list of available commands, refer to "IP main toolbar" on page 281 or "Dashboard toolbar" on page 213.
3. **Tabs —** Provides quick access to the following views:
   - **Dashboard tab —** Provides a high-level overview of the network managed by Management application server. For more information, refer to "Dashboard Management" on page 211.
   - **IP tab —** Displays the Master Log, Minimap, Connectivity Map (topology), and Product List. For more information, refer to the "IP tab overview".
4. **Status bar —** Displays the connection, port, product, special event, Call Home, and backup status, as well as Server and User data.

Management server and client

The Management application has two parts: the Server and the Client. The Server is installed on one machine and stores device-related information; it does not have a user interface. To view information through a user interface, you must log in to the Server through a Client. The Server and Clients may reside on the same machine, or on separate machines. If you are running Professional, the server and the client must be on the same machine.

Logging into a server

You must log into a server to monitor your network.

NOTE
You must have an established user account on the server to log in.

To log into a server, complete the following steps.

1. Double-click the desktop icon or open the application from the **Start** menu.

   The **Log In** dialog box displays (Figure 2).

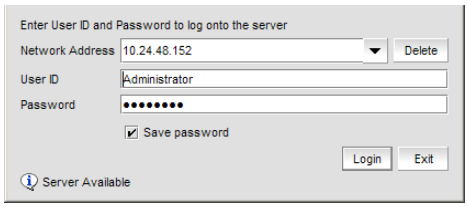


FIGURE 2 Log In dialog box

2. Log into another server by entering the IP address to the other server in the **Network Address** field.

   NOTE
   The server must be the exact same version, edition, starting port number, and network size as the client.

3. Remove a server from the **Network Address** list by selected the IP address and clicking **Delete**.
4. Choose one of the following optins:
   - If you configured authentication to CAC, enter your PIN in the CAC PIN field.
   - If you configured authentication to the local database, an external server (RADIUS, LDAP, or TACACS+), or a switch, complete the following steps.

     a. Enter your user name and password.
     The defaults are **Administrator** and **password**, respectively.

     NOTE
     Do not enter *Domain\User_Name* in the **User ID** field for LDAP server authentication.

     b. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.
     To change your password, refer to "Changing your password" on page 207.
5. Click **Login**.
6. Click **OK** on the **Login Banner** dialog box.

   The Management application displays.

Launching a remote client

NOTE
For higher performance, use a 64-bit JRE.

To launch a remote client, complete the following steps.

1. Open a web browser and enter the IP address of the Management application server in the **Address** bar.

   If the web server port number does not use the default (443 if is SSL Enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address. For example, *IP_Address*:*Port_Number*.

   The Management application web start screen displays.

2. Click the Management application web start link.

   The **Log In** dialog box displays.

3. Log into another server by entering the IP address to the other server in the **Network Address** field.

   NOTE
   The server must be the exact same version, edition, starting port number, and network size as the client.

4. Remove a server from the **Network Address** list by selected the IP address and clicking **Delete**.

5. Choose one of the following options:

   - If you configured authentication to CAC, enter your PIN in the CAC PIN field.
   - If you configured authentication to the local database, an external server (RADIUS, LDAP, or TACACS+), or a switch, complete the following steps.

     a. Enter your user name and password.
     The defaults are **Administrator** and **password**, respectively.

     NOTE
     Do not enter *Domain**User_Name* in the **User ID** field for LDAP server authentication.

     b. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.
     To change your password, refer to "Changing your password" on page 207.

6. Click **Login**.

7. Click **OK** on the **Login Banner** dialog box.

   The Management application displays.

Clearing previous versions of the remote client

The remote client link in the **Start** menu does not automatically upgrade when you upgrade the Management application. You must clear the previous version from the Java cache.

To clear the Java cache, complete the following steps.

1. Select **Start > Settings > Control Panel > Java**.

   The **Java Control Panel** dialog box displays.

2. Click **View** on the **General** tab.

   The **Java Cache Viewer** dialog box displays.

3. Right-click the application and select **Delete**.

4. Click **Close** on the **Java Cache Viewer** dialog box.

5. Click **OK** on the **Java Control Panel** dialog box.

   To create a remote client link in the **Start** menu, refer to "Launching a remote client" on page 4.

Launching the Configuration Wizard

You can re-launch the Configuration wizard to change the following configurations:

- Server IP
- Server Ports

NOTE
Changes to these configurations require a server restart.

NOTE
You can only restart the server using the Server Management Console (**Start > Programs >** *Management_Application_Name* **12.X.X > Server Management Console**).

1. Choose one of the following options:
   - On Windows systems, select **Start > Programs >** *Management_Application_Name* **12.X.X >** *Management_Application_Name* **Configuration**.
   - On UNIX systems, execute `sh Install_Home/bin/configwizard` on the terminal.
2. Click **Next** on the **Welcome** screen.
3. Click **Yes** on the confirmation message.
4. Complete the following steps on the **FTP/SCP/SFTP Server** screen.
   a. Choose one of the following options:
      - Select **Built-in FTP/SCP/SFTP Server** to configure an internal FTP/SCP/SFTP server and select one of the following options:
        - Select **Built-in FTP Server** to configure an internal FTP server
          The internal FTP server uses a default account and port 21. You can configure your own account from the **Options** dialog box. For instructions, refer to "Configuring an internal FTP server" on page 173.
        - Select **Built-in SCP/SFTP Server** to configure an internal SCP/SFTP server
          The internal SCP/SFTP server uses a default account and port 22. You can configure your own account from the **Options** dialog box. For instructions, refer to "Configuring an internal SCP or SFTP server" on page 174.

- Select **External FTP/SCP/SFTP Server** to configure an external FTP server.
  You can configure the external FTP server settings from the **Options** dialog box. For instructions, refer to "Configuring an external FTP, SCP, or SFTP server" on page 175.

b. Click **Next**.

If port 21 or 22 is busy, a message displays. Click **OK** to close the message and continue. Once the Management application is configured make sure port 21 or 2221 is free and restart the Server to start the FTP/SCP/SFTP service.

NOTE
If you use an FTP/SCP/SFTP Server which is not configured on the same machine as the Management application, the Firmware Repository feature will not be available.

5. Complete the following steps on the **Server IP Configuration** screen.

NOTE
If the Management server or client has multiple Network Interface Cards and if any of these interfaces are not plugged in, you must disable them; otherwise, the following features do not work properly:

Server impact

- Configuration wizard (does not display all IP addresses)
- Trap and Syslog auto registration
- Report content (Ipconfiguration element does not display all server IP addresses)
- Network OS configuration backup through FTP
- Trace dump through FTP

Client impact

- Options dialog box (does not display all IP addresses)
- Firmware import and download dialog box
- Firmware import for Fabric OS and Network OS products
- FTP button in Technical Support Repository dialog box
- Technical supportSave of Fabric OS, Network OS, and Host products through FTP

a. Select an address from the **Server IP Configuration** list.

b. Select an address from the **Switch - Server IP Configuration Preferred Address** list.

NOTE
If the "hostname" contains invalid characters, the host name does not display in the list. Valid characters include alphanumeric and dash (-) characters. The IP address is selected by default. If an IPv6 address is selected, server start up will fail.

If DNS is not configured for your network, do not select the 'hostname' option from either the **Server IP Configuration** or **Switch - Server IP Configuration Preferred Address** list. Selecting the 'hostname' option prevents clients and devices from communicating with the Server.

If you select a specific IP address from the **Server IP Configuration** screen and the selected IP address changes, you will not be able to connect to the server. To change the IP address, refer to "Configuring an explicit server IP address" on page 157.

c. Click **Next**.

6. Complete the following steps on the **Server Configuration** screen.

NOTE
Do not use port 2638 for any of these port numbers. Port 2638 is used internally by the server.

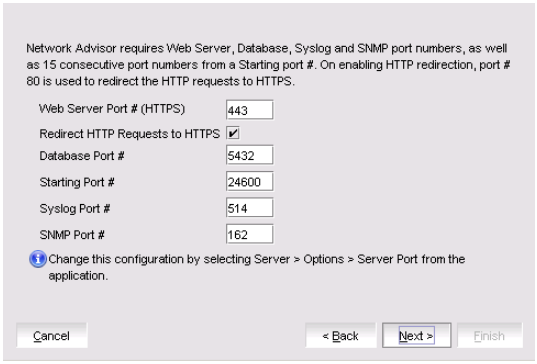


FIGURE 3 **Server Configuration screen**

a. Enter a port number in the **Web Server Port # (HTTPS)** field (default is 443).

b. Enable HTTP redirection to HTTPS by selecting the **Redirect HTTP Requests to HTTPS** check box.

When you enable HTTP redirection, the server uses port 80 to redirect HTTP requests to HTTPS. You can configure the server port settings from the **Options** dialog box (**Server Port** pane). For instructions, refer to "Configuring the server port" on page 177.

c. Enter a port number in the **Database Port #** field (default is 5432).

d. Enter a port number in the **Starting Port Number** field (default is 24600).

NOTE
For Professional software, the server requires 15 consecutive free ports beginning with the starting port number.

NOTE
For Trial and Licensed software, the server requires 18 consecutive free ports beginning with the starting port number.

e. Enter a port number in the **Syslog Port Number** field (default is 514).

NOTE
If the default syslog port number is already in use, you will not receive any syslog messages from the device. To find and stop the process currently running on the default Syslog port number, refer to the *Installation and Migration Guide*.

f. Enter a port number in the **SNMP Port Number** field (default is 162).

g. Click **Next**.

If you enter a syslog port number already in use, a message displays. Click **No** on the message to remain on the **Server Configuration** screen and edit the syslog port number (return to step 6a). Click **Yes** to close the message and continue with step 7.

If you enter a port number already in use, a Warning displays next to the associated port number field. Edit that port number and click **Next**.

7. Verify your configuration information on the **Server Configuration Summary** screen and click **Next**.
8. Complete the following steps on the **Start Server** screen:
   a. Select the **Start Client** check box, if necessary.
   b. Click **Finish**.

      After all of the services (Server and Client) are started, the **Log In** dialog box displays.
9. Click **Yes** on the restart server confirmation message.
10. Choose one of the following optins:
    - If you configured authentication to CAC, enter your PIN in the CAC PIN field.
    - If you configured authentication to the local database, an external server (RADIUS, LDAP, or TACACS+), or a switch, enter your user name and password.

      The defaults are **Administrator** and **password**, respectively.

      NOTE
      Do not enter *Domain\User_Name* in the **User ID** field for LDAP server authentication.
11. Click **Login**.
12. Click **OK** on the Login Banner.

Viewing active sessions

To view the Management application active sessions, complete the following steps.

1. Select **Server > Active Sessions**.

   The **Active Sessions** dialog box displays (Figure 5).

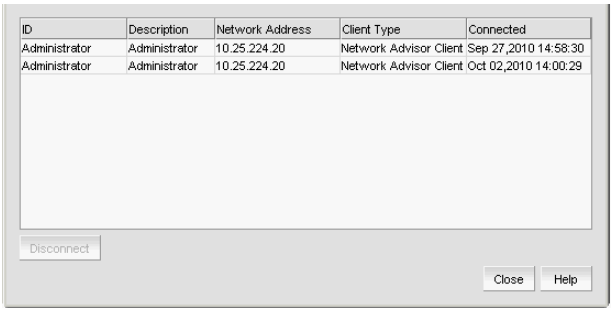


FIGURE 4 **Active Sessions dialog box**

2. Review the active session information.

   The following information displays:
   - **ID** — Displays the name of the user (for example, Administrator).
   - **Description** — Displays the description of the user (for example, Operator).
   - **Network Address** — Displays the network address of the user.

- **Client Type** — Displays the type of Management application client.
- **Connected** — Displays the date and time the user connected to the server.

3. Click **Close**.

Disconnecting users

To disconnect a user, complete the following steps.

1. Select **Server > Active Sessions**.

   The **Active Sessions** dialog box displays.

2. Select the user you want to disconnect and click **Disconnect**.
3. Click **Yes** on the confirmation message.
4. The user you disconnected receives the following message:

   The Client has been disconnected by *User_Name* from *IP_Address* at *Disconnected_Date_and_Time*.

5. Click **Close**.

   When you disconnect a client from using the Active Sessions dialog box, the following event displays in the Master Log: Disconnect Client *User_Name* @ *IP_Address*.

Viewing server properties

To view the Management application server properties, complete the following steps.

1. Select **Server > Server Properties**.

   The **Server Properties** dialog box displays.

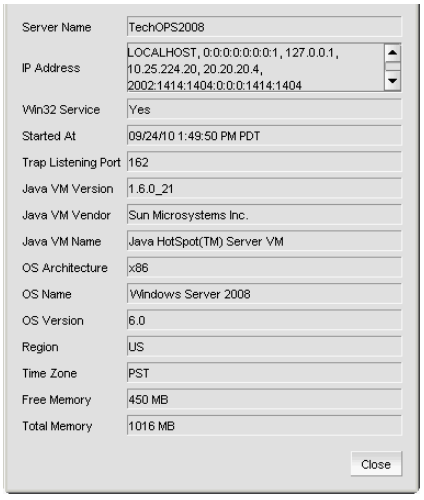


FIGURE 5 Server Properties dialog box

2. Review the information.

TABLE 4 Server Properties

Field/Component	Description
Free Memory	The amount of free memory on the server.
IP Address	The IP address in IPv4 or IPv6 format.
Java VM Name	The Java Virtual Machine name.
Java VM Vendor	The Java Virtual Machine vendor.
Java VM Version	The Java Virtual Machine version running on the server.
Server Name	The server's name.
OS Architecture	The operating system architecture on the server.
OS Name	The name of the operating system running on the server.
OS Version	The operating system version running on the server.
Region	The server's geographical region.
Started At	The time the server was started.
Time Zone	The server's time zone.
Total Memory	The total amount of memory on the server.
Trap Listening Port	The number of the UDP port that listens for SNMP traps.
Win32 Service	Specifies whether the Win32 service is available on the server. On Unix servers, displays as 'No'.

3. Click **Close** to close the **Server Properties** dialog box.

Viewing port status

The Port Status dialog box enables you to determine the availability of ports required for key Management application features. You can view the port status for the following ports:

- CIM Indication for Event Handling — Port 24618
- CIM Indication for HCM Proxy — Port 24619
- FTP — Port 21
- SCP/SFTP — Port 22
- sFlow — Port 6343
- SNMP Trap — Port 162
- Syslog — Port 514
- TFTP — Port 69
- Web Server (HTTP) — Port 80
- Web Server (HTTPS) — Port 443

To view the port status, complete the following steps.

1. Click the port status icon ( ).

   The **Port Status** dialog box displays.

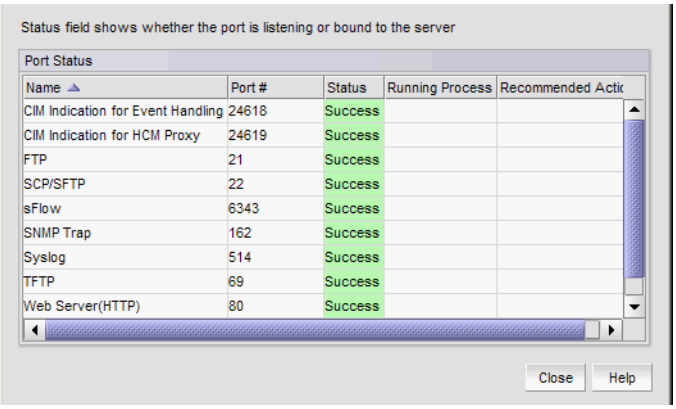


FIGURE 6 Port Status dialog box

2. Review the port status details:
   - **Name** — The Port name. Options include CIM Indication for Event Handling, CIM Indication for HCM Proxy, FTP, SCP/SFTP, sFlow, SNMP Trap, Syslog, TFTP, Web Server (HTTP), and Web Server (HTTPS).
   - **Port #** — The required port number.
   - **Status** — The status of the port. The status options are as follows:
     - Success — The port is listening or bound to the server.
     - Failed — The port fails to listen or bind to the server. It is occuppied by another process.
     - Paritally Failed — The port is used by the server as well as other applications.
     - Disabled (external FTP port only) — This is considered a normal status.
   - **Running Process** – The name of the process using the port (not the Management applciation). Blank when the port is only used by the Management applciation server. If multiple processes occupy the same port, the process names display in a comma-separated list.
   - **Recommended Actions** — Suggested action to take to resolve the issues.
3. Click **Close**.

Server and client ports

In some cases, a network may utilize virtual private network (VPN) or firewall technology, which can prohibit communication between Products and the Servers or Clients. In other words, a Server or Client can find a Product, appear to log in, but is immediately logged out because the Product cannot reach the Server or Client. To resolve this issue, check to determine if the ports in the table below need to be opened up in the firewall.

NOTE
Professional edition does not support remote clients.

Table 5 lists the default port numbers and whether or not it needs to be opened up in the firewall and includes the following information:

- **Port Number** — The port at the destination end of the communication path.
- **Ports** — The name of the port.

- **Transport** — The transport type (TCP or UDP).
- **Description** — A brief description of the port.
- **Communication Path** — The "source" to "destination" vaules. Client and Server refer to the Management application client and server unless stated otherwise. Product refers to the Fabric OS, Network OS, or IronWare devices.
- **Open in Firewall** — Whether the port needs to be open in the firewall.

TABLE 5 Port usage and firewall requirements

Port Number	Ports	Transport	Description	Communication Path	Open in Firewall
20[1]	FTP Port (Control)	TCP	FTP Control port for internal FTP server	Client–Server Product–Server	Yes
21[1]	FTP Port (Data)	TCP	FTP Data port for internal FTP server	Client–Server Product–Server	Yes
22[2]	SSH or SCP or SFTP	TCP	Secure telnet and secure upload and download to product	Server–Product Client –Product Product – Server	Yes
23	Telnet	TCP	Telnet port from server/client to product	Server–Product Client–Product	Yes
25[2]	SMTP Server port	TCP	SMTP Server port for e-mail communication if you use e-mail notifications without SSL	Server–SMTP Server	Yes
49[2]	TACACS+ Authentication port	TCP	TACACS+ server port for authentication if you use TACACS+ as an external authentication	Server–TACACS+ Server	Yes
69	TFTP	UDP	File upload/download to product	Product-Server	Yes
80[2]	Management application HTTP server	TCP	Non-SSL HTTP/1.1 connector port if you use secure client-server communication. You need this port for HTTP redirection	Client–Server	Yes
80[1]	Product HTTP server	TCP	Product non-SSL http port for http and CAL communication if you do not use secure communication to the product	Server–Product	Yes
			Product non-SSL http port for http and CAL communication if you do not use secure communication to the product and you do not use the Management application server proxy	Client–Product	Yes
161[2]	SNMP port	UDP	Default SNMP port	Server–Product	Yes
162[2]	SNMP Trap port	UDP	Default SNMP trap port	Product-Server	Yes
389[2]	LDAP Authentication Server Port	UDP TCP	LDAP server port for authentication if you use LDAP as an external authentication	Server–LDAP Server	Yes

TABLE 5 Port usage and firewall requirements (Continued)

Port Number	Ports	Transport	Description	Communication Path	Open in Firewall
443[1,2]	HTTPS server	TCP	HTTPS (HTTP over SSL) server port if you use secure client - server communication	Client-Server	Yes
443[2]			HTTPS (HTTP over SSL) server port if you use secure communication to the product	Server–Product	Yes
443			HTTPS (HTTP over SSL) server port if you use secure communication to the product and you do not use the Management application server proxy	Client–Product	Yes
443[2]			HTTPS (HTTP over SSL) server port if you use vCenter discovery	Server-vCenter Server	Yes
465[2]	SMTP Server port for SSL	TCP	SMTP Server port for e-mail communication if you use e-mail notifications with SSL	Server-SMTP Server	Yes
514[2]	Syslog Port	UDP	Default Syslog Port	Product–Server Managed Host - Server	Yes
636[2]	LDAP Authentication SSL port	TCP	LDAP server port for authentication if you use LDAP as an external authentication and SSL is enabled	Server–LDAP Server	Yes
1812[2]	RADIUS Authentication Server Port	UDP	RADIUS server port for authentication if you use RADIUS as an external authentication	Server–RADIUS Server	Yes
1813[2]	RADIUS Accounting Server Port	UDP	RADIUS server port for accounting if you use RADIUS as an external authentication	Server–RADIUS Server	Yes
5432	Database port	TCP	Port used by database if you access the database remotely from a third-party application	Remote ODBC–Database	Yes
5988	SMI Server port	TCP	SMI server port on the Management application and the CIM/SMI port on HBAs if you use SMI Agent without SSL	SMI Client- Server	Yes
				Server-Managed Host	Yes
5989[1,2]	SMI Server port with SSL enabled	TCP	SMI Agent port on the Management application and the CIM/SMI port on HBAs if you use SMI Agent with SSL	SMI Agent Server–Client	Yes
				Server-Managed Host	Yes

TABLE 5 Port usage and firewall requirements (Continued)

Port Number	Ports	Transport	Description	Communication Path	Open in Firewall
6343[2]	sFlow	UDP	Receives sFlow data from products if you are monitoring with sFlow	Product-Server	Yes
24600[1,2]	JNP (Java Naming Protocol) port	TCP	Use for service location. Uses SSL for privacy.	Client–Server	Yes
24601[1,2]	EJB (Enterprise Java Bean) connection port	TCP	Client requests to server. Uses SSL for privacy.	Client–Server	Yes
24602[1,2]	HornetQ Netty port	TCP	Use for JMS (Java Message Service), async messages from server to client. Uses SSL for privacy.	Client–Server	Yes
24603[1,2]	JMX RMI port	TCP	Use for JMS control. Uses SSL for privacy.	Client–Server	Yes
24604[1,2]	RMI naming service port	TCP		Client–Server	Yes
24605[1,2]	RMI/JRMP invoker port	TCP		Client–Server	Yes
24606[1,2]	Event Handling CIM Indication listener port	TCP	Used for HBA management	Managed Host - Server	Yes
24607[1,2]	HCM Proxy CIM Indication Listener port	TCP	Used for HBA management	Managed Host - Server	Yes
24608[2]	Reserved for future use	TCP	Not used	Client - Server	No
24609[2]	Reserved for future use	TCP	Not used	Client - Server	No
24610[2]	Reserved for future use	TCP	Not used	Client - Server	No
24611[2]	JBoss Transaction Services Recovery Manager port	TCP	Not used remotely	Server	Yes
24612[2]	JBoss Transaction Status Manager port	TCP	Not used remotely	Server	Yes
24613[2]	JBoss Pooled invoker port	TCP	Not used remotely	Server	Yes
24614[2]	JBoss Socket invoker port	TCP	Not used remotely	Server	Yes
24615[2]	JBoss RMI dynamic class loading port	TCP	Web service port, not used remotely	Server	Yes
24616[2]	Apache JServ port	TCP	Proxys web server requests, not used remotely	Server	Yes
24617[2]	Remote Management application connector access port	TCP	Not used remotely	Server	Yes
34568	HCM Agent discovery port	TCP	Used for HBA management via JSON	Server - Managed Host	Yes
55556[1]	Launch in Context (LIC) client hand shaking port	TCP	Client port used to check if a Management application client opened using LIC is running on the same host **NOTE:** If this port is in use, the application uses the next available port.	Client	No

1. Port does not need to be open in the firewall for Professional edtion.

2. The default port number. You must use the same port number for all products or hosts managed by the Management server. This port is configurable in the Management server; however, some products and firmware versions do not allow you to configure a port.

Accessibility features for the Management application

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

The following list includes the major accessibility features in the Management application:

- Keyboard shortcuts
- Look and Feel

Keyboard shortcuts

You can use the keystrokes shown in the table below to perform common functions.

NOTE
To open a menu using keystrokes, press ALT plus the underlined letter. To open a submenu, open the menu, then press the key for the underlined letter (SHIFT plus letter for capitals) of the submenu option.

TABLE 6 Keyboard shortcuts

Menu Item or Function	Keyboard Shortcut
All Panels	F12
Collapse	CTRL + L
Command Tool	SHIFT + F4
Connectivity Map	F7
Copy	CTRL + C
Cut	CTRL + X
Delete	Delete
Delete All	CTRL +Delete
Help	F1
Internet Explorer	SHIFT + F2
Master Log	F5
FireFox	SHIFT + F1
Paste	CTRL + V
Product List	F9
Properties	Alt-Enter
Select All	CTRL + A
Show Ports	F4
SSH	Shift-F5
View Utilization	CTRL + U

TABLE 6 Keyboard shortcuts

Menu Item or Function	Keyboard Shortcut
Zoom In	CTRL + NumPad+
Zoom Out	CTRL + NumPad-

Look and feel customization

You can configure the Management application to mimic your system settings as well as define the size of the font.

'Look' refers to the appearance of graphical user interface widgets and 'feel' refers to the way the widgets behave.

The Management application currently uses the '*Management_Application* Default Look and Feel' for some of the components (for example, Layout, Minimap, and so on) and the "Java Metal Look and Feel" for others.

Setting the look and feel

NOTE
Setting the look and feel is only supported on Windows systems.

The following table details the Management application components that change when you set the look and feel as well as those components that do not change.

TABLE 7 Look and feel changes

Components Affected	Components Not Affected
All Java native components with Metal Look And Feel are affected.	The Connectivity map does not change when devices are present. You must change the theme using the map display settings (**View > Map Display**).
The Menu bar, Tool bar, Status bar, as well as all tables and dialog boxes are affected.	All icons and images are not affected.
Layout is affected only when it is empty.	The Minimap is not affected.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Look and Feel** in the **Category** list.

3. Choose from one of the following options:

   - Select **Default** to configure the look and feel back to the Management application defaults.
   - Select **System** to configure the Management application to have the look and feel of your system.

     This changes the look and feel for the components that use 'Java Metal Look and Feel'. For example, if you have your system display color scheme set to 'High Contrast #1', then the Management application will be set to 'High Contrast #1'. Font size of the components is not affected by theme changes.

4. Click **Apply** or **OK** to save your work.

5. Click **OK** on the message.

NOTE
Changes do not take affect until after you restart the client.

Changing the font size

The **Options** dialog box enables you to change the font size for all components including the Connectivity map of the Management application interface.

Font size changes proportionately in relation to the system resolution. For example, if the system resolution is 1024 x 768, the default font size would be 8 and large font size would be 10.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Look and Feel** in the **Category** list.
3. Select one of the following options from the **Font Size** list:
   - Select **Default** to return to the default font size.
   - Select **Small** to change the font to a smaller font size.
   - Select **Large** to change the font to a larger font size.

   NOTE
   Changing the font size to **Large** may cause the interface components (for example, text and button labels) to display incorrectly.

4. Click **Apply** or **OK** to save your work.
5. Click **OK** on the message.

NOTE
Changes do not take affect until after you restart the client.

PostgreSQL database

You can connect to the database using one of the following options:

- pgAdmin III
- ODBC client
- Command line interface

Connecting to the database using pgAdmin III

To access the PostgreSQL database, complete the following steps.

1. Choose one of the following options:
   - On Windows systems, launch the dbadmin.bat script in the *Install_Home*\bin\ directory.
   - On UNIX systems, launch the dbadmin script in the *Install_Home*\bin\ directory.

2. Selecting **File > Add Server**.

   The **New Server Registration** dialog box displays.

3. Enter the *DB_server_IP_address* or “localhost” in the **Host** field.
4. Enter the port number (default is 5432) on which the PostgreSQL server is running in the **Port** field.
5. Enter your username (default is dcmuser) in the **Username** field.
6. Enter your password (password) in the **Password** field.
7. Click **OK** on the **New Server Registration** dialog box.

   The **pgAdmin III** application displays.

8. To browse data in the database, complete the following steps.
   a. Expand the **Tables** tree in the **Object browser** pane.
   b. Right-click a table in the list and select **View Data > View All Rows**.
9. To execute a freestyle SQL query in the database, complete the following steps.
   a. Expand the **Tables** tree in the **Object browser** pane.
   b. Right-click a table in the list and select **Scripts > SELECT script**.

      The **Query** dialog box displays.

10. Select **File > Exit** to close the **pgAdmin III** application.

Connecting to the database using the ODBC client (Windows systems)

The Open Database Connectivity (ODBC) driver enables you to configure the data source name (DSN) for the database.

To install the ODBC driver and create a new data source, complete the following steps.

1. Double-click edb_psqlodbc.exe located on the DVD (*DVD_Drive/Management_Application*/odbc/Windows).
2. Install the file to the usual location for your system’s application files (for example, C:\Program Files*Management_Application* ODBC Driver) on the **Select Install Folder** screen and click **Next**.

   NOTE
   If you select an invalid location, the ODBC driver is installed in a different location than where the ODBC executable drivers are located.

3. On the **Ready to Install** screen click **Next**.
4. Click **Finish** to complete the installation.
5. Choose one of the following opitions:
   - (32-bit OS) Select **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**.
   - (62-bit OS) (Windows only) Select **Start > Run**, type `%windir%\SysWOW64\odbcad32.exe` and press **Enter**.

The **ODBC Data Source Administrator** dialog box displays.

6. Click the **System DSN** tab.
7. Click **Add**.

   The **Create a New Data Source** dialog box displays.
8. Select **PostgreSQL Unicode**.
9. Click **Finish**.

   The **PostgreSQL Unicode ODBC Driver (psqlODBC) Setup** dialog box displays.
10. Enter a name for the data source in the **Datasource** field.
11. Enter the description of the database in the **Description** field.
12. Enter the name of the database in the **Database** field.
13. Select **enable** or **disable** from the **SSL Mode** list to specify whether or not to use SSL when connecting to the database.
14. Enter the IP address or host name of the Management application server in the **Server** field.
15. Enter the database server port number (default is 5432) in the **Port Number** field.
16. Enter the database user name in the **User Name** field.
17. Enter the password in the **Password** field.
18. Click **Test** to test the connection.
19. Click **OK** on the **Connection Test** dialog box.
20. Click **Save**.
21. Click **OK** on the **ODBC Data Source Administrator** dialog box.
22. To export data, select **Data > Import External Data > New Database Query** and complete the steps in the **Data Connection Wizard**.

Connecting to the database using the ODBC client (Linux systems)

NOTE
The ODBC driver is not supported on 64-bit Linux systems.

You must have the Open Database Connectivity (ODBC) driver to allow remote clients to export data and generate reports. The ODBC driver enables you to configure the data source name (DSN) for the Network Advisor database.

Before you install the Linux ODBC driver, download the ODBC RedHat Package Manager (RPM) file based on the Linux version.

TABLE 8 ODBC RedHat Package Manager (RPM) file requirements

Linux version	RedHat Package Manager file
SUSE	Rpm –I unixODBC-2.2.12-197.17.i586.rpm
RedHat or Oracle Enterprise	Rpm –i unixODBC-2.2.11-1.i386.rpm

Installing the ODBC driver on Linux systems

To install the ODBC driver and , complete the following steps.

1. Execute the following command in the terminal:

```
> su
>chmod 777 edb_psqlodbc.bin
> ./edb_psqlodbc.bin
```

2. On the **Setup psqlODBC** screen click **Next**.
3. Install the file to the usual location for your system's application files (for example, /opt/PostgreSQL/psqlODBC) on the **Installation Directory** screen and click **Next**.

NOTE
If you select an invalid location, the ODBC driver is installed in a different location than where the ODBC executable drivers are located.

4. On the **Ready to Install** screen click **Next**.
5. On the **Completing the psqlODBC Setup Wizard** screen click **Finish** to complete the installation.

Adding the Datasourse on Linux systems

Before you edit the INI files, make sure the PostgreSQL database is up and running.

NOTE
For RedHat and Oracle Enterprise systems, the odbc.ini and odbcinst.ini files are located in /etc. For SUSE systems, the odbc.ini and odbcinst.ini files are located in /etc/unixODBC.

1. Open the odbc.ini file in an editor and enter the datasource information as follows:

```
[TestDB]
Description = PostgreSQL 8.4
Driver = /opt/PostgreSQL/psqlODBC/lib/psqlodbcw.so
Database = dcmdb
Servername = 172.26.1.54
UserName = dcmadmin
Password = passw0rd
Port = 5432
```

2. Save and close the odbc.ini file.
3. Open the odbcinst.ini file in a text editor and make sure that the driver path information is correct.

   After you install the PostgreSQL ODBC driver, the odbcinst.ini should automatically update the driver path. If the direver path is not updated, add the following:

```
[psqlODBC]
Description=PostgreSQL ODBC driver
Driver=/opt/PostgreSQL/psqlODBC/lib/psqlodbcw.so
```

4. Save and close the odbcinst.ini file.

Testing the connection on Linux systems

To test the connection, complete the following steps.

1. Download and install Open Office.
2. Select **File > New > Database**.

   The **Database Wizard** displays.
3. On the **Select database** screen, complete the following steps.
   a. Select the **Connect to an existing database** option.
   b. Select **ODBC** from the list.
   c. Click **Next**.
4. On the **Set up ODBC connection** screen, complete the following steps.
   a. Click **Browse**.

      The datasource saved in the odbc.ini file is populated in the **Datasource** dialog box.
   b. Select the datasource and click **OK** on the **Datasource** dialog box.
   c. Click **Next**.
5. On the **Set up user authentication** screen, complete the following steps.
   a. Enter the database user name in the **User name** field.
   b. Select the **Password required** check box.
   c. Click **Test Connection** to test the connection.

      The **Authentication Password** dialog box displays.
   d. Enter the database password in the **Password** field and click **OK**.
   e. Click **OK** on the **Connection Test** dialog box.

      If an error message (file not found while testing the connection) displays, copy the lib files from the <postgresSQL path>/lib/* directory to the /usr/lib/ directory.
   f. Click **Next**.
6. On the **Save and proceed** screen, click **Finish**.

Executing SQL queries from the CLI

To execute SQL queries from the command line interface (CLI) , complete the following steps.

1. Choose one of the following options:
   - On Windows systems, launch the dbsql.bat script in the *Install_Home*\bin\ directory.
   - On UNIX systems, launch the dbsql script in the *Install_Home*\bin\ directory.
2. Execute your query from the command window.
3. Close the command window.

Changing the database user password

To change the read/write or read only database password, complete the following steps in the *Install_Home*/bin directory.

1. Open a command window.
2. Type **dbpassword** *User_Name Password New_Password Confirm_Password* and press **Enter**.

   Where *User_Name* is your user name, *Password* is your current password, and *New_Password* and *Confirm_Password* are your new password. The read/write user name and password defaults are dcmadmin and passw0rd (zero), respectively. The read only user name and password defaults are dcmuser and password (all lowercase), respectively.

   If the password changed successfully, the following message displays:
   Password changed successfully.

   If an error occurs and the password did not change, the following message displays:
   Error while updating password. Please try again.
   Press any key to continue.

   If the current password and new password are the same, the following message displays:
   Old and New passwords cannot be same. Use different password and try again.
   Press any key to continue.

   If the new password and confirm password do not match, the following message displays:
   New password and confirm password do not match. Please try again.
   Press any key to continue.
3. Launch the Server Management Console.
4. Click the **Services** tab.
5. Click **Stop** to stop all services.
6. Click **Close** to close the Server Management Console.
7. Launch the Server Management Console.
8. Click **Start** to start all services.

   NOTE
   If the server is configured to use an external FTP server, the Server Management Console does not attempt to start the built-in FTP service.
9. Click **Close** to close the Server Management Console.

Supported open source software products

Table 9 lists the open source software third-party software products used in this release.

TABLE 9 Open source software third-party software products

Open Source Software	License Type
7-ZipLZMASDK 4.65	public domain
Abator 1.1	Apache License v2.0
ApacheAnt 1.7.1	Apache License v2.0

TABLE 9 Open source software third-party software products

Open Source Software	License Type
ApacheCommonsBeanUtils 1.8.1	Apache License v2.0
ApacheCommonsCodec 1.4	Apache License v2.0
ApacheCommonsCollections 3.2.1	Apache License v2.0
ApacheCommonsCompress 1.0	Apache License v2.0
ApacheCommonsConfiguration 1.6	Apache License v2.0
ApacheCommonsDBCP 1.2.2	Apache License v2.0
ApacheCommonsDigester 2.0	Apache License v2.0
ApacheCommonsDiscovery 0.4	Apache License v2.0
ApacheCommonsFileUpload 1.2.1	Apache License v2.0
ApacheCommonsHTTPClient 3.1	Apache License v2.0
ApacheCommonsIO 1.4	Apache License v2.0
ApacheCommonsJXPath 1.3	Apache License v2.0
ApacheCommonsLang 2.4	Apache License v2.0
ApacheCommonsLogging 0.4	Apache License v2.0
ApacheCommonsMath 2.0	Apache License v2.0
ApacheCommonsNet 2.0	Apache License v2.0
ApacheCommonsPool 1.5.4	Apache License v2.0
ApacheCommonsValidator 1.3.1	Apache License v2.0
Apache Extras Companion for Apache log4j 1.1	Apache License v2.0
ApacheFTPServer 1.0.3	Apache License v2.0
Apache Log4j 1.2.16	Apache License v2.0
ASM 3.2	Custom License
Axis 1.4	Apache License v2.0
AXL Radius Client API 3.29	AXL Radius Client License
BeanScriptingFramework 2.4.0	Apache License v2.0
BeanShell 2.0b4	Sun Public License / Gnu Lesser Public License
BouncyCastleCryptoProvider 1.45	Bouncy Castle License
CastorBindingFramework 0.9.9.1	Apache License v2.0
Conf M 1.9.3	Java-based software library
DNSJava 2.0.7	BeanShell Software License
dom4j 1.6.1	dom4j License
EnterpriseDTFTP 1.5.6	LGPL
GlazedLists 1.8.0	LGPL or MPL
GoogleGuice 1.0	Apache
HPInsightSoftwareVCEMWebClientSDK 6.2	HP SOFTWARE DEVELOPMENT KIT LICENSE AGREEMENT

TABLE 9 Open source software third-party software products

Open Source Software	License Type
HornetQ 2.0.0	Apache License v2.0
iBATISDAOFramework 2.2.0	Apache
iBatisforJava 2.3.4	Apache License v2.0
Infinispan 4.0.0 FINAL	LGPL v2.1
InstallAnywhere 2010	Commercial
Ireasoning SNMP API 4.0	IREASONING
iTextJavaPDFLibrary 2.1.7	Affero General Public License
JasperReports 3.6.1	GNU Lesser General Public License version 3
JavaCIFSClientLibrary 1.3.12	LGPL v2.1
JavaServiceWrapper 3.3.9	Custom License
JavaTar2.5andTarTool1.4	public domain
JaxenXpathLibrary 1.1.1	Jaxen License
JbcParser 3.7	Math Parser License
JBossApplicationServer 5.1.0 GA	LGPL
JBossWeb 2.1.9	GNU Lesser General Public License version 3
JCalendar 1.3.3	LGPL v2.1
JCommon 1.0.16	LGPL v2.1
JDOM 1.1.1	Apache Style
JFreeChart 1.0.13	LGPL v2.1
JGoodiesForms 1.2.1	BSD
JGoodiesLooks 2.2.2	BSD
JGraph 5.13.0.1	BSD Style
JIDE 2.10.1	JIDE Software License
Jmesa 2.4.5	Apache
JSON-RPCJava 1.0.1	Apache License v2.0
KajabityTools 0.1	Apache License v2.0
L2Fprod.comCommonComponents 7.3	Apache License v2.0
MaverickJavaSSHAPI 1.4.25	SSH Tools License
MimeTypeDetectionUtility 2.1.2	Apache License v2.0
MyBatisPersistenceFrameworkandSchhemaMigrationsforJava 3.0.2 GA	Apache License v2.0
OpenSAML 2.3.0	Apache License v2.0
OpenSSLforLinux 1.0.0a	OpenSSL License
PostgreSQL 9.2.1	PostgreSQL License
QualityFirstLibrary 0.99.0	Mozilla License V1.1 and qflib License
Quartz Enterprise Job Scheduler 1.66	Apache License v2.0

TABLE 9 Open source software third-party software products

Open Source Software	License Type
RockSawRawSocketLibrary 1.0.0	Apache License v2.0
SafeNet Sentinel Caffe 1.6.1	SafeNet License
SafeNet Sentinel RMS SDK 8.2.2	SafeNet License
Sblim-cim-client 1.3.9.3	HCM Sblim CIM Client
SimpleLoggingFacadeforJava 1.5.8	SLF4J License
JavaRuntimeEnvironment 1.6.0_31	Commercial
TableLayout 2009-06-10	Custom License
VIJavaAPI 2.1	BSD License
WBEM Solutions J WBEM Server 3.4.4	Commercial
WebNMSSNMPAPI 4.0.6	WebNMS License
XML RPC 1.2-B1	Open Source
YourKitJavaProfiler 9.5.1	YourKit License

1 Supported open source software products

Chapter

2

Patches

In this chapter

Installing a patch

The patch installer enables you to update the Management application between releases. Each patch installer includes the previous patches within a specific release. For example, patch F (11.X.Xf) includes the upgrades in the patch installers for A (11.X.Xa) through E (11.X.Xe).

To install a patch, complete the following steps.

1. Stop all services by completing the following steps.
    a. Launch the Server Console.
    b. Click the **Services** tab.
    c. Click **Stop** to stop all services.

    NOTE
    If you perform patch upgrade while services are running, an error message displays.

2. Go to the `/bin` directory.

    Install_Home/bin (Windows)

    /opt/*Application_Name*/bin (UNIX)

3. Execute the patch file for your operating system:

    `patch.bat` (Windows)

    `patch.sh` (UNIX)

    The **Upgrade** dialog box displays.

4. Browse to the patch file.

    The patch zip file uses the following naming convention: <*Application*>_<*Major_Version*><*Minor_Version*><*Revision_Number*><*Patch_Version*>_<*Company_Name*>.zip (for example na_1130a_<*Company_Name*>.zip).

5. Click **Upgrade**.

    If the patch process is interrupted (for example, loss of power), you must restart the patch process.

    The patch installer performs the following functions:

- Extracts patch files to the *Install_Home* folder.
- Creates a back up (zip) of the original files to be updated and copies the zip file to the *Install_Home*\patch-backup directory (for example, *Install_Home*\patch-backup\na_11-3-0a.zip).

  The first time you apply a patch, the back up patch zip file uses the following naming convention: <*Application*>_<*Major_Version*>-<*Minor_Version*>-<*Revision_Number*><*Patch_Version*>.zip (for example, *Install_Home*\patch-backup\na_11-3-0a.zip).

  Each additional time you apply a patch, the back up patch zip file uses the following naming convention: <*Application*>_<*Major_Version*>-<*Minor_Version*>-<*Revision_Number*><*Patch_Version*>-<*Previous_Patch_Version*>.zip (for example, *Install_Home*\patch-backup\na_11-3-0-patch-a.zip).
- Generates a patch log.
- Updates the conf file (*Install_Home*\conf\patch.conf) to include the patch version applied and patch created date.
- Updates the patch version in the **About** dialog box (Select **Help > About** in the main window).

6. Start all services by completing the following steps.
   a. Launch the Server Console.
   b. Click the **Services** tab.
   c. Click **Start** to start all services.

Uninstalling a patch

Note that only one set of back up files are retained which enables you revert back to the previous version. You can only revert back one version. For example:

- If you upgrade from patch A to patch B, you can revert back to patch A.
- If you upgrade from patch A to patch B to patch C then to patch F, you can only revert back to patch C.

To uninstall a patch, complete the following steps.

1. Stop all services by completing the following steps.
   a. Launch the Server Console.
   b. Click the **Services** tab.
   c. Click **Stop** to stop all services.
2. Go to the *Install_Home/*patch-backup directory.
3. Extract the patch zip file (for example, na_1120a_<*Company_Name*>.zip).
4. Open the restore.xml file from the extracted files.

   The artifacts (jar files, war files, and so on) you need to replace display as separate file tags in the restore.xml file. The location of each artifact in the extracted folder is detailed in the src value under each file tag.
5. Go to the location of the first artifact (as shown in the src value under the file tag).

6. Copy the artifact from the extracted folder to the source folder in the *Install_Home*/patch-backup directory.
7. Repeat step 5 and 6 for all artifacts listed in the restore.xml folder.
8. Go to the *Install_Home*/conf directory.
9. Open the version.properties file in a text editor.
10. Change the patch version (patch.version) value to the reverted patch (for example, if you are reverting from patch F to patch C then `patch.version = c`).

    If the previous version is the initial version (no patches), change the patch version value to none (for example, `patch.version = None`).
11. Go to the *Install_Home*/patch-backup/conf directory.
12. Copy the patch.conf file in this directory to the *Install_Home*/conf directory.

    If the previous version is the initial version (no patches), delete the patch.conf file in the *Install_Home*/conf directory.
13. Start all services by completing the following steps.
    a. Launch the Server Console.
    b. Click the **Services** tab.
    c. Click **Start** to start all services.

Chapter

3

Discovery

In this chapter

IP discovery overview

NOTE
Discovery only displays products that are assigned to your area of responsibility (AOR). For more information about user accounts, refer to "Areas of responsibility" on page 194.

NOTE
You must have the Discover Setup - IP privilege to configure and run discovery. For more information about privileges, refer to "User Privileges" on page 1283.

NOTE
You must have the **All IP Products** AOR (area of responsibility) in your user account to discover new products. For more information about user accounts, refer to "User accounts" on page 185.

NOTE
IP discovery requires Internet Control Message Protocol (ICMP) or Telnet support on the device to determine device reachability.

Discovery is the method that the Management application uses to find data networking devices on the network. When the Management application discovers devices, it finds all IP addresses on a device and stores them in the Management application database. The Management application uses the primary address of a product to communicate with the product. The primary address is determined using the following rules:

- If you configure discovery to prefer loopback addresses (refer to "Defining global setting preferences" on page 60), and there are loopback IP addresses configured in the product; and the loopback IP address is reachable from the Management application server, then the loopback IP address is the primary IP address of the product.
- If you did not configure discovery to prefer loopback addresses, the original IP address used to discover the product is the primary IP address of the product.

The primary address is the address that appears on the Network Object Manager and other configuration and display panels in the Management application.

The Management application provides two types of discovery, simple discovery and profile-based discovery.

Simple discovery discovers the device with a specific IP address and/or DNS name. It is triggered by device configuration changes on SNMP traps, certain configuration deployments to a device, and adding device or rediscovering a device from the **Discover Setup – IP** dialog box.

Profile-based discovery allows you to define the discovery policy. It provides more flexible ways to specify IP addresses to discover. It also enables you to discover new devices from already discovered devices.

Profile-based discovery uses the following steps to build a list of candidate IP addresses to probe.

1. Discovery runs one of the following programs:
   - On Windows systems, use ipconfig to find the default gateway.
   - On UNIX systems, use netstat -r -n to determine the "seed" routers and extract IP addresses from the program output.

     Discovery adds these IP addresses to the list of candidate IP addresses.

2. Discovery queries the database to retrieve the IP address for each previously discovered device and adds these IP addresses to the list of candidate IP addresses.
3. Discovery adds the IP addresses from the IP address file to the list of candidate addresses.
4. As the discovery cycle proceeds, discovery adds addresses from the ping sweep address ranges to the list of candidate addresses.
5. Discovery searches for neighbors of a discovered device using the information located in the device's SNMP Link Layer Discovery Protocol (LLDP), Foundry Discovery Protocol (FDP), Cisco Discovery Protocol (CDP), and Address Resolution Protocol (ARP) tables. To search for neighbors, you must configure discovery to search for neighbor addresses (refer to "Configuring advanced discovery profile preferences" on page 78).

After creating the list of candidate IP addresses, discovery uses multiple threads to probe devices. You can define how many threads can be used at one time. Threads operate in parallel, so communication to multiple devices occurs simultaneously. Each thread takes one address from the list of candidate IP addresses and probes it. The first step in probing is to determine whether the device is reachable or not. Discovery provides two methods to determine reachability. The first method uses ICMP ping to probe the device. The second method opens a connection to the IP address (currently to the Telnet port). This serves as a "ping" to confirm that the IP address is reachable and some device is listening. By default, if the device responds by either accepting or rejecting the connection, then the connection is closed and discovery continues.

The next step uses SNMP queries. The first query determines whether the device is a IronWare OS or Network OS device or not. Discovery rotates through a list of candidate SNMP community strings until it finds one that works. For devices that already exist in the database, the community string recorded in the database for that device is tried first.

If you configure discovery to search for neighbor addresses (refer to "Configuring advanced discovery profile preferences" on page 78), the second query scans the device's SNMP ARP table. Discovery adds any IP address from the ARP table to the list of candidate IP addresses.

Similarly, if you configure discovery to search for neighbor addresses (refer to "Configuring advanced discovery profile preferences" on page 78), the third query scans the device's SNMP LLDP, FDP, and CDP tables. Any neighbor IP address is added to the list of candidate IP addresses to probe. Discovery adds any IP address from the LLDP, FDP, and CDP tables to the list of candidate IP addresses.

Discovery also tries to determine the host name of the device by requesting the Management application server operating system to perform various mappings of the device IP addresses to host names and host names back to IP addresses, using whatever mechanism the operating system uses (typically Domain Name Server) to determine the host name for a device.

If discovery determines that the device is reachable and manageable, then discovery uses the full set of SNMP queries to collect asset information from the device. Discovery then adds or updates the device in the database and sends notification to other applications.

Rediscovery updates can occur using any of the following methods:

- Lazy polling.
- Adaptive discovery (triggered by snmp traps).
- Manual rediscovery (refer to "IP Rediscovery" on page 108).

Configuration requirements

Before configuring discovery, obtain the following information:

- SNMPv1 and SNMPv2c read-write community strings or SNMPv3 read-write credentials for the devices to be included in discovery. Make sure that devices you want to manage have the SNMP credentials configured. For more information, refer to "IP SNMP credentials" on page 46.
- Device IP addresses and subnets to probe during discovery. For more information, refer to "Configuring address ranges" on page 66, "Adding user credentials" on page 52, and "Defining global setting preferences" on page 60.

Discovery of IPv6 addresses

The Management application discovers both IPv4 and IPv6 addresses of devices that have the IPv6 MIB objects implemented. The Management application discovers IPv4 addresses of devices running IPv6 that do not have IPv6 MIB support. For more information, refer to "Defining global setting preferences" on page 60.

NOTE
IronWare IPv6 devices must support the set of MIBs presented in Table 10 on page 34. To determine IPv6 MIB object support on the device, refer to the release notes and user documentation for your IPv6 product.

NOTE
Third-party IPv6 devices must support the set of MIBs presented in Table 11 on page 36.

MIB support

IP discovery requires SNMP management information base (MIB) support on the device for management information collection. For a list of required MIBs, refer to Table 10 on page 34 or Table 11 on page 36.

TABLE 10 Required MIB support for IronWare OS devices

IETF standard	MIB name	Required MIB object	Data collected
N/A	Brocade MIB		
IEEE 802.1AB	LLDP-MIB	lldpObjects.lldpRemoteSystemsData	For Layer 2 topology information: Entire lldpObjects.lldpRemoteSystemsData

TABLE 10 Required MIB support for IronWare OS devices (Continued)

IETF standard	MIB name	Required MIB object	Data collected
RFC 1213	MIB-II	mib-2.system mib-2.interfaces.ifTable mib-2.ip.ipAddrTable	From mib-2.interfaces.ifTable for interface level information: • ifName/ifDescr • ifAlias • ifType • ifMtu • ifSpeed • ifPhysAddress • ifAdminStatus • ifOperStatus • ifLastChange From mib-2.ip.ipAddrTable for IP subnet information: • ipAdEntAddr • ipAdEntNetMask From mib-2.ip.ipAddrTable for Layer 3 topology information: • ipForwarding
RFC 2465	IPv6-MIB	ipv6MIBObjects ipv6NetToMediaTable ipv6MIBObjects.ipv6AddrTable	From ipv6MIBObjects and ipv6NetToMediaTable for interface level information: • ifName/ifDescr • ifAlias • ifType • ifMtu • ifSpeed • ifPhysAddress • ifAdminStatus • ifOperStatus • ifLastChange From ipv6MIBObjects.ipv6AddrTable for IP subnet information: • ipv6AddrAddress • ipv6AddrPfxLength
RFC 2863	IF-MIB	ifMIBObjects.ifXTable	From ifMIBObjects.ifXTable for interface level information: • ifName/ifDescr • ifAlias • ifType • ifMtu • ifSpeed • ifPhysAddress • ifAdminStatus • ifOperStatus • ifLastChange
RFC 4363	Q-BRIDGE-MIB	dot1qVlan.dot1qPortVlanTable	For VLAN information: Entire dot1qVlan.dot1qPortVlanTable

Table 11 provides a list of MIB support required for third-party devices.

TABLE 11 Required MIB support for third-party devices

IETF standard	MIB name	Required MIB object	Data collected
RFC 1213	MIB-II	mib-2.system mib-2.interfaces.ifTable mib-2.ip.ipAddrTable	From mib-2.interfaces.ifTable for interface level information: • ifName/ifDescr • ifAlias • ifType • ifMtu • ifSpeed • ifPhysAddress • ifAdminStatus • ifOperStatus • ifLastChange From mib-2.ip.ipAddrTable for IP subnet information: • ipAdEntAddr • ipAdEntNetMask From mib-2.ip.ipAddrTable for Layer 3 topology information: • ipForwarding
RFC 2465	IPv6-MIB	ipv6MIBObjects ipv6NetToMediaTable ipv6MIBObjects.ipv6AddrTable	From ipv6MIBObjects and ipv6NetToMediaTable for interface level information: • ifName/ifDescr • ifAlias • ifType • ifMtu • ifSpeed • ifPhysAddress • ifAdminStatus • ifOperStatus • ifLastChange From ipv6MIBObjects.ipv6AddrTable for IP subnet information: • ipv6AddrAddress • ipv6AddrPfxLength
RFC 2863	IF-MIB	ifMIBObjects.ifXTable	From ifMIBObjects.ifXTable for interface level information: • ifName/ifDescr • ifAlias • ifType • ifMtu • ifSpeed • ifPhysAddress • ifAdminStatus • ifOperStatus • ifLastChange

TABLE 11 Required MIB support for third-party devices (Continued)

IETF standard	MIB name	Required MIB object	Data collected
RFC 4133	ENTITY-MIB	entPhysicalTable entAliasMappingTable (if available)	For module (line card) information: Entire entPhysicalTable Entire entAliasMappingTable, if available
RFC 4293	IP-MIB	mib2.ip.ipAddressTable	For ip address and subnet information ipAddressAddrType ipAddressAddr ipAddressIfIndex ipAddressType ipAddressPrefix

VDX/VCS discovery

NOTE
Discovery of a VDX device requires Network OS 2.1.0 or later.

NOTE
Discovery a VCS fabric requires that the seed switch must be running Network OS 2.1.0 or later; however, the fabric can include members running Network OS 2.0.0.

NOTE
VDX/VCS discovery requires read and write IP Discovery privilege. For more information about privileges, refer to "User Privileges" on page 1283.

NOTE
You must have the **All IP Products** AOR (area of responsibility) in your user account to discover new products. For more information about user accounts, refer to "User accounts" on page 185.

Network OS devices can only be discovered from the IP tab. You can discover a standalone VDX or VCS-enabled devices as well as VCS fabrics. VDX/VCS devices display in the Network Objects, L2 Topology, Ethernet Fabrics, IP Topology, and VLAN Topology views.

VDX device and VCS fabric discovery uses the Read/Write Login Prompt credentials for authentication (refer to "Adding user credentials" on page 52). You cannot discover VDX devices using root level privileges. If you do not provide discovery credentials, the Management application uses the default switch credentials for the admin account. You can edit the credentials for multiple VDX/VCS devices when they all have same firmware version (refer to "Editing IP device discovery" on page 87).

VCS fabrics display in a tree structure with member nodes. When you discover a new fabric and initial discovery is complete, the fabric automatically tracks the fabric members. Subsequently, if a member is removed from the fabric, a minus (-) icon displays (see table below) next to the product icon.

TABLE 12

	Device Removed

VCS devices use the following to determine reachability:

- Reachable — The VDX/VCS product is online and is accessible by ICMP, Netconf, and SNMP; therefore, it is reachable.
- Degraded Link — The VDX/VCS product is not accessible by one of the following: ICMP, Netconf, or SNMP.
- Not Reachable — The VDX/VCS product is offline and is not accessible by any of the following: ICMP, Netconf, and SNMP.

The following sections detail the VDX/VCS discovery behavior.

Network OS discovery IP address format

You can discover Network OS devices using an IPv4 or IPv6 address. To configure the preferred IP format for the Management application server to connect with Network OS devices, refer to "Configuring the preferred IP format" on page 170.

During discovery, if the product has both an IPv4 and IPv6 address, the Management server uses the preferred address. If a product does not have the preferred address type, the Management server uses the other IP type. If the Management application is not IPv6 capable, the Management application cannot discover products with an IPv6 address directly (as a seed switch). The Management application can discover products with an IPv6 address indirectly when the seed switch has an IPv4 address.

VCS in-band management interface discovery

You can discover VCS devices using in-band or out-of-band management interfaces. If you configure a VCS cluster member with both in-band and out-of-band management interfaces, the Management application uses the in-band management interface to fetch device data and the member switch displays the in-band management interface IP address in the application. If you do not configure an in-band management interface, the Management application uses the out-of-band management interface for data collection.

Mapping VCS in-band management

For VCS device in-band management, you must map the VCS device WWN to the in-band management interface IP address in the DeviceWWNToIPMap text file; otherwise, discovery fails.

1. Open the in-band mapping file (DeviceWWNToIPMap.txt) in a text editor (such as, Notepad).

   The DeviceWWNToIPMap.txt file is located in the *Install_Home*/conf/discovery/ip directory.

2. Enter the in-band IP addresses you want to include in discovery.

   You must use the following format: the device WWN, followed by a space, and then the valid in-band IP address.

   Example

   10:00:00:05:33:51:62:42 172.26.20.10

```
# DeviceWWNToIPMap.txt
# In-Band Management IP address should be mapped to Device WWN.
# The format consists of two columns per line, separated by white space.
# Each column consists of Device WWN followed by white space and followed by
In-band IP address
```

```
#
# A sample entry:
# 10:00:00:05:33:51:62:42 172.26.20.10
#
# Changes to this file do not require restarting the management server.
```

3. Select **File > Save**.

Standalone discovery

- When you discover a VDX device that is not VCS-enabled, it displays as an individual L2 (DCB) device.
- When you enable VCS mode on a discovered VDX device, after rediscovery the VDX displays as a VCS fabric.

VCS fabric discovery

NOTE
Professional edition can only discover a VCS fabric with one member.

NOTE
IP Base edition can only discover a VCS fabric with two members.

- When you discover a VDX device that is VCS-enabled and is not connected to other VCS-enabled devices, it displays as a VCS fabric with one member.
- When you discover a VDX device that is VCS-enabled and is connected to other VCS-enabled devices, it displays as a VCS fabric with all connected VCS-enabled devices as members of the fabric.
- When you discover any member in a VCS fabric through individual IP device discovery, that member acts as the seed switch and discovers all other members in the VCS fabric. The principal switch of the VCS fabric displays as a VCS fabric. The VCS fabric members display as individual L2 (DCB) devices.
- When you discover multiple members in a VCS fabric through profile discovery, the principal switch acts as the seed switch and discovers all other members (not included in profile discovery) in the VCS fabric. The principal switch of the VCS fabric displays as a VCS fabric. The VCS fabric members display as individual L2 (DCB) devices.

VCS fabric rediscovery

Rediscovery is the refreshing of the asset data for the selected product. Rediscovery of a VCS-enabled device or VCS fabric uses the following behavior:

- If you select a fabric seed switch, rediscovery refreshes the fabric membership information.
- If you select a fabric member, rediscovery refreshes the fabric member's asset data.
- If you select a missing fabric member, rediscovery results in the discovery of new fabric or discovery of a standalone switch (dependent on what happened to the disconnected member). You can also delete missing fabric members from discovery (refer to "Deleting IP devices from discovery" on page 93).

NOTE
If you do not have the **All IP Products** AOR in your user account, you cannot rediscover missing fabric members.

Seed switch failover

The Management application uses the seed switch to discover other members in the VCS fabric. When you discover devices through individual discovery, the seed switch is the first member you discover in the VCS fabric. When you discover devices through profile discovery, the seed switch is the principal switch in the VCS fabric.

- If VCS mode is disabled on the seed switch, the Management application triggers rediscovery of the other members in the VCS fabric and selects another member to act as the seed switch.
- If the seed switch becomes unreachable, the Management application selects another member of the VCS fabric to act as the seed switch.
- If the seed switch becomes unreachable from the Management application and looses connectivity with the VCS fabric, the Management application selects another member of the VCS fabric to act as the seed switch.
- If the seed switch looses connectivity with the VCS fabric but is still reachable from the Management application, the VCS fabric splits into two fabrics. When this occurs, the Management application selects another member of the VCS fabric to act as the seed switch and manages the original seed switch as a separate VCS fabric. When two fabrics regain connectivity, the Management application uses the original seed switch as the seed switch for the merged VCS fabric.

VCS fabric split and merge

- If the seed switch looses connectivity with the VCS fabric but is still reachable from the Management application, the Management application selects another member of the VCS fabric to act as the seed switch and manages the original seed switch as a separate VCS fabric.

  When the original seed switch rejoins the original VCS fabric, the Management application uses the original seed switch as the seed switch for the merged VCS fabric.

- If a member (not the seed switch) looses connectivity with the VCS fabric but is still reachable from the Management application, the VCS fabric splits into two fabrics. The Management application treats the member that lost connectivity as a separate VCS fabric.

  When the member rejoins the original VCS fabric, the Management application uses the VCS fabric that was discovered first as the merged VCS fabric.

Network OS 2.0 device limitations

VDX devices running Network OS 2.0.0 cannot be discovered directly. However, if you discover a VCS fabric (running Network OS 2.1.0 or later) that contains VDX devices (running Network OS 2.0.0), the Network OS 2.0.0 devices are included in discovery of the fabric and display on the topology map. Network OS 2.0.0 devices have the following limitations:

- Display as unreachable members in the fabric.
- Assets (ports, LAGs, VLANs, and so on) are not collected.

- TRILL links between Network OS 2.1.0 devices and Network OS 2.0.0 devices do not display.

Logical chassis cluster mode discovery

Logical chassis cluster mode requires Network OS 4.0 or later and is one of two types of VCS modes. In logical chassis cluster mode, both the data and configuration paths are distributed. The entire cluster can be configured from the principal node. The other VCS mode is *fabric cluster mode*, in which the data path for nodes is distributed, but the configuration path is not distributed and each node keeps its configuration database independently. The generic term *VCS mode* applies to both fabric cluster mode and logical chassis mode unless otherwise stated.

The **State** column of the **Discover Setup - IP** Dialog shown in Figure 7 is applicable only to nodes that are members of a logical chassis cluster. The possible node states are described later in this section.

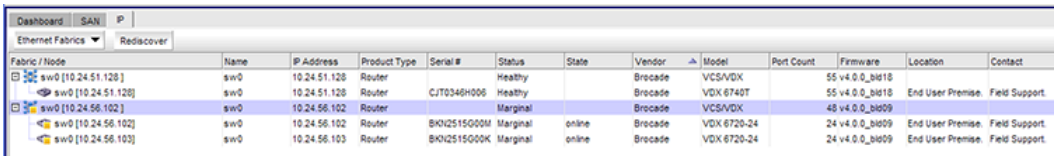


FIGURE 7 **Discovery Setup - IP dialog box with node state for logical chassis cluster**

Logical chassis cluster discovery includes the following behavior:

- Manual- or profile-based discovery is the same as for a cluster in fabric cluster mode.
- Uses the IP address of any member of the logical chassis cluster for discovery.
- Sets the cluster IP address to the IP address of the principal node.

NOTE
You can change the principal node for the cluster by running the **logical-chassis principal-priority** command from the NOS prompt. For more information, refer to the *Network OS Command Reference*.

- Principal-switch failover does not occur if the cluster is unstable (for example, if the chassis had been disabled for maintenance) because refresh collection will fail.
- If the cluster is configured with a virtual IP address before its discovery, and then discovery is initiated, the cluster IP displays the virtual IP address instead of the IP address of the principal node.
- If the cluster is configured with a virtual IP address after it is discovered by the Management application, the virtual IP address is collected and saved in the database for the next lazy polling or next adaptive collection.
- If another switch becomes the principal switch, the Management application sets the cluster IP address to that of the new principal switch at the next lazy polling or next adaptive collection.

- The **State** column in the **Discover Setup - IP** dialog shown in Figure 7 applies only to nodes that are in logical chassis mode. Possible states are:
  - Online—A node that is currently connected and operational.
  - On discovery, only online members are considered active cluster members. The Management application server collects the device, port, and LAG information of active cluster members. The the Management application client displays the member node as a cluster member in the Ethernet Fabrics topology.
  - Offline—A cluster member node that cannot be reached by the primary cluster node.
  - On refresh, if the member was an active member of a cluster and is now offline, the member is marked as missing. If the member is not online after three consecutive short ticks, auto-discovery gets initiated. If auto-chasing fails, the member remains missing.
  - Rejoining—A node that is in the process of rejoining its cluster.
  - On refresh, if the member was an active member of the cluster and is now rejoining, then the member is marked as missing. If the member is not online after three consecutive short ticks, auto discovery gets initiated. If auto chasing fails, the member remains missing.
  - Replacing—A node that is being replaced.
  - On refresh, if a member node is in the Replacing state, the member is shown as missing.
  - If the member is in the Replacing state for more than three consecutive short ticks, auto-discovery gets initiated. If auto-chasing fails, the member remains missing.

Administratively removing a node from a logical chassis cluster

You can remove a node from a logical chassis cluster by using the Network OS command line interface. For instructions, refer to the *Network OS Administrator's Guide* and the *Network OS Command Reference*, versions 4.0 or later.

Once the node is removed, all configurations corresponding to that node are removed from the cluster configuration database.

The deleted node gets rebooted automatically and boots in VCS-disabled mode.

The deleted node also gets marked as missing in the cluster.

The Management application initiates auto-discovery immediately, and the deleted node gets rediscovered in its current state.

As an example, Figure 8 shows the **Discover Setup - IP** dialog box before the administrator removes a node from the cluster.

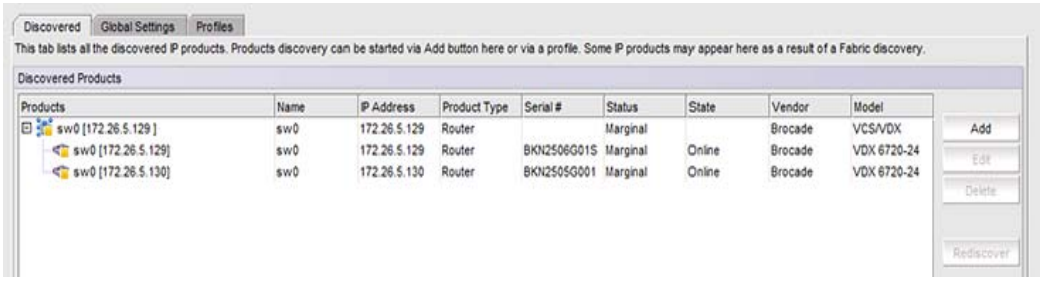


FIGURE 8 Discover Setup - IP dialog box before removal of node

Figure 9 shows the **Discover Setup - IP** dialog box after the administrator has removed the node with the IP address of 172.26.5.130 from its logical chassis cluster.

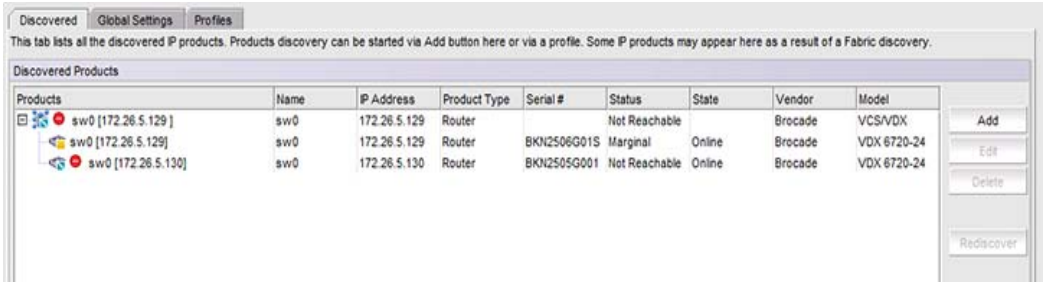


FIGURE 9 Discover Setup - IP dialog box after disabling the node from logical chassis cluster

Figure 10 shows the **Discover Setup - IP** dialog box after The Management application has performed rediscovery. The node with the IP address of 172.26.5.130 is shown as a degraded link.

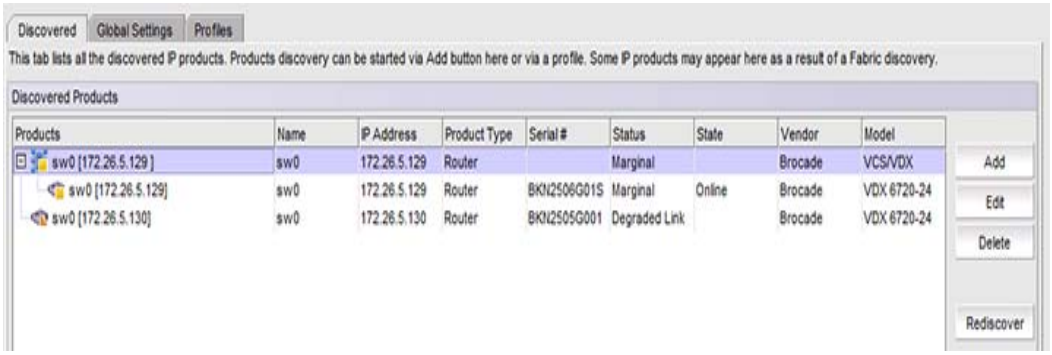


FIGURE 10 Discover Setup - IP dialog box after rediscovery

How the Management application handles a cluster mode change

In Network OS release 4.0, an administrator can change the mode of a cluster from fabric cluster mode to logical chassis cluster mode, and vice versa. For instructions, refer to the *Network OS Administrator's Guide* and the *Network OS Command Reference*.

NOTE
All cluster-specific configurations are lost during a cluster-mode change.

On refresh collection, the Management application detects the mode change and retains all database entries related to the cluster.

HyperEdge stack discovery

HyperEdge stacks must contain at least one ICX 6610 device and one ICX 6650 device and all stacking members must be running IronWare 8.0 or later (the exact same version). HyperEdge stacks support up to 8 units in stack. Note that you do not recieve an error or warning message when unit number exceeds 8. However, the HyperEdge stack may stop functioning.

For stacking between ICX 6610 devices, use the 40 Gbps Ethernet ports as the stacking ports.

For stacking between ICX 6610 and ICX 6450 devices, use the 10 Gbps Ethernet ports as the stacking ports. The 10 Gbps Ethernet ports must have the POD license enabled with 10 Gbps speed. On the ICX 6610 device, you must configure a 10 Gbps Ethernet port as a peripheral port. You can connect the ICX 6450 device 10 Gbps Ethernet port to the ICX 6610 device peripheral port.

For stacking between ICX 6450 devices, use the 10 Gbps Ethernet ports as the stacking ports.

If the ICX 6610 device have full Layer 2 and Layer 3 features, HyperEdge stacking extends the ICX 6610 device Layer 3 and other advanced capabilities to the ICX 6450 device to process packets going to ICX 6450 ports.

For HyperEdge stacking management, the master/active and standby units must be the ICX 6610 device. Management of the stacking device is through the master unit only. This includes SNMP, sFlow, syslog, tftp, telnet and ssh traffic. The management port on each member unit (except the master unit) of an HpyerEdge stack, is not visible and does not function.

Configuring IP profile discovery

NOTE
You must have the **All IP Products** AOR (area of responsibility) in your user account to discover new products. For more information about user accounts, refer to "User accounts" on page 185.

To configure profile discovery, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

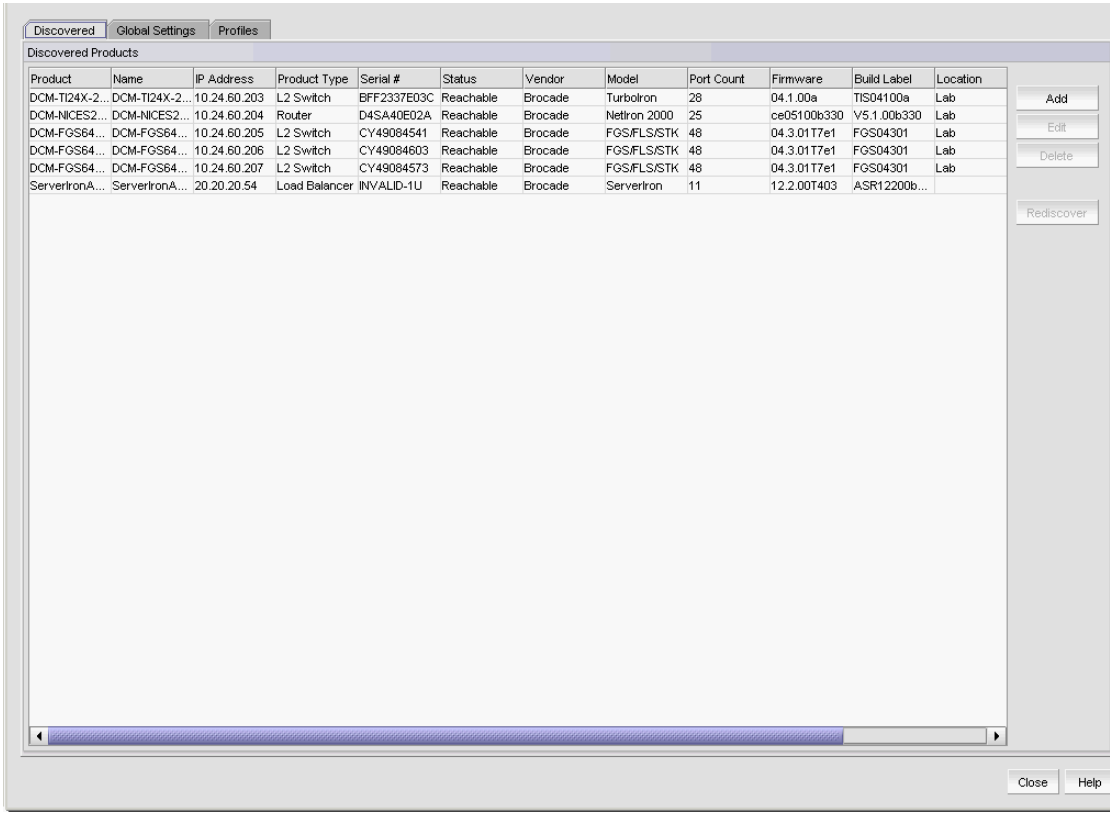


FIGURE 11 Discover Setup - IP dialog box

2. Click the **Global Settings** tab.
   a. To set SNMP credentials, refer to "IP SNMP credentials" on page 46.
   b. To configure default user names and passwords, refer to "Default IP user credentials" on page 52.
   c. To configure global setting preferences, refer to "Defining global setting preferences" on page 60.
3. Click the **Profiles** tab.
   a. To create a discovery profile, refer to "IP discovery profiles" on page 64.
   b. To include and exclude product types, refer to "IP Object identifier filters" on page 58.
   c. To include and exclude devices and enable ping sweep, refer to "Configuring address ranges" on page 66.
   d. To configure profile preferences, refer to "Configuring advanced discovery profile preferences" on page 78.
4. Click **Start** to start discovery. To run profile discovery, refer to "Starting discovery manually" on page 80.
5. Click **Close** to close the **Discover Setup - IP** dialog box.
6. Click **Yes** on the confirmation message.

Configuring IP simple discovery

NOTE
You must have the **All IP Products** AOR (area of responsibility) in your user account to discover new products. For more information about user accounts, refer to "User accounts" on page 185.

To configure simple discovery, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. To add individual devices, refer to "Adding an IP device to discovery" on page 84.
3. Click **Close** to close the **Discover Setup - IP** dialog box.
4. Click **Yes** on the confirmation message.

IP SNMP credentials

NOTE
The Management application supports SNMPv1, SNMPv2c, and SNMPv3.

The Management application requires SNMP credentials to obtain information from devices and to deploy configurations to devices. Because different devices may have different credentials, discovery can store many sets of credentials to make sure that the correct credentials are available when contacting a device.

Two types of credentials can be used for discovery: SNMPv1 and SNMPv2c read-write community strings and SNMPv3 read-write credentials. If SNMPv1 or SNMPv2c is enabled on a device, use read-write community strings. If SNMPv3 is enabled on a device, use SNMPv3 read-write credentials.

When a device is contacted, discovery tries the credentials in the order that they are listed on the **SNMP** tab on the **Global Setting** tab of the **Discover Setup - IP** dialog box until it finds one that matches the credentials on the device. Discovery tries the SNMPv3 credentials first. If none of the SNMPv3 credentials work, discovery tries the SNMPv1 and SNMPv2c credentials. Discovery must detect the read only credentials to proceed to the read-write credentials. If discovery does not detect any read-write credential, the device may still be discovered; however, all write operations through SNMP (such as configure device) do not execute properly. When a match is found, the device becomes discovered to the Management application, and its properties are saved in the database so that it can be managed by the Management application.

Devices not discovered through profile-based discovery can be added individually. For more information, refer to "Adding an IP device to discovery" on page 84.

Adding SNMPv1 and SNMPv2c credentials

If SNMPv1 or SNMPv2c is enabled, or if you want to use community strings to gain access to the device, define community strings.

To add a SNMPv1 or SNMPv2c read-write community string, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.

3. Click the **SNMP** tab.

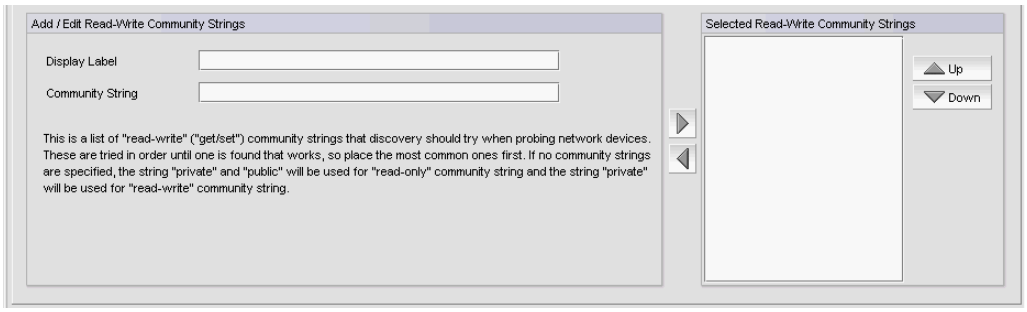


FIGURE 12 SNMPv1 or SNMPv2c credentials

4. Enter a unique label to identify the community string in the **Display Label** field of the **Add/Edit Read-Write Community Strings** list.

   This label can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

5. Enter the unique community string in the **Community Strings** field.

   The community string can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The string displays as asterisks.

6. Click the right arrow button to add the read-write community string to the **Selected Read-Write Community Strings** list.

   NOTE
   Discovery uses the read-write community string to detect both SNMP read and SNMP write community strings.

   If the devices use multiple community strings, use the **Up** or **Down** buttons to place the most commonly used community string at the top of the **Selected Read-Write Community Strings** list to make discovery run more efficiently.

   NOTE
   If the **Selected Read-Write Community Strings** list does not contain any community strings, the Management application uses the "public" and "private" community strings.

7. Click **Apply** to save your work.

8. Click **Close** to close the **Discover Setup - IP** dialog box.

9. Click **Yes** on the confirmation message.

Adding SNMPv3 credentials

To add SNMPv3 read-write credentials, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.

3. Click the **SNMP** tab.

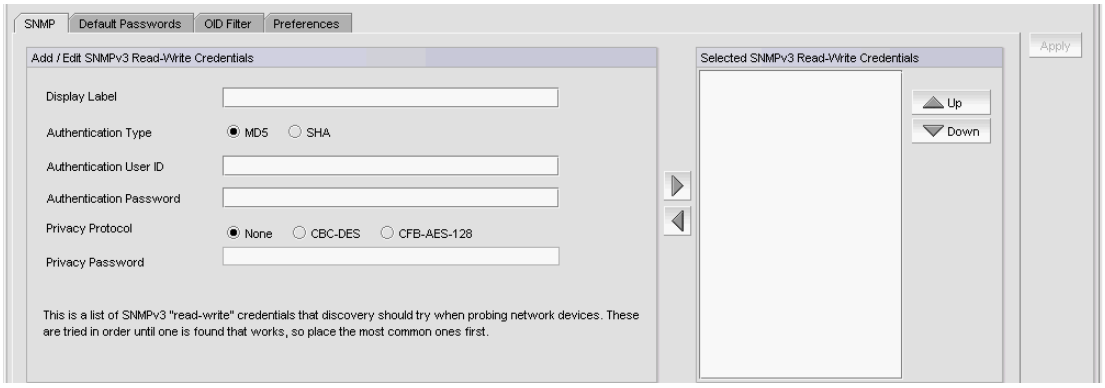


FIGURE 13 SNMPv3 credentials

4. Enter a unique label to identify the credentials in the **Display Label** field of the **Add/Edit SNMPv3 Read-Write Credentials** area.

   This label can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

5. Enter the SNMPv3 user name in the **User ID** field.

   The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

6. Select one of the following protocols from the **Authentication Protocol** list:

   - None
   - HMAC_MD5
   - HMAC_SHA

7. Enter the SNMPv3 authentication password in the **Authentication Password** field.

   The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password displays as asterisks.

8. Select one of the following protocols from the **Privacy Protocol** list:

   - None
   - CBC-DES
   - CFB_AES-128

   If you select a privacy protocol, the selected protocol encrypts the SNMP request and response packets.

9. Enter the privacy password in the **Privacy Password** field.

The password can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password displays as asterisks.

10. Click the right arrow button to add the SNMPv3 read-write credentials to the **Selected SNMPv3 Read-Write Credentials** list.

NOTE
If the devices use multiple credentials, use the **Up** or **Down** buttons to place the most commonly used credentials at the top of the **Selected SNMPv3 Read-Write Credentials** list to make discovery run more efficiently.

11. Click **Apply** to save your work.
12. Click **Close** to close the **Discover Setup - IP** dialog box.
13. Click **Yes** on the confirmation message.

Editing SNMPv1 and SNMPv2c credentials

To edit a SNMPv1 or SNMPv2c read-write community string, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.
3. Click the **SNMP** tab.
4. Select the community string you want to edit in the **Selected Read-Write Community Strings** list and click the left arrow button.

   The selected credentials display in the **Add/Edit Read-Write Community Strings** area.

5. Enter a unique label to identify the community string in the **Display Label** field the **Add/Edit Read-Write Community Strings** area.

   This label can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

6. Enter the unique community string in the **Community Strings** field.

   The community string can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The string displays as asterisks.

7. Click the right arrow button to add the read-write community string to the **Selected Read-Write Community Strings** list.

NOTE
If the devices use multiple community strings, use the **Up** or **Down** buttons to place the most commonly used community string at the top of the **Selected Read-Write Community Strings** list to make discovery run more efficiently.

NOTE
If the **Selected Read-Write Community Strings** list does not contain any community strings, the Management application uses the "public" and "private" community strings.

8. Click **Apply** to save your work.
9. Click **Close** to close the **Discover Setup - IP** dialog box.
10. Click **Yes** on the confirmation message.

Editing SNMPv3 credentials

To edit SNMPv3 read-write credentials, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Global Settings** tab.
3. Click the **SNMP** tab.
4. Select the SNMPv3 credentials you want to edit in the **Selected SNMPv3 Read-Write Credentials** list and click the left arrow button.

   The selected credentials display in the **Add/Edit SNMPv3 Read-Write Credentials** area.
5. Enter a unique label to identify the credentials in the **Display Label** field of the **Add/Edit SNMPv3 Read-Write Credentials** area.

   This label can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.
6. Enter the SNMPv3 user name in the **User ID** field.

   The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.
7. Select one of the following protocols from the **Authentication Protocol** list:
   - None
   - HMAC_MD5
   - HMAC_SHA
8. Enter the SNMPv3 authentication password in the **Authentication Password** field.

   The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.
9. Select one of the following protocols from the **Privacy Protocol** list:
   - None
   - CBC-DES
   - CFB_AES-128

   If you select a privacy protocol, the selected protocol encrypts the SNMP request and response packets.
10. Enter the privacy password in the **Privacy Password** field.

    The password can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.
11. Click the right arrow button to add the SNMPv3 read-write credentials to the **Selected SNMPv3 Read-Write Credentials** list.

NOTE
If the devices use multiple credentials, use the **Up** or **Down** buttons to place the most commonly used credentials at the top of the **Selected SNMPv3 Read-Write Credentials** list to make discovery run more efficiently.

12. Click **Apply** to save your work.
13. Click **Close** to close the **Discover Setup - IP** dialog box.
14. Click **Yes** on the confirmation message.

Reordering SNMP credentials in the list

Discovery probes the network for devices, according to the order in the list of SNMPv3 read-write credentials or SNMPv1 or SNMPv2c read-write community strings. Discovery uses the first item to find devices that are associated with those credentials or community strings, then continues down the list. Therefore, place the most commonly used credentials or community strings first.

To rearrange the SNMPv3 read-write credentials or SNMPv1 or SNMPv2c read-write community strings lists, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Global Settings** tab.
3. Click the **SNMP** tab.
4. Select an entry in the **Selected SNMPv3 Read-Write Credentials** or **Selected Read-Write Community Strings** list and use the **Up** and **Down** buttons to rearrange the entries.
5. Click **Apply** to save your work.
6. Click **Close** to close the **Discover Setup - IP** dialog box.
7. Click **Yes** on the confirmation message.

Deleting SNMP credentials from the list

To delete an entry from the SNMPv3 read-write credentials or SNMPv1 or SNMPv2c read-write community strings lists, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Global Settings** tab.
3. Click the **SNMP** tab.
4. Choose one of the following options:
   - Select the SNMPv3 read-write credentials you want to delete in the **Selected SNMPv3 Read-Write Credentials** list and click the left arrow button.
   - Select the SNMPv1 or SNMPv2c read-write community string you want to delete in the **Selected Read-Write Community Strings** list and click the left arrow button.
5. Click **Apply** to save your work.

6. Click **Close** to close the **Discover Setup - IP** dialog box.
7. Click **Yes** on the confirmation message.

Default IP user credentials

The Management application uses default user names and passwords to access devices when contacting these devices through the command line interface (CLI) on the network. You can enter a list of default names and passwords in the Management application before running discovery. Discovery uses this list to contact devices to determine the correct user name and password for the device. The first time discovery contacts a device, the Management application enters the default names and passwords for the device into the Management application database. This feature saves you the trouble of entering authentication passwords for every newly discovered device.

NOTE
Discovery does not remove an invalid user name or password from the device information unless it is able to replace it with a valid one.

The Management application groups default user names and passwords by the following password types:

- **Read/Write Login Prompt** — The login prompt the device uses when logging in by Telnet or CLI to the device.
- **Read/Write Enable Prompt** — The enable prompt the device uses in CLI mode to go to device enable mode.
- **Enable Super User** — The super user enable password configured on the device for Telnet login. You can configure the super user enable password by using the **enable super-user-password** CLI command. The super user enable password can be used to authenticate users with the super user privilege configured on the device.

You can define more than one password for each password type. Discovery uses the passwords in the order they are listed when it probes the devices.

Adding user credentials

To add default user names and passwords, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Global Settings** tab.
3. Click the **Default Passwords** tab.

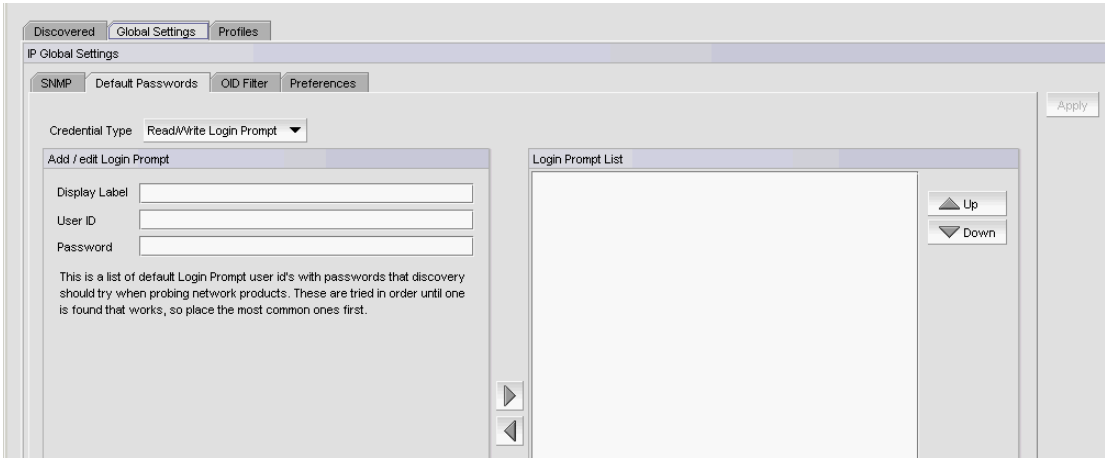


FIGURE 14 Default Passwords

4. Enter a login prompt user name and password by selecting **Read/Write Login Prompt** from the **Credential Type** list and completing the following steps.

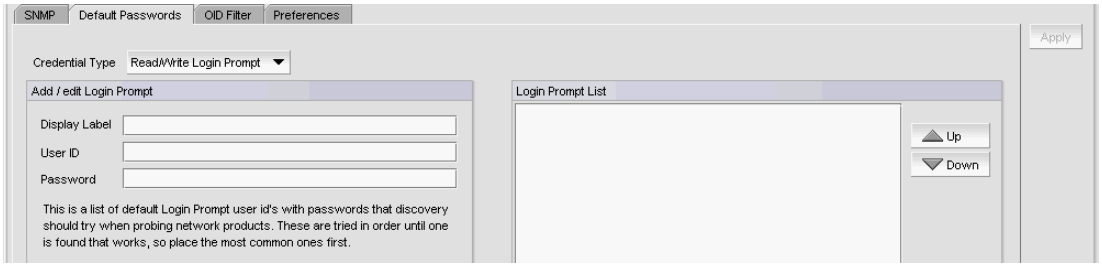


FIGURE 15 Read/Write Login Prompt

a. Enter a unique label to identify the credentials in the **Display Label** field.

   This label can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters.

b. Enter the user name in the **User ID** field.

c. Enter the user password in the **Password** field.

d. Click the right arrow button.

e. If the devices use multiple user names and passwords, use the **Up** or **Down** buttons to place the most commonly used at the top of the **Login Prompt** list to make discovery run more efficiently.

5. Enter an enable prompt user name and password by selecting **Read/Write Enable Prompt** from the **Credential Type** list and completing the following steps.

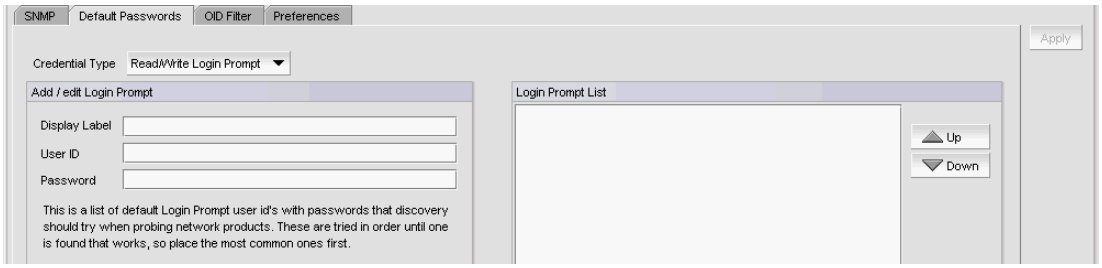


FIGURE 16 Read/Write Enable Prompt

   a. Enter a unique label to identify the credentials in the **Display Label** field.

      This label can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters.

   b. Enter the user name in the **User ID** field.

   c. Enter the user password in the **Password** field.

   d. Click the right arrow button.

   e. If the devices use multiple user names and passwords, use the **Up** or **Down** buttons to place the most commonly used at the top of the **Enable Prompt** list to make discovery run more efficiently.

6. Enter a super user password by selecting **Enable Super User** from the **Credential Type** list and completing the following steps.

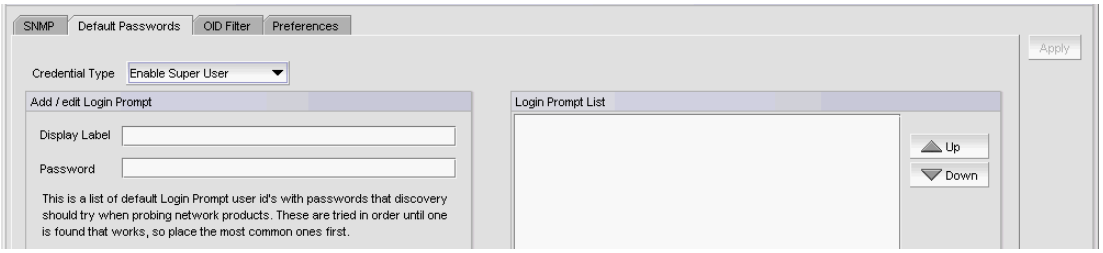


FIGURE 17 Enable Super User

   a. Enter a unique label to identify the credentials in the **Display Label** field.

      This label can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters.

   b. Enter the super user password in the **Password** field.

   c. Click the right arrow button.

   d. If the devices use multiple user names and passwords, use the **Up** or **Down** buttons to place the most commonly used at the top of the **Enable Super User** list to make discovery run more efficiently.

7. Click **Apply** to save your work.

8. Click **Close** to close the **Discover Setup - IP** dialog box.
9. Click **Yes** on the confirmation message.

Editing login prompt user credentials

To edit a login prompt user name and password, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Global Settings** tab.
3. Click the **Default Passwords** tab.
4. Select **Read/Write Login Prompt** from the **Credential Type** list.
5. Select the user credential entry you want to edit in the **Login Prompt List** and click the left arrow button.

   The selected credentials display in the **Add/edit Login Prompt** area.
6. Edit the unique label to identify the credentials in the **Display Label** field.

   This label can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters.
7. Edit the user name in the **User ID** field.
8. Edit the user password in the **Password** field.
9. Click the right arrow button.
10. If the devices use multiple user names and passwords, use the **Up** or **Down** buttons to place the most commonly used at the top of the **Login Prompt List** to make discovery run more efficiently.
11. Click **Apply** to save your work.
12. Click **Close** to close the **Discover Setup - IP** dialog box.
13. Click **Yes** on the confirmation message.

Editing enable prompt user credentials

To edit an enable prompt user name and password, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Global Settings** tab.
3. Click the **Default Passwords** tab.
4. Select **Read/Write Enable Prompt** from the **Credential Type** list.
5. Select the user credential entry you want to edit in the **Login Prompt List** and click the left arrow button.

   The selected credentials display in the **Add/edit Login Prompt** area.

6. Edit the unique label to identify the credentials in the **Display Label** field.

   This label can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters.

7. Edit the user name in the **User ID** field.
8. Edit the user password in the **Password** field.
9. Click the right arrow button.
10. If the devices use multiple user names and passwords, use the **Up** or **Down** buttons to place the most commonly used at the top of the **Login Prompt List** to make discovery run more efficiently.
11. Click **Apply** to save your work.
12. Click **Close** to close the **Discover Setup - IP** dialog box.
13. Click **Yes** on the confirmation message.

Editing enable super user credentials

To edit an enable super user, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.
3. Click the **Default Passwords** tab.
4. Select **Enable Super User** from the **Credential Type** list.
5. Select the user credential entry you want to edit in the **Login Prompt List** and click the left arrow button.

   The selected credentials display in the **Add/edit Login Prompt** area.

6. Edit the unique label to identify the credentials in the **Display Label** field.

   This label can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters.

7. Edit the super user password in the **Password** field.
8. Click the right arrow button.
9. If the devices use multiple user names and passwords, use the **Up** or **Down** buttons to place the most commonly used at the top of the **Login Prompt List** to make discovery run more efficiently.
10. Click **Apply** to save your work.
11. Click **Close** to close the **Discover Setup - IP** dialog box.
12. Click **Yes** on the confirmation message.

Reordering user credentials in the list

Discovery tries the user credentials in order until one set of credentials is found that works, so place the most common ones first.

To rearrange the user credentials, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Global Settings** tab.
3. Click the **Default Passwords** tab.
4. Select one of the following password types from the **Credential Type** list:
   - Read/Write Login Prompt
   - Read/Write Enable Prompt
   - Enable Super User
5. Select an entry in the **Login Prompt List** and use the **Up** and **Down** buttons to rearrange the entries.
6. Click **Apply** to save your work.
7. Click **Close** to close the **Discover Setup - IP** dialog box.
8. Click **Yes** on the confirmation message.

Deleting user credentials from the list

To delete an entry from the SNMPv3 read-write credentials or SNMPv1 or SNMPv2c read-write community strings lists, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Global Settings** tab.
3. Click the **Default Passwords** tab.
4. Select one of the following password types from the **Credential Type** list:
   - Read/Write Login Prompt
   - Read/Write Enable Prompt
   - Enable Super User
5. Select an entry in the **Login Prompt List** and click the left arrow button.
6. Click **Apply** to save your work.
7. Click **Close** to close the **Discover Setup - IP** dialog box.
8. Click **Yes** on the confirmation message.

IP Object identifier filters

The object identifier (OID) filter allows you to select which product types to include or exclude from discovery.

If you add a third-party product OID to the **Included Product Types** list during discovery and later move it to the **Excluded Product Types** list, note that you will not be able to discover a new device with that product OID. However, other functionality such as traps, fault management, statistics, performance data collection, product polling for health monitoring and so on continue to run as with any other discovered product.

Including product types

To include third-party product types in discovery, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.
3. Click the **OID Filter** tab.

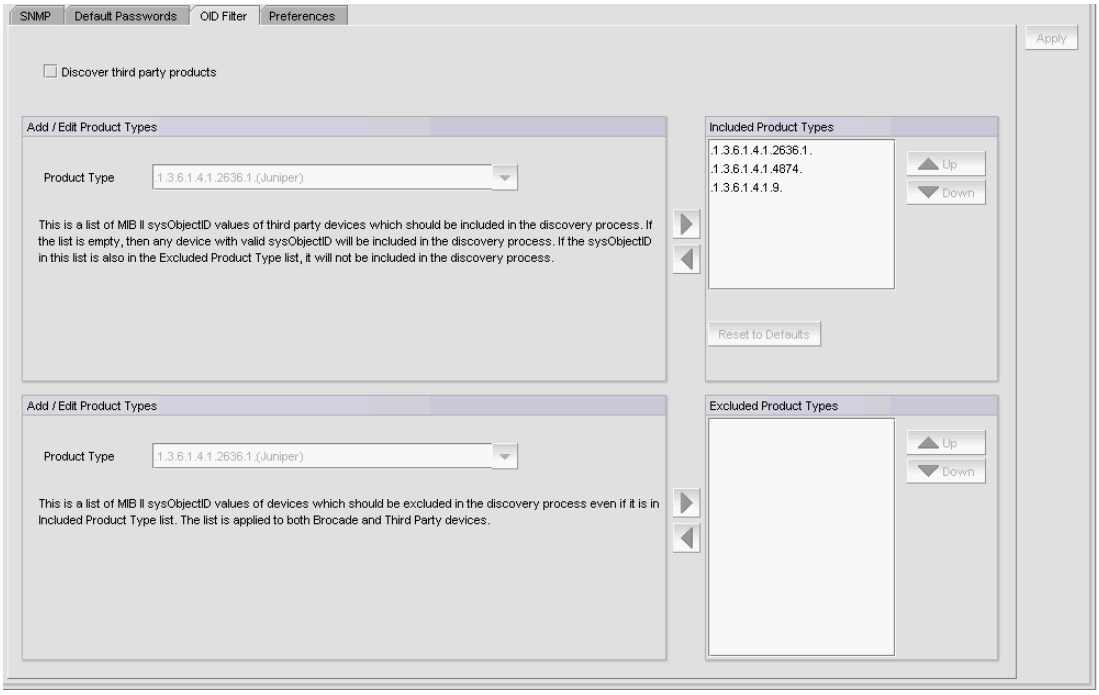


FIGURE 18 OID Filter tab

4. Select the **Discover third party products** check box to include third-party devices in discovery.

5. In the top **Add/Edit Product Types** area, choose one of the following options:
   - Enter the device's sysObjectID you want to include in the **Product Type** list.
   - Select an existing device sysObjectID from the **Product Type** list.

     Table 13 lists the default third party product types.

TABLE 13 Default third-party product types

Product sysObjectID	Vendor
.1.3.6.1.4.1.9.	Cisco
.1.3.6.1.4.1.4874.	Juniper
.1.3.6.1.4.1.2636.1.	Juniper

6. Click the right arrow button to add the product type to the **Included Product Types** list.

   The **Included Product Types** list displays the third-party device sysObjectIDs to include in discovery. If this list is empty, discovery includes any device with a valid sysObjectID. If a sysObjectID in this list is also in the **Excluded Product Types** list, discovery excludes it.
7. Click **Apply** to save your work.
8. Click **Close** to close the **Discover Setup - IP** dialog box.
9. Click **Yes** on the confirmation message.

Excluding product types

To exclude third-party product types from discovery, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Global Settings** tab.
3. Click the **OID Filter** tab.
4. In the bottom **Add/Edit Product Types** area, choose one of the following options:
   - Enter the device's sysObjectID you want to include in the **Product Type** list.
   - Select an existing device sysObjectID from the **Product Type** list.

     Table 13 lists the default third party product types.
5. Click the right arrow button to add the product type to the **Excluded Product Types** list.

   The **Excluded Product Types** list displays the third-party device sysObjectiDs to exclude from discovery. If a sysObjectID in this list is also in the **Included Product Types** list, discovery excludes it.
6. Click **Apply** to save your work.
7. Click **Close** to close the **Discover Setup - IP** dialog box.
8. Click **Yes** on the confirmation message.

Deleting product types from the list

To delete an entry from the **Included Product Types** or **Excluded Product Type** list, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.
3. Click the **OID Filter** tab.
4. Select an entry from the **Included Product Types** or **Excluded Product Type** list and click the left arrow button.
5. Click **Apply** to save your work.
6. Click **Close** to close the **Discover Setup - IP** dialog box.
7. Click **Yes** on the confirmation message.

Defining global setting preferences

To define global setting preferences, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.
3. Click the **Preferences** tab.

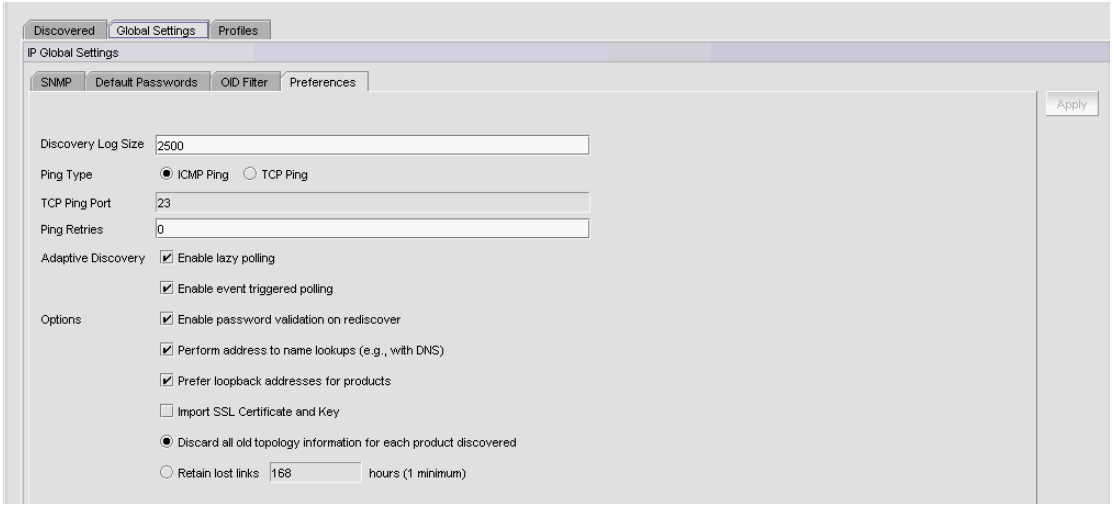


FIGURE 19 Preferences tab

4. Enter a value (from 32 through 10000) for the number of live discovery log messages to store on the server in the **Discovery Log Size** field.

   The default is 2500.

5. Select one of the following **Ping Type** options:
   - **ICMP Ping** (default). Go to step 7.
   - **TCP Ping**. Continue with step 6.
6. Enter the TCP port number (from 1 through 65536) in the **TCP Ping Port** field.

   The default is 23.
7. Enter the number of times (from 0 through 10) to ping the device when ping is unsuccessful in the **Ping Retries** field.

   The default is 0.
8. Select the **Enable lazy polling** check box to periodically rediscover all devices in the database.

   NOTE
   This setting cannot be disabled for DCB switches.

   The lazy polling function sends login and log messages to the Master Log and the switch console. If you are receiving too many messages due to lazy polling, clear the check box to disable off lazy polling.

   You cannot change the lazy polling interval for IronWare OS or Network OS devices. The lazy polling interval is based on the size of your network. For IronWare OS devices, default values are as follows:
   - Small: 2 minutes
   - Medium: 15 minutes
   - Large: 30 minutes

   For Network OS devices, default values are as follows:
   - Small: 15 minutes
   - Medium: 30 minutes
   - Large: 60 minutes
9. Select the **Enable event triggered polling** check box to enable adaptive discovery on the predefined SNMP traps.

   NOTE
   This setting cannot be disabled for DCB switches.

   NOTE
   Network OS devices must be running version 4.0 or later to enable this setting.

   NOTE
   For Network OS devices, adaptive discovery is also performed for Syslog events.
10. Select the **Enable password validation on rediscover** check box to enable CLI user credential validation when rediscovering devices.
11. Select the **Perform address to name lookups (e.g. with DNS)** check box to configure discovery to use the local DNS server for address-to-name resolution.
12. Select the **Prefer loopback addresses for products** check box to enable discovery to choose an IP address associated with a router loopback interface to be the router primary IP address.

Clear the check box to configure discovery to select the original IP address used to discover the device.

13. Select the **Import SSL Certificate and Key** check box to enable discovery to download and synchronize certificates from SSL capable Application products.
14. Choose one of the following options:
    - Select the **Discard all old topology information for each product discovered** option to delete all existing device topology data when running discovery.
    - Select the **Retain lost links __ hours (1 minimum)** option to configure how long to retain lost links on the topology maps and enter a value (from 1 through 9999) in the field. The default is 168 hours.
15. Click **Apply** to save your work.
16. Click **Close** to close the **Discover Setup - IP** dialog box.
17. Click **Yes** on the confirmation message.

Configuring event-based collection

If you discover more than 550 IP products, the Management application automatically turns off event-based collection. To restart event-based collection, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

   The **Discover Setup - IP** dialog box displays.
2. Reduce the managed count by completing the following steps.
   a. Select the IP devices you want to remove from discovery in the **Discovered Products** table.

      Select multiple devices by holding down the CTRL key and clicking more than one device.

      NOTE
      You cannot delete an active member from a VCS fabric.

   b. Click **Delete**.
3. Turn on event-based collection by completing the following steps.
   a. Click the **Global Settings** tab.
   b. Click the **Preferences** tab.
   c. Select the **Enable lazy polling** check box to periodically rediscover all devices in the database.

      NOTE
      This settings cannot be disabled for DCB switches.

   d. Select the **Enable event triggered polling** check box to enable adaptive discovery on the predefined SNMP traps.

NOTE
This settings cannot be disabled for DCB switches.

NOTE
Network OS devices must be running version 4.0 or later to enable this setting.

NOTE
For Network OS devices, adaptive discovery is also performed for Syslog events.

The lazy polling function sends login and log messages to the Master Log and the switch console. If you are receiving too many messages due to lazy polling, clear the check box to disable off lazy polling.

You cannot change the lazy polling interval for IronWare OS or Network OS devices. The lazy polling interval is based on the size of your network. For IronWare OS devices, default values are as follows:

- Small: 2 minutes
- Medium: 15 minutes
- Large: 30 minutes

For Network OS devices, default values are as follows:

- Small: 15 minutes
- Medium: 30 minutes
- Large: 60 minutes

e. Click **Apply** to save your work.

4. Click **Close** to close the **Discover Setup - IP** dialog box.
5. Click **Yes** on the confirmation message.

IP discovery profiles

NOTE
You cannot configure a discovery profile if you do not have the **All IP Products** AOR (area of responsibility) in your user account.

A discovery profile contains the settings you configure when discovery is run. These settings include address range parameters, ping sweep parameters, SNMP settings, default passwords, and other settings. The Management application is shipped with a default discovery profile named "Default". You can create more than one discovery profile. You can select one discovery profile to run automatically at startup. After startup, one or more profiles can be run consecutively.

Configuring a discovery profile

NOTE
You cannot configure a discovery profile if you do not have the **All IP Products** AOR (area of responsibility) in your user account.

To configure a discovery profile, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab

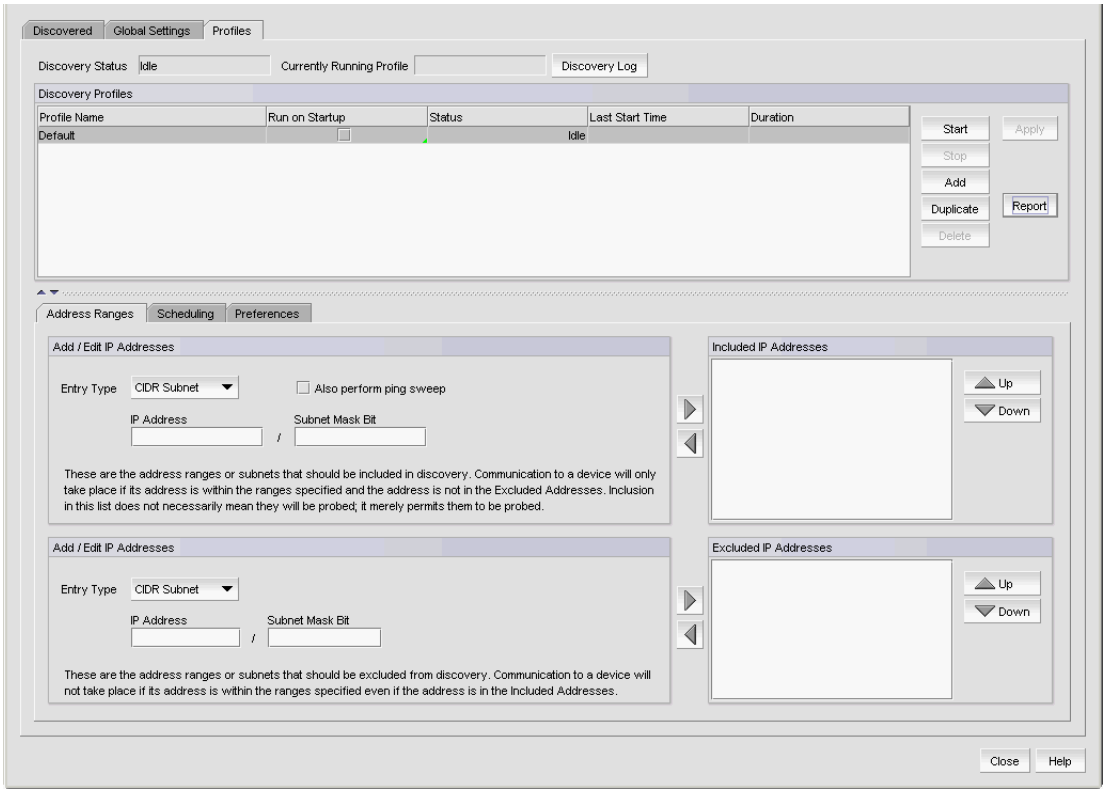


FIGURE 20 Profile tab

3. Click **Add**.

   A new row (named “new_profile”) displays in the **Discovery Profiles** table.

4. Click “new_profile” in the **Profile Name** field to enter a unique name for the profile.

   This name can be from 1 through 255 characters long, case sensitive, and allows all printable ASCII characters.

5. Click the **Address Ranges** tab to configure address ranges for the profile.

   For step-by-step instructions, refer to “Configuring address ranges” on page 66.

6. Click the **Scheduling** tab to configure a discovery schedule for the profile.

   For step-by-step instructions, refer to “Scheduling discovery” on page 72.

7. Click the **Preferences** tab to configure preferences for the profile.

   For step-by-step instructions, refer to “Configuring advanced discovery profile preferences” on page 78.

8. Click the **Global Settings** tab.

   To set SNMP credentials, refer to “IP SNMP credentials” on page 46.

   To configure default user names and passwords, refer to “Default IP user credentials” on page 52.

   To configure global setting preferences, refer to “Defining global setting preferences” on page 60.

9. Click **Apply** to save your changes.

10. Click **Close** to close the **Discover Setup - IP** dialog box.

11. Click **Yes** on the confirmation message.

Duplicating a discovery profile

NOTE
You cannot duplicate a discovery profile if you do not have the **All IP Products** AOR (area of responsibility) in your user account.

To duplicate a discovery profile, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab

3. Select the profile you want to copy and click **Duplicate**.

   A new row (named “Copy of *profile_name*”) displays in the **Discovery Profiles** table

4. Click “Copy of *profile_name*” in the **Profile Name** field to enter a unique name for the profile.

   This name can be from 1 through 255 characters long, case sensitive, and allows all printable ASCII characters.

5. Click the **Address Ranges** tab to configure address ranges for the profile.

For step-by-step instructions, refer to "Configuring address ranges" on page 66 or "Editing address ranges" on page 70.

6. Click the **Scheduling** tab to configure a discovery schedule for the profile.

   For step-by-step instructions, refer to "Scheduling discovery" on page 72.

7. Click the **Preferences** tab to configure preferences for the profile.

   For step-by-step instructions, refer to "Configuring advanced discovery profile preferences" on page 78.

8. Click the **Global Settings** tab.

   To set SNMP credentials, refer to "IP SNMP credentials" on page 46.

   To configure default user names and passwords, refer to "Default IP user credentials" on page 52.

   To configure global setting preferences, refer to "Defining global setting preferences" on page 60.

9. Click **Apply** to save your changes.
10. Click **Close** to close the **Discover Setup - IP** dialog box.
11. Click **Yes** on the confirmation message.

Configuring address ranges

To include and exclude addresses from profile discovery, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab
3. Select the profile you want to edit in the **Discovery Profiles** table and click the **Address Ranges** tab.
4. Include an address range by choosing one of the following options:
   - To include an address range using the CIDR subnet format, refer to "Adding CIDR subnet addresses" on page 67.
   - To include an address range using the subnet format, refer to "Adding subnet addresses" on page 68.
   - To include an address range using the address range format, refer to "Adding IP addresses" on page 68.
   - **To include all addresses, sele**ct all addresses fr**om the Entry Type list.**
5. Select the **Also perform ping sweep** check box to perform ping sweep on the address range.
6. Click the right arrow button to add the address range to the **Included IP Addresses** list.
7. Exclude an address range by choosing one of the following options:
   - To exclude an address range using the CIDR subnet format, refer to "Excluding CIDR subnet addresses" on page 69.
   - To exclude an address range using the subnet format, refer to "Excluding subnet addresses" on page 69.

- To exclude an address range using the address range format, refer to "Excluding IP addresses" on page 70.

NOTE
To exclude a VCS fabric, you must add all members of the VCS fabric to the exclude list.

8. Click the right arrow button to add the address range to the **Excluded IP Addresses** list.
9. Click **Apply** to save your changes.
10. Click **Close** to close the **Discover Setup - IP** dialog box.
11. Click **Yes** on the confirmation message.

Adding CIDR subnet addresses

To add CIDR subnet addresses (IPv4 and IPv6), complete the following steps.

1. Select **CIDR Subnet** from the **Entry Type** list.

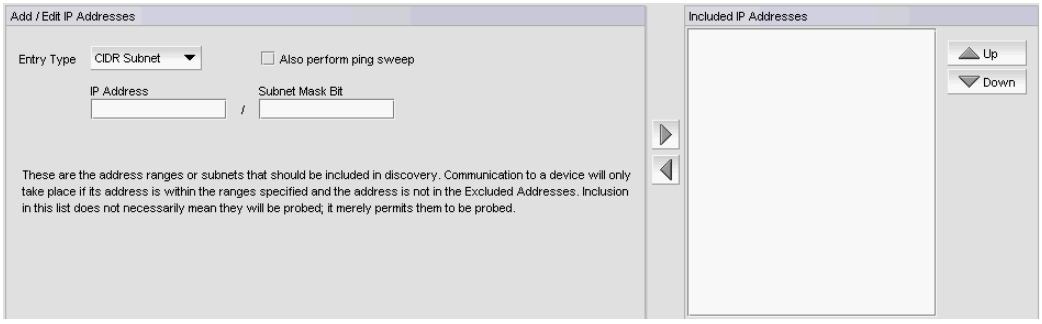


FIGURE 21 Include CIDR Subnet

2. Enter the IP address in the **IP Address** field.
3. Enter the number of subnet mask bits in the **Subnet Mask Bits** field.

   For IPv4, the number of subnet mask bits is from 0 through 32.

   For IPv6, the number of subnet mask bits is from 0 through128.
4. **To exclude** an address range **using the CIDR Subnet format, refer to** **"Excluding CIDR subnet addresses" on page 69****.**
5. To finish configuring the address ranges, return to **"Configuring address ranges" on page 66****.**

Adding subnet addresses

To add subnet addresses (IPv4 only), complete the following steps.

1. Select **Subnet** from the **Entry Type** list.

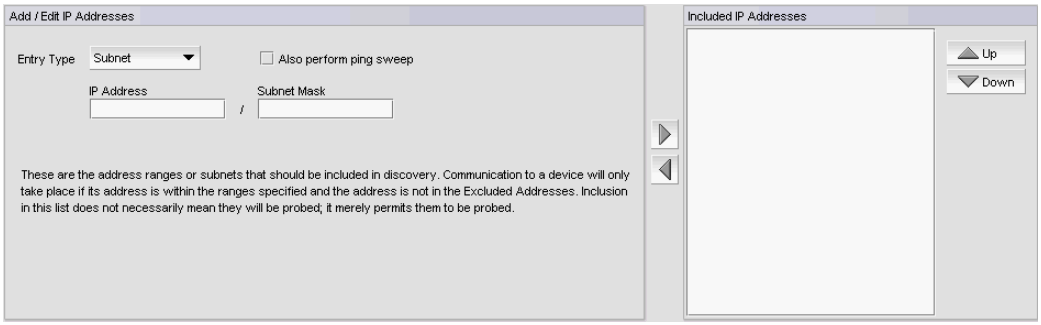


FIGURE 22 Include Subnet

2. Enter the IP address in the **IP Address** field.
3. Enter the subnet mask in the **Subnet Mask** field.
4. **To exclude** an address range **using the Subnet format, refer to** **"Excluding subnet addresses"** on page 69**.**
5. To finish configuring the address ranges, return to **"Configuring address ranges"** on page 66**.**

Adding IP addresses

To add an IP address range (IPv4 and IPv6), complete the following steps.

1. Select **IP Address** from the **Entry Type** list.

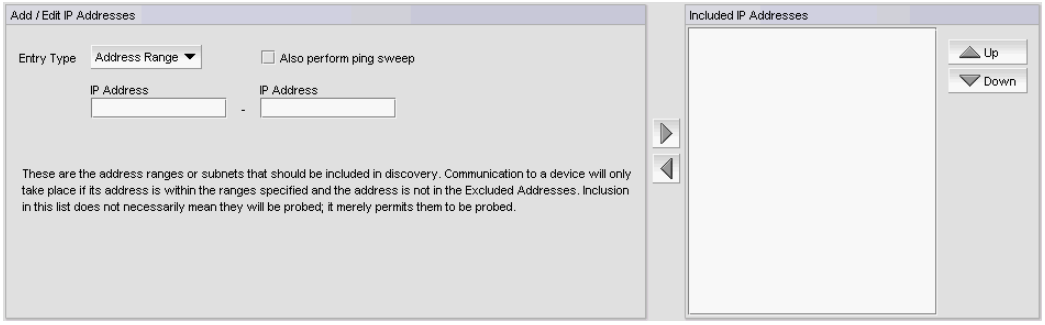


FIGURE 23 Include Address Range

2. Enter the first IP address in the range in the first **IP Address** field.
3. Enter the last IP address in the range in the second **IP Address** field.
4. **To exclude** an address range **using the IP Address format, refer to** **"Excluding IP addresses"** on page 70**.**
5. To finish configuring the address ranges, return to **"Configuring address ranges"** on page 66**.**

Excluding CIDR subnet addresses

To exclude CIDR subnet addresses (IPv4 and IPv6), complete the following steps.

1. Select **CIDR Subnet** from the **Entry Type** list.

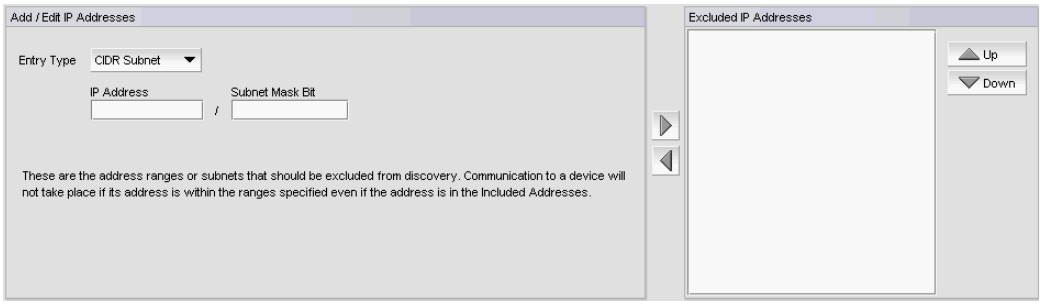


FIGURE 24 Exclude CIDR Subnet

2. Enter the IP address in the **IP Address** field.
3. Enter the subnet mask bits in the **Subnet Mask Bits** field.

   For IPv4, the subnet mask bits is between 0 and 32.

   For IPv6, the subnet mask bits is between 0 and 128.
4. **To include** an address range **using the CIDR Subnet format, refer to** **"Adding CIDR subnet addresses"** on page 67**.**
5. To finish configuring the address ranges, return to **"Configuring address ranges"** on page 66**.**

Excluding subnet addresses

To exclude subnet addresses (IPv4 only), complete the following steps.

1. Select **Subnet** from the Entry Type list.

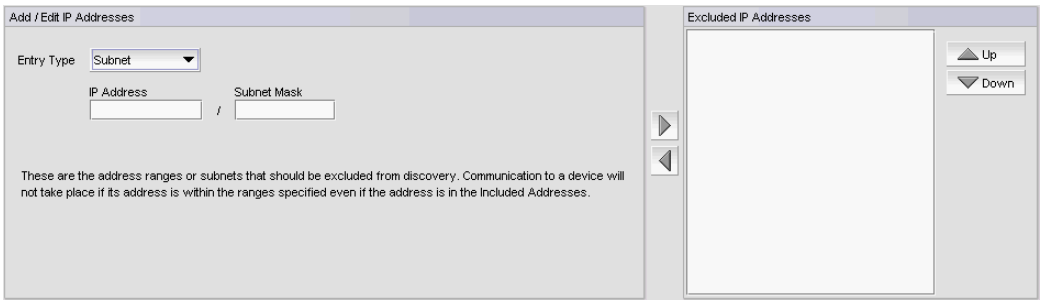


FIGURE 25 Exclude Subnet

2. Enter the IP address in the **IP Address** field.
3. Enter the subnet mask in the **Subnet Mask** field.
4. **To include** an address range **using the Subnet format, refer to** **"Adding subnet addresses"** on page 68**.**
5. To finish configuring the address ranges, return to **"Configuring address ranges"** on page 66**.**

Excluding IP addresses

NOTE
To exclude a VCS fabric, you must add all members of the VCS fabric to the exclude list.

To exclude an IP address range (IPv4 and IPv6), complete the following steps.

1. Select **IP Address** from the **Entry Type** list.

FIGURE 26 Exclude Address Range

2. Enter the first IP address in the range in the first **IP Address** field.
3. Enter the last IP address in the range in the second **IP Address** field.
4. **To include** an address range **using the Address Range format, refer to** **"Adding IP addresses"** on page 68**.**
5. To finish configuring the address ranges, return to **"Configuring address ranges"** on page 66**.**

Editing address ranges

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Profiles** tab
3. Select the profile you want to edit in the **Discovery Profiles** table and click the **Address Ranges** tab.
4. To edit an included address range, select the address range you want to edit in the **Included IP Addresses** list.
5. Click the left arrow button to display the address range details in the top **Add/Edit IP Addresses** area.
6. Edit the included address range by choosing one of the following options:
   - To edit the included addresses using the CIDR subnet format, refer to "Editing CIDR subnet addresses" on page 71.
   - To edit the included addresses using the subnet format, refer to "Editing subnet addresses" on page 71.
   - To edit the included addresses using the address range format, refer to "Editing IP addresses" on page 71.
7. Select the **Also perform ping sweep check** box to perform ping sweep on the address range.

8. To edit an excluded address range, select the address range you want to edit in the **Excluded IP Addresses** list.
9. Click the left arrow button to display the address range details in the bottom **Add/Edit IP Addresses** area.
10. Edit the excluded address range by choosing one of the following options:
    - To edit the excluded addresses using the CIDR subnet format, refer to "Editing CIDR subnet addresses" on page 71.
    - To edit the excluded addresses using the subnet format, refer to "Editing subnet addresses" on page 71.
    - To edit the excluded addresses using the address range format, refer to "Editing IP addresses" on page 71.
11. Click the right arrow button to add the address range to the **Excluded IP Addresses** list.
12. Click **Apply** to save your changes.
13. Click **Close** to close the **Discover Setup - IP** dialog box.
14. Click **Yes** on the confirmation message.

Editing CIDR subnet addresses

To edit the CIDR subnet address (IPv4 and IPv6) range, complete the following steps.

1. Change the IP address in the **IP Address** field.
2. Change the number of subnet mask bits in the **Subnet Mask Bits** field.

   For IPv4, the number of subnet mask bits is from 0 through 32.

   For IPv6, the number of subnet mask bits is from 0 through 128.
3. To finish editing the address ranges, return to **"Editing address ranges"** on page 70.

Editing subnet addresses

To edit the subnet address (IPv4 only) range, complete the following steps.

1. Change the IP address in the **IP Address** field.
2. Change the subnet mask in the **Subnet Mask** field.
3. To finish editing the address ranges, return to **"Editing address ranges"** on page 70.

Editing IP addresses

To edit the IP address range (IPv4 and IPv6), complete the following steps.

1. Change the first IP address in the range in the first **IP Address** field.
2. Change the last IP address in the range in the second **IP Address** field.
3. To finish editing the address ranges, return to **"Editing address ranges"** on page 70.

Scheduling discovery

You can create multiple schedules (to a maximum of 32) for each profile. When it is time for a schedule to run, discovery handles schedules in the following manner:

- If discovery is already running for the profile, the scheduled discovery drops.
- If discovery is already running for a different profile, the scheduled discovery is queued. Once all discovery jobs in the queue finish, the scheduled discovery runs.
- If no discovery is running, the scheduled discovery starts.

To schedule a discovery profile, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab
3. Select the profile you want to edit in the **Discovery Profiles** table and click the **Scheduling** tab.

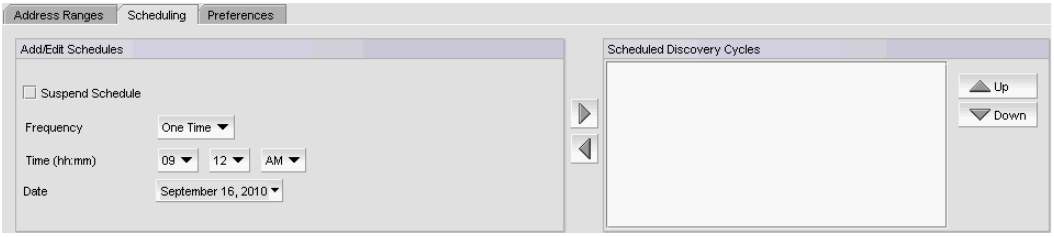


FIGURE 27 Scheduling tab

4. Choose one of the following options to configure the frequency at which discovery runs for the profile:
   - To configure discovery to run only once, refer to "Configuring a one-time discovery schedule" on page 73.
   - To configure hourly discovery, refer to "Configuring an hourly discovery schedule" on page 73.
   - To configure daily discovery, refer to "Configuring a daily discovery schedule" on page 74.
   - To configure weekly discovery, refer to "Configuring a weekly discovery schedule" on page 74.
   - To configure monthly discovery, refer to "Configuring a monthly discovery schedule" on page 75.
   - To configure yearly discovery, refer to "Configuring a yearly discovery schedule" on page 75.
5. Rearrange schedules in the **Scheduled Discovery Cycles** list by selecting an item in the list and clicking the **Up** or **Down** buttons to move it.
6. Click **Apply** to save your changes.
7. Click **Close** to close the **Discover Setup - IP** dialog box.
8. Click **Yes** on the confirmation message.

Configuring a one-time discovery schedule

To configure a one-time discovery schedule, complete the following steps.

1. Select **One Time** from the **Frequency** list.

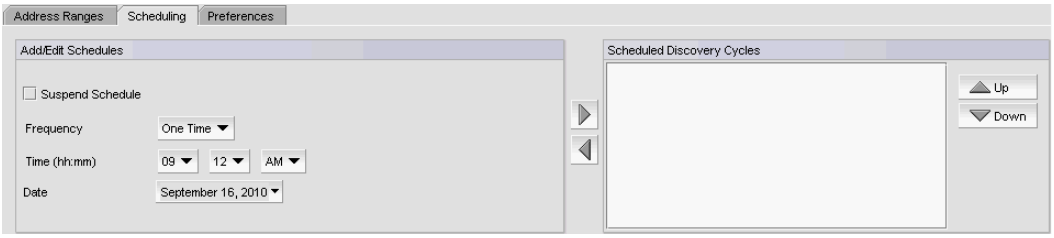


FIGURE 28 Scheduling tab - One Time

2. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Click the **Date** list to select a date from the calendar.
4. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
5. To finish configuring the discovery schedule, return to "Scheduling discovery" on page 72.

Configuring an hourly discovery schedule

To configure an hourly discovery schedule, complete the following steps.

1. Select **Hourly** from the **Frequency** list.

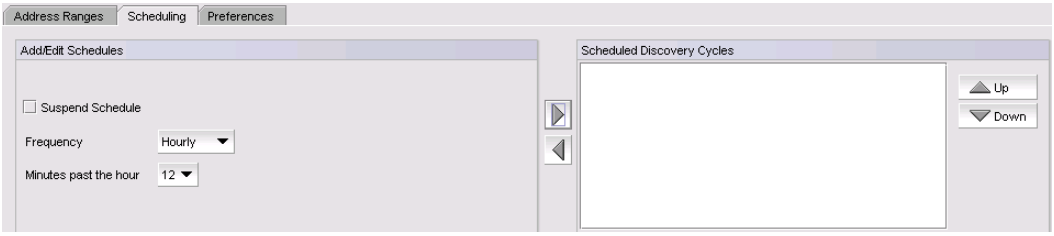


FIGURE 29 Scheduling tab - Hourly

2. Select the minute past the hour you want discovery to run from the **Minutes past the hour** list.

   Where the minute value is from 00 through 59.

3. To finish configuring the discovery schedule, return to "Scheduling discovery" on page 72.

Configuring a daily discovery schedule

To configure a daily discovery schedule, complete the following steps.

1. Select **Daily** from the **Frequency** list.

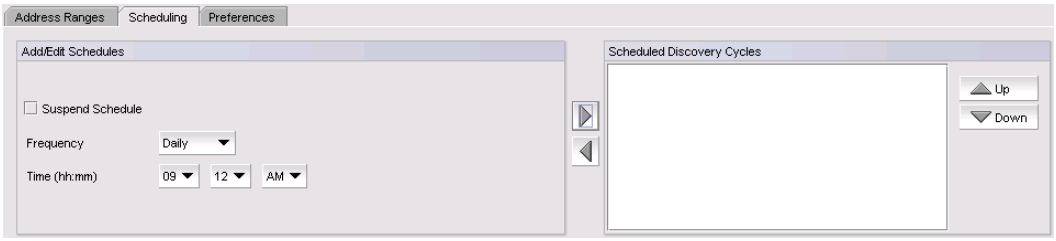


FIGURE 30 Scheduling tab - Daily

2. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
4. To finish configuring the discovery schedule, return to "Scheduling discovery" on page 72.

Configuring a weekly discovery schedule

To configure a weekly discovery schedule, complete the following steps.

1. Select **Weekly** from the **Frequency** list.

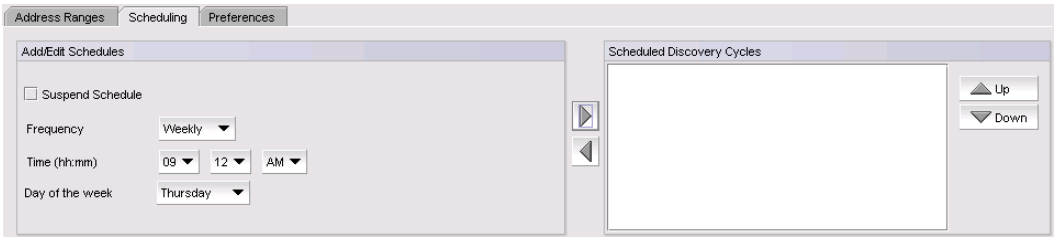


FIGURE 31 Scheduling tab - Weekly

2. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Select the day you want discovery to run from the **Day of the Week** list.
4. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
5. To finish configuring the discovery schedule, return to "Scheduling discovery" on page 72.

Configuring a monthly discovery schedule

To configure a monthly discovery schedule, complete the following steps.

1. Select **Monthly** from the **Frequency** list.

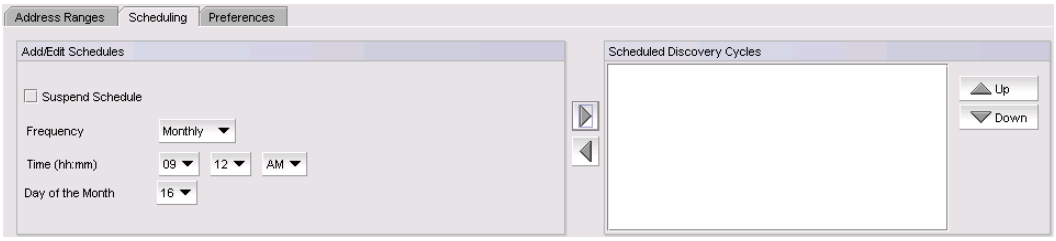


FIGURE 32 Scheduling tab - Monthly

2. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Select the day you want discovery to run from the **Day of the Month** list (1 through 31).
4. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
5. To finish configuring the discovery schedule, return to "Scheduling discovery" on page 72.

Configuring a yearly discovery schedule

To configure a yearly discovery schedule, complete the following steps.

1. Select **Yearly** from the **Frequency** list.

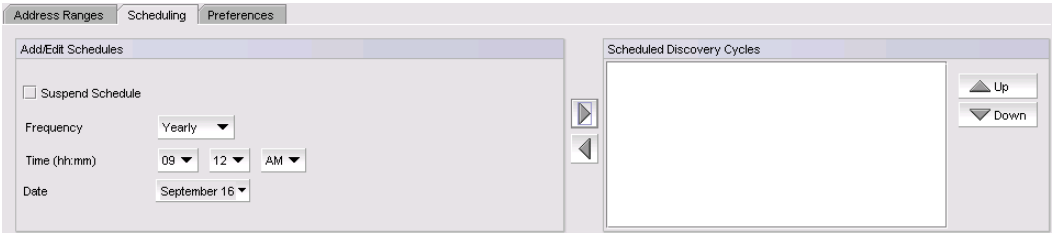


FIGURE 33 Scheduling tab - Yearly

2. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Click the **Date** list to select a date from the calendar.
4. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
5. To finish configuring the discovery schedule, return to "Scheduling discovery" on page 72.

Suspending a discovery schedule

To suspend a discovery profile schedule, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab
3. Select the profile for which you want to suspend a discovery schedule in the **Discovery Profiles** table and click the **Scheduling** tab.
4. Select the schedule you want to suspend in the **Scheduled Discovery Cycles** list and click the left arrow button.
5. Click the Suspend check box and click the right arrow button to return the schedule to the **Scheduled Discovery Cycles** list.

   The suspended schedule displays at the bottom of the **Scheduled Discovery Cycles** list.

6. Click **Apply** to save your changes.
7. Click **Close** to close the **Discover Setup - IP** dialog box.
8. Click **Yes** on the confirmation message.

Editing a discovery schedule

To edit a discovery schedule, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab
3. Select the profile you want to edit in the **Discovery Profiles** table and click the **Scheduling** tab.
4. Select the schedule you want to edit from the **Scheduled Discovery Cycles** list.
5. Click the left arrow button to display the schedule in the **Add/Edit Schedules** area.
6. Choose one of the following options to change the discovery schedule:
   - To edit the one-time discovery schedule, refer to "Editing a one-time discovery schedule" on page 77.
   - To edit the hourly discovery schedule, refer to "Editing an hourly discovery schedule" on page 77.
   - To edit the daily discovery schedule, refer to "Editing a daily discovery schedule" on page 77.
   - To edit the weekly discovery schedule, refer to "Editing a weekly discovery schedule" on page 77.
   - To edit the monthly discovery schedule, refer to "Editing a monthly discovery schedule" on page 78.
   - To edit the yearly discovery schedule, refer to "Editing a yearly discovery schedule" on page 78.

7. Rearrange schedules in the **Scheduled Discovery Cycles** list by selecting an item in the list and clicking the **Up** or **Down** buttons to move it.
8. Click **Apply** to save your changes.
9. Click **Close** to close the **Discover Setup - IP** dialog box.
10. Click **Yes** on the confirmation message.

Editing a one-time discovery schedule

To edit a one-time discovery schedule, complete the following steps.

1. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
2. Click the **Date** list to select a date from the calendar.
3. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
4. To finish editing the discovery schedule, return to "Editing a discovery schedule" on page 76.

Editing an hourly discovery schedule

To edit an hourly discovery schedule, complete the following steps.

1. Select the minute past the hour you want discovery to run from the **Minutes past the Hour** list.

   Where the minute value is from 00 through 59.
2. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
3. To finish editing the discovery schedule, return to "Editing a discovery schedule" on page 76.

Editing a daily discovery schedule

To edit a daily discovery schedule, complete the following steps.

1. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
2. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
3. To finish editing the discovery schedule, return to "Editing a discovery schedule" on page 76.

Editing a weekly discovery schedule

To edit a weekly discovery schedule, complete the following steps.

1. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
2. Select the day you want discovery to run from the **Day of the Week** list.
3. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.

4. To finish editing the discovery schedule, return to "Editing a discovery schedule" on page 76.

Editing a monthly discovery schedule

To edit a monthly discovery schedule, complete the following steps.

1. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

2. Select the day you want discovery to run from the **Day of the Month** list (1 through 31).
3. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
4. To finish editing the discovery schedule, return to "Editing a discovery schedule" on page 76.

Editing a yearly discovery schedule

To edit a yearly discovery schedule, complete the following steps.

1. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

2. Click the **Date** list to select a date from the calendar.
3. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
4. To finish editing the discovery schedule, return to "Editing a discovery schedule" on page 76.

Configuring advanced discovery profile preferences

To configure advanced discovery profile preferences, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab.
3. Select the profile you want to edit in the **Discovery Profiles** table and click the **Preferences** tab.

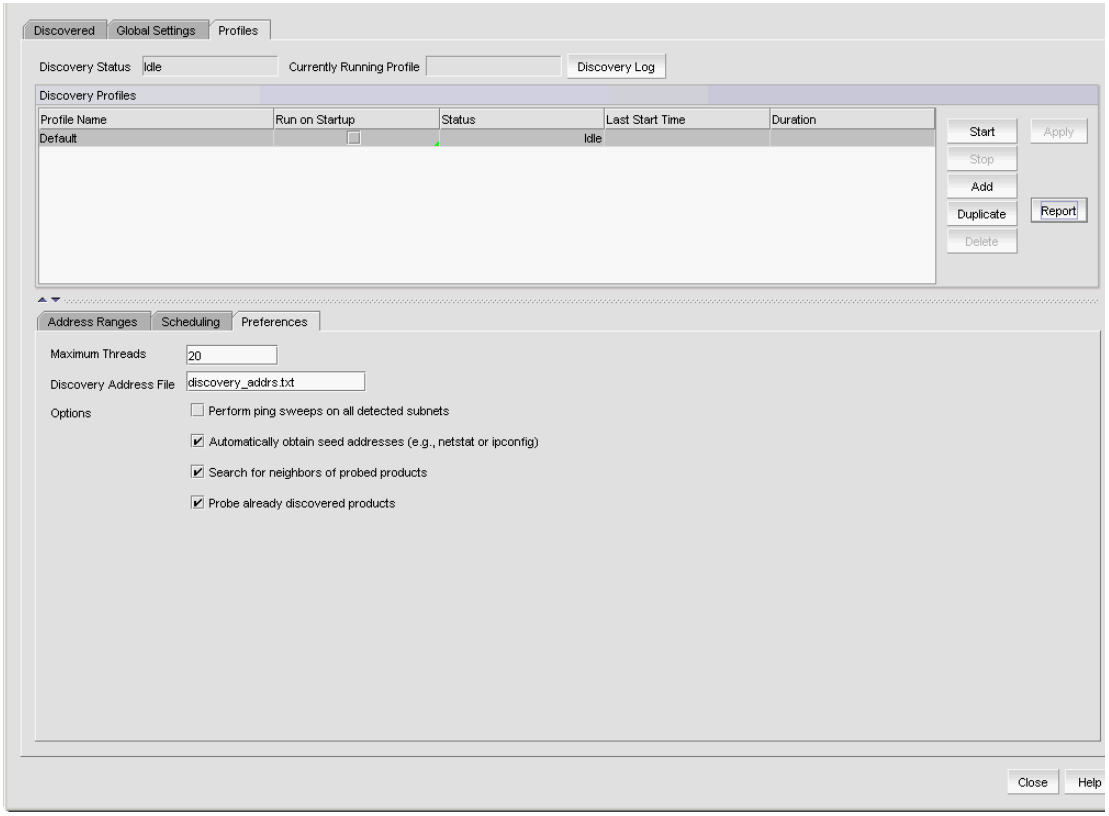


FIGURE 34 **Preferences tab**

4. Enter the maximum number (from 1 through 100) of simultaneous connections to devices allowed by discovery in the **Maximum Threads** field.
5. Enter the name of the file that contains specific IP addresses to probe in the **Discovery Address File** field.

   The file supports both IPv4 and IPv6 addresses. This file must be located in the *Install_Home*\conf\discovery\ip folder on the server. The default file is the discovery_addrs.txt file; however, you can create additional files. To create a discovery address file, refer to "Creating a discovery address file" on page 80.
6. Select the **Perform Ping sweeps on all detected subnets** check box to systematically ping all IP addresses in any subnet detected through the normal discovery process.
7. Select the **Automatically obtain seed addresses** check box to use netstat or ipconfig to capture a starting candidate IP address with which to begin the discovery process.
8. Select the **Search for neighbors of probed products** check box to read all ARP, LLDP, FDP, and CDP tables to find neighboring devices.
9. Select the **Probe already discovered products** check box to rediscover devices previously discovered.
10. Click **Apply** to save your changes.
11. Click **Close** to close the **Discover Setup - IP** dialog box.
12. Click **Yes** on the confirmation message.

Deleting a discovery profile

You can delete any of the discovery profiles except the “Default” profile.

To delete a discovery profile, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab.
3. Select the profile you want to delete in the **Discovery Profiles** table and click **Delete**.
4. Click **Apply** to save your changes.
5. Click **Close** to close the **Discover Setup - IP** dialog box.
6. Click **Yes** on the confirmation message.

Creating a discovery address file

You can configure multiple profiles to use different discovery address files. You can configure multiple profiles to use the same discovery address file.

To create a discovery address file, complete the following steps.

1. Open a text editor (such as Notepad).
2. Enter the IP addresses you want to include in discovery.

```
# discovery_addrs.txt
#
# Discovery reads this file at the
# start of each discovery cycle.
# Discovery probes the IP addresses in
#this file, as long as they are not
# excluded by any scoping restrictions.
#
10.1.2.54
10.55.2.68
```

3. Select **File > Save**.
4. Browse to the *Install_Home*\conf\discovery\ip folder.

   This file must be saved to the *Install_Home*\conf\discovery\ip folder on the server.

5. Enter a name for the file.
6. Click **Save**.

Starting discovery manually

To start discovery for a profile, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab.

3. Select the discovery profile on which you want to start discovery in the **Discovery Profiles** table and click **Start**.
4. Click **Close** to close the **Discover Setup - IP** dialog box.
5. Click **Yes** on the confirmation message.

Starting discovery automatically

To run discovery for a profile at startup, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Profiles** tab.
3. Select the check box in the **Run on Startup** column for the discovery profile in the **Discovery Profiles** table.

   NOTE
   You can only configure one profile to run discovery on startup.
4. Click **Apply** to save your work.
5. Click **Close** to close the **Discover Setup - IP** dialog box.
6. Click **Yes** on the confirmation message.

Stopping discovery

To stop discovery for a profile, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Profiles** tab.
3. Select the discovery profile on which you want to stop discovery in the **Discovery Profiles** table and click **Stop**.
4. Click **Close** to close the **Discover Setup - IP** dialog box.
5. Click **Yes** on the confirmation message.

Viewing discovery status

To view discovery status, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Profiles** tab.
3. Review the status in the **Status** column of the **Discovery Profiles** table.

   Status updates dynamically for any changes. Options include the following statuses:

   - **Running** — Discovery is in progress for the profile.

- **Waiting** — Discovery will start for this profile once the current profile discovery completes.
- **Scheduled** — Discovery will be run for this profile at the scheduled time.
- **Idle** — Discovery is not running.
- **Terminating** — Discovery for the profile is either completing or has been terminated.

4. Click **Close** to close the **Discover Setup - IP** dialog box.
5. Click **Yes** on the confirmation message.

Viewing discovery reports

To view a report for a discovery profile, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab.
3. Select the discovery profile for which you want to view a report in the **Discovery Profiles** table and click **Report**.

   The report displays with the following information.

   - **Discovery Summary** table — Provides discovery statistics.
   - **Discovery Configuration** table — Records the discovery parameters.
   - **Detail** — Provides discovery process details.

4. Click **Close** to close the **Discover Setup - IP** dialog box.
5. Click **Yes** on the confirmation message.

E-mailing discovery reports

To e-mail a report for a discovery profile, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab.
3. Select the discovery profile for which you want to e-mail a report in the **Discovery Profiles** table and click **Report**.
4. Click **E-mail** to send the report in an e-mail message.
5. Enter an e-mail address in the **E-mail Recipients** field or click the associated button to select an e-mail address from the **Users** list.
6. (Optional) Enter additional e-mail addresses in the **E-mail Recipients** field.

   To send an e-mail message to more than one recipient, separate the e-mail addresses using a semicolon (;) delimiter.

7. Click **Send** to send the report.
8. Click **Close** to close the **Discover Setup - IP** dialog box.
9. Click **Yes** on the confirmation message.

Exporting discovery reports

To export a report for a discovery profile, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab.
3. Select the discovery profile for which you want to export a report in the **Discovery Profiles** table and click **Report**.
4. Choose one of the following options:
   - To export the report to a .csv file, select **Export > Export as CSV.**
   - To export the report to an HTML file, select **Export > Export as HTML.**

   The **File Download** dialog box displays.
5. Click **Save**.

   The **Save As** dialog box displays.
6. Browse to the file location where you want to save the report.
7. Click **Save**.
8. Click **Close** to close the **Discover Setup - IP** dialog box.
9. Click **Yes** on the confirmation message.

Viewing the discovery log

The discovery log displays the status of the current discovery activity. To configure the discovery log size, refer to "Defining global setting preferences" on page 60.

To view the discovery log, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab.
3. Click **Discovery Log**.

   The **Discovery Status Log** dialog box displays with a list of discovery status messages. If discovery is running, the discovery status messages automatically display and update dynamically in the dialog box with the latest message at the top.
4. Click **Close** to close the **Discovery Status Log** dialog box.
5. Click **Close** to close the **Discover Setup - IP** dialog box.

Individual IP device discovery

Simple discovery discovers the device with a specific IP address. It is triggered by device configuration changes on SNMP traps, certain configuration deployments to a device, and adding device or rediscovering a device.

Adding an IP device to discovery

NOTE
You cannot discover new products if you do not have the **All IP Products** AOR (area of responsibility) in your user account.

To add an individual IP device to discovery, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click **Add**.

   The **Add product** dialog box displays.

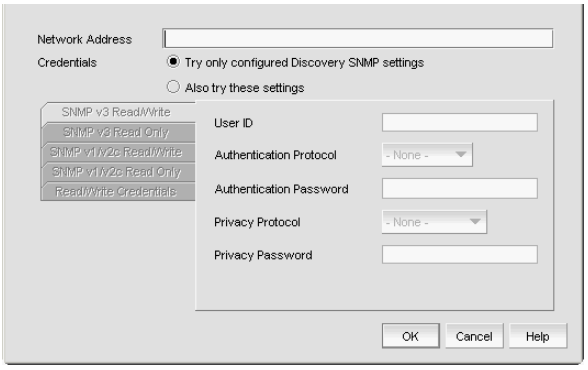


FIGURE 35 Add product dialog box

3. Choose one of the following options:

   - Enter the IP address (IPv4 or IPv6) of the IP device in the **Network Address** field.
   - Enter the host name or DNS name (up to 64 characters) of the IP device in the **Network Address** field.

   NOTE
   The Management application does not validate the Network address until you save your work.

4. Select one of the following options:

   - **Try only configured Discovery SNMP settings** — Select to use the SNMP settings configured in the **Global Settings** tab to contact the device.
   - **Also try these settings** — Select to use specific SNMP settings to contact the device. If you do not enter SNMP settings or if the settings do not authenticate on the device, the application uses the SNMP settings configured in the **Global Settings** tab to contact the device.

NOTE
You can configure both SNMPv3 and SNMPv1/SNMPv2c credentials at the same time; however, discovery tries the SNMPv3 credentials before trying the SNMPv1 and SNMPv2c credentials.

5. Configure the SNMPv3 read-write credentials by completing the following steps.

NOTE
These credentials are not applicable for DCB devices.

a. Click the **SNMPv3 Read/Write** tab.

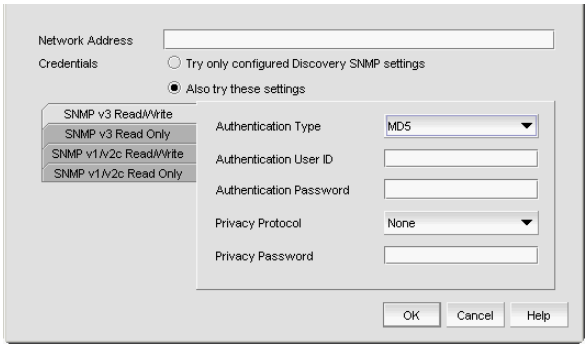


FIGURE 36 SNMPv3 credentials

b. Enter the SNMPv3 user name in the **User ID** field.

The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

c. Select one of the following protocols from the **Authentication Protocol** list:

- None
- **HMAC_MD5**
- HMAC_SHA

d. Enter the SNMPv3 authentication password in the **Authentication Password** field.

The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

e. Select one of the following protocols from the **Privacy Protocol** list:

- None
- CBC-DES
- CFB_AES-128

If you select a privacy protocol, the selected protocol encrypts the SNMP request and response packets.

f. Enter the privacy password in the **Privacy Password** field.

The password can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

6. Configure the SNMPv3 read only credentials by completing the following steps.

a. Click the **SNMPv3 Read Only** tab.

b. Enter the SNMPv3 user name in the **User ID** field.

The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

c. Select one of the following protocols from the **Authentication Protocol** list:

- None
- **HMAC_MD5**
- HMAC_SHA

d. Enter the SNMPv3 authentication password in the **Authentication Password** field.

The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

e. Select one of the following privacy protocol types from the **Privacy Protocol** list:

- None
- CBC-DES
- CFB_AES-128

If you select a privacy protocol, the selected protocol encrypts the SNMP request and response packets.

f. Enter the privacy password in the **Privacy Password** field.

The password can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

7. Configure the SNMPv1 and SNMPv2c read-write credentials by completing the following steps.

a. Click the **SNMPv1/v2c Read/Write** tab.

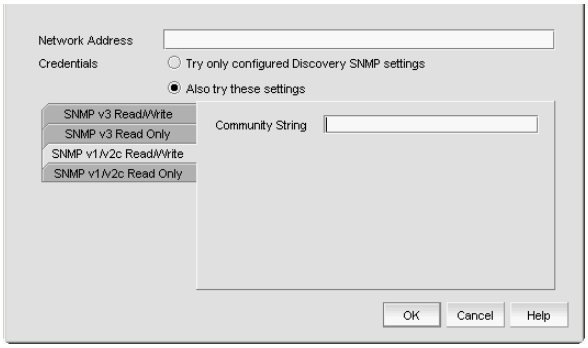


FIGURE 37 SNMPv1/v2c credentials

b. Enter the community string in the **Community** field.

The community string can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The string displays as asterisks.

NOTE
If you do not enter a community string in the field, discovery uses the "public" and "private" community strings to probe the devices.

8. Configure the SNMPv1 and SNMPv2c read only credentials by completing the following steps.
   a. Click the **SNMPv1/v2c Read Only** tab.
   b. Enter the community string in the **Community** field.

      The community string can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The string displays as asterisks.

      NOTE
      If you do not enter a community string in the field, discovery uses the "public" and "private" community strings to probe the devices.

9. Configure the Read/Write credentials by completing the following steps.
   a. Click the **Read/Write Credentials** tab.

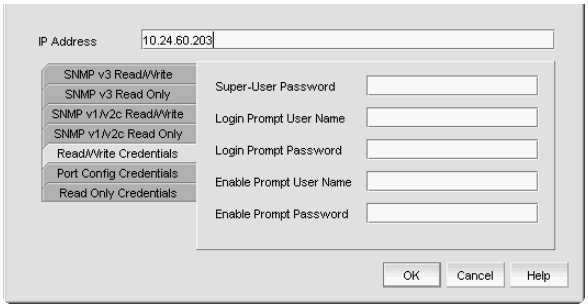


FIGURE 38 Read/Write credentials

   b. Enter the unique user name in the **Login Prompt User Name** field.

      The user name can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters.

   c. Enter the password in the **Login Prompt Password** field.

      The password can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters. The password displays as asterisks. Not applicable to DCB devices.

10. Click **OK** on the **Add product** dialog box.

    The **Discover Setup - IP** dialog box displays with the added IP device in the **Discovered Products** table.

11. Click **Close** to close the **Discover Setup - IP** dialog box.

Editing IP device discovery

NOTE
Although, you can configure third-party product password settings through discovery, the Management application ignores these third-party product settings.

To edit one or more IP devices, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Select one or more IP devices you want to edit in the **Discovered Products** table.

   Select multiple devices by holding down the CTRL key and clicking more than one device.

NOTE
You cannot edit IronWare and Network OS devices at the same time.

NOTE
You can only edit multiple Network OS devices that are running the same firmware level.

3. Click **Edit**.

   The **Edit product** dialog box displays.

4. Select one of the following options:

   - **Try only configured Discovery SNMP settings** — Select to use the SNMP settings configured in the **Global Settings** tab to contact the device.
   - **Also try these settings** — Select to use specific SNMP settings to contact the device. If you do not enter SNMP settings or if the settings do not authenticate on the device, the application uses the SNMP settings configured in the **Global Settings** tab to contact the device.

     NOTE
     You can configure both SNMPv3 and SNMPv1/SNMPv2c credentials at the same time; however, discovery tries the SNMPv3 credentials before trying the SNMPv1 and SNMPv2c credentials.

5. Change the SNMPv3 read-write credentials by completing the following steps.

NOTE
These credentials are not applicable for DCB devices.

   a. Click the **SNMPv3 Read/Write** tab.

FIGURE 39 SNMPv3 credentials

   b. Enter the SNMPv3 user name in the **User ID** field.

      The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

   c. Select one of the following protocols from the **Authentication Protocol** list:

      - None

- **HMAC_MD5**
- HMAC_SHA

d. Enter the SNMPv3 authentication password in the **Authentication Password** field.

The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

e. Select one of the following privacy protocol types from the **Privacy Protocol** list:

- None
- CBC-DES
- CFB_AES-128

If you select a privacy protocol, the selected protocol encrypts the SNMP request and response packets.

f. Enter the privacy password in the **Privacy Password** field.

The password can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

6. Change the SNMPv3 read only credentials by completing the following steps.

a. Click the **SNMPv3 Read Only** tab.

b. Enter the SNMPv3 user name in the **User ID** field.

The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

c. Select one of the following protocols from the **Authentication Protocol** list:

- None
- **HMAC_MD5**
- HMAC_SHA

d. Enter the SNMPv3 authentication password in the **Authentication Password** field.

The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

e. Select one of the following privacy protocol types from the **Privacy Protocol** list:

- None
- CBC-DES
- CFB_AES-128

If you select a privacy protocol, the selected protocol encrypts the SNMP request and response packets.

f. Enter the privacy password in the **Privacy Password** field.

The password can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

7. Change the SNMPv1 and SNMPv2c read-write credentials by completing the following steps.

a. Click the **SNMPv1/v2c Read/Write**. tab

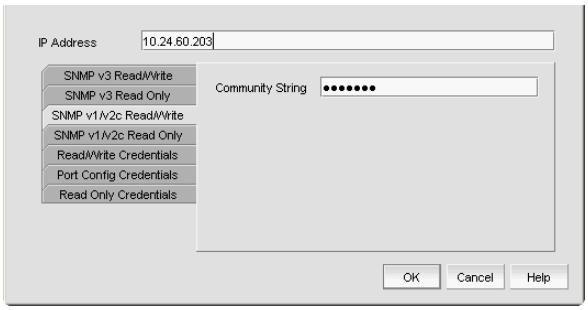


FIGURE 40 SNMPv1/v2c settings

b. Enter the unique community string in the **Community** field.

The community string can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The string displays as asterisks.

NOTE
If you do not enter a community string in the field, discovery uses the "public" and "private" community strings to probe the devices.

8. Change the SNMPv1 and SNMPv2c read only credentials by completing the following steps.
   a. Click the **SNMPv1/v2c Read Only** tab.
   b. Enter the unique community string in the **Community** field.

The community string can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The string displays as asterisks.

NOTE
If you do not enter a community string in the field, discovery uses the "public" and "private" community strings to probe the devices.

9. Change the Read/Write credentials by completing the following steps.
   a. Click the **Read/Write Credentials** tab.

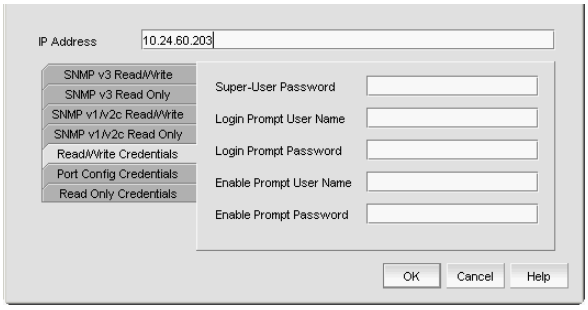


FIGURE 41 Read/Write credentials

b. Enter the password in the **Super-User Password** field.

The password can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters. Not applicable to DCB devices.

c. Change the unique user name in the **Login Prompt User Name** field.

   The user name can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters.

d. Change the password in the **Login Prompt Password** field.

   The password can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

e. Change the unique user name in the **Enable Prompt User Name** field.

   The user name can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters. Not applicable to DCB devices.

f. Change the password in the **Enable Prompt Password** field.

   The password can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks. Not applicable to DCB devices.

10. Change the Port Config credentials by completing the following steps.

NOTE
These credentials are not applicable for DCB, VDX, or VCS devices.

a. Click the **Port Config Credentials** tab.

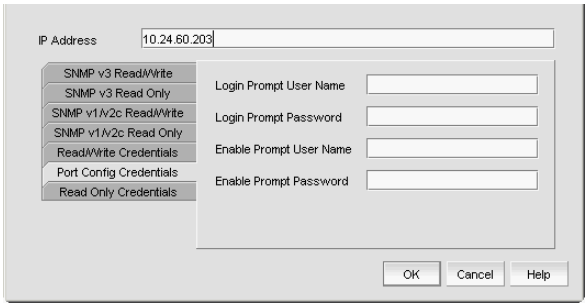


FIGURE 42 Port Config credentials

b. Change the unique user name in the **Login Prompt User Name** field.

   The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

c. Change the password in the **Login Prompt Password** field.

   The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

d. Change the unique user name in the **Enable Prompt User Name** field.

   The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

e. Change the password in the **Enable Prompt Password** field.

   The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

11. Change the Read Only credentials by completing the following steps.

NOTE
These credentials are not applicable for DCB, VDX, or VCS devices.

a. Click the **Read Only Credentials** tab.

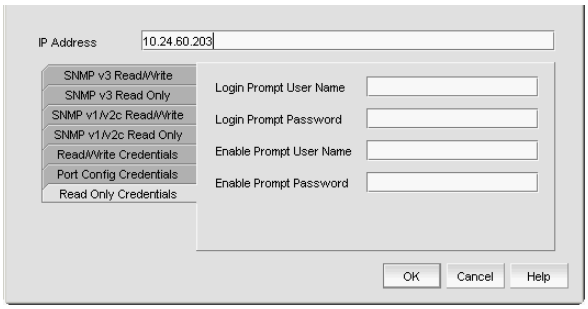


FIGURE 43 **Read Only credentials**

a. Change the unique user name in the **Login Prompt User Name** field.

The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

b. Change the password in the **Login Prompt Password** field.

The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

c. Change the unique user name in the **Enable Prompt User Name** field.

The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

d. Change the password in the **Enable Prompt Password** field.

The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

12. Click **OK** on the **Edit product** dialog box.

The **Discover Setup - IP** dialog box displays with the updated IP device in the **Discovered Products** table.

13. Click **Close** to close the **Discover Setup - IP** dialog box.

Deleting IP devices from discovery

To delete one or more IP devices from discovery, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Select the IP devices you want to remove from discovery in the **Discovered Products** table.

   Select multiple devices by holding down the CTRL key and clicking more than one device.

   NOTE
   You cannot delete an active member from a VCS fabric.

3. Click **Delete**.

Host discovery

The Management application enables you to discover individual hosts, import a group of Host from a comma separated values (CSV) file, or import all hosts from discovered fabrics or VM managers.

NOTE
Host discovery requires HCM Agent 2.0 or later.

NOTE
SMI and WMI discovery are not supported.

Discovering Hosts by Network address or host name

To discover a Host by Network address or host name, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

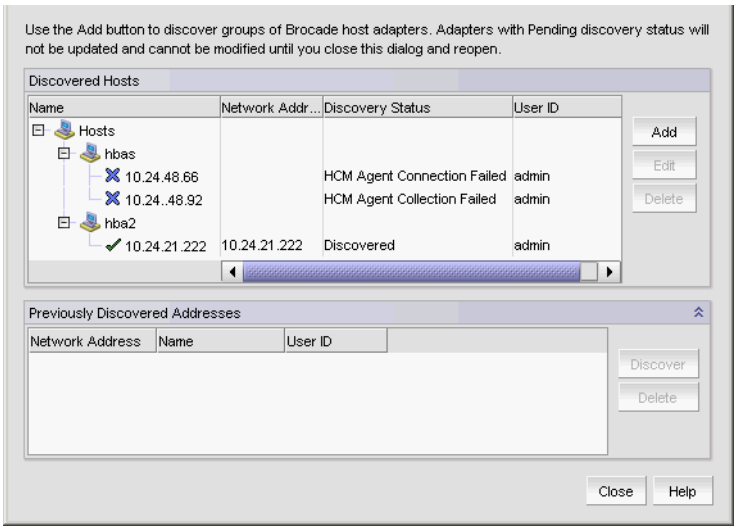


FIGURE 44 Discover Host Adapters dialog box

2. Click **Add**.

   The **Add Host Adapters** dialog box displays.

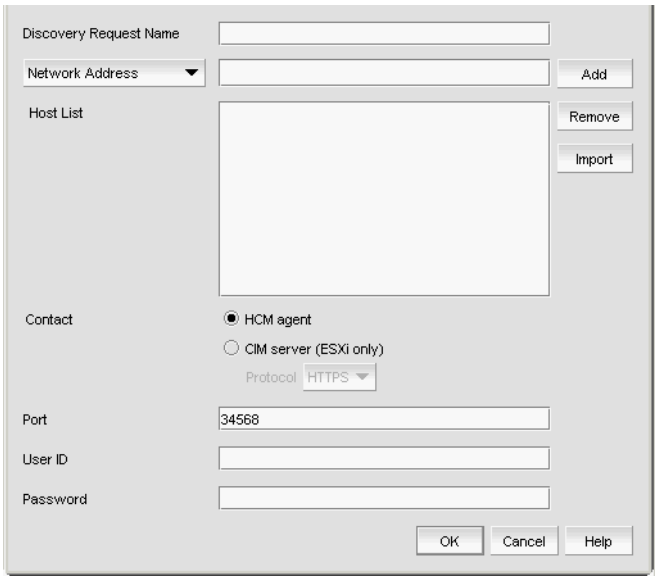


FIGURE 45 Add Host Adapters dialog box

3. (Optional) Enter a discovery request name (such as, Manual 06/12/2009) in the **Discovery Request Name** field.
4. Select **Network Address** from the list.
5. Enter the IP address (IPv4 or IPv6 formats) or host name in the **Network Address** field.
6. Click **Add**.

   The IP address or host name of the Host displays in the **Host List**.

7. Configure Host credentials by choosing one of the following options:
   - To configure HCM agent credentials, select the **HCM agent** option. Go to step 9.
   - To configure CIM server credentials, select the **CIM server (ESXi only)** option. Continue with step 8.

   If you do not need to configure Host credentials, skip to step 13.
8. Configure discovery authentication by choosing one of the following options:
   - To configure discovery with authentication, select the **HTTPS** from the **Protocol** list.
   - To configure discovery without authentication, select the **HTTP** from the **Protocol** list.
9. Enter the port number in the **Port** field.

   HCM agent default is 34568. CIM server HTTPS default is 5989. CIM server HTTP default is 5988.
10. Enter your username in the **User ID** field.

    HCM agent default is admin. Leave this field blank for the CIM server.
11. Enter your password **Password** field.

    HCM agent default is password. Leave this field blank for the CIM server.
12. Repeat step 5 through step 11 for each Host you want to discover.
13. Click **OK** on the **Add Host Adapters** dialog box.

    If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

    A Host Group displays in **Discovered Hosts** table with pending status. To update the status from pending you must close and reopen the **Discover Host Adapters** dialog box.
14. Click **Close** on the **Discover Host Adapters** dialog box.

Importing Hosts from a CSV file

To discover Hosts by importing a CSV file, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.
2. Click **Add**.

   The **Add Host Adapters** dialog box displays.

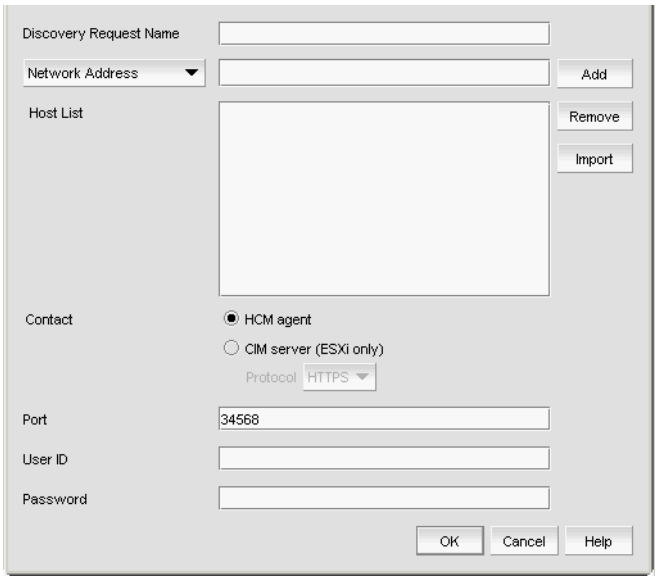


FIGURE 46 Add Host Adapters dialog box

3. Enter a discovery request name (such as, MyFabric) in the **Discovery Request Name** field.
4. Click **Import**.

   The **Open** dialog box displays.
5. Browse to the CSV file location.

   The CSV file must meet the following requirements:

   - Comma separated IP address or host names
   - No commas within the values
   - No escaping supported

     For example, XX.XX.XXX.XXX, XX.XX.X.XXX, computername.company.com
6. Click **Open**.

   The CSV file is imported to the **Add Host Adapters** dialog box. During import, duplicate values are automatically dropped. When import is complete, the imported values display in the **Host List**. If the file cannot be imported, an error displays.
7. Verify the imported values in the **Host List**.
8. Configure Host credentials by choosing one of the following options:

   - To configure HCM agent credentials, select the **HCM agent** option. Go to step 10.
   - To configure CIM server credentials, select the **CIM server (ESXi only)** option. Continue with step .

   If you do not need to configure Host credentials, skip to step 13.
9. Configure discovery authentication by choosing one of the following options:

   - To configure discovery with authentication, select the **HTTPS** from the **Protocol** list.
   - To configure discovery without authentication, select the **HTTP** from the **Protocol** list.

10. Enter the port number in the **Port** field.

    HCM agent default is 34568. CIM server HTTPS default is 5989. CIM server HTTP default is 5988.

11. Enter your username in the **User ID** field.

    HCM agent default is admin. Leave this field blank for the CIM server.

12. Enter your password **Password** field.

    HCM agent default is password. Leave this field blank for the CIM server.

13. Click **OK** on the **Add Host Adapters** dialog box.

    If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

    A Host Group displays in **Discovered Hosts** table with pending status. To update the status from pending you must close and reopen the **Discover Host Adapters** dialog box.

14. Click **Close** on the **Discover Host Adapters** dialog box.

Importing Hosts from a Fabric

To discover a Host from a discovered fabric, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Click **Add**.

   The **Add Host Adapters** dialog box displays.

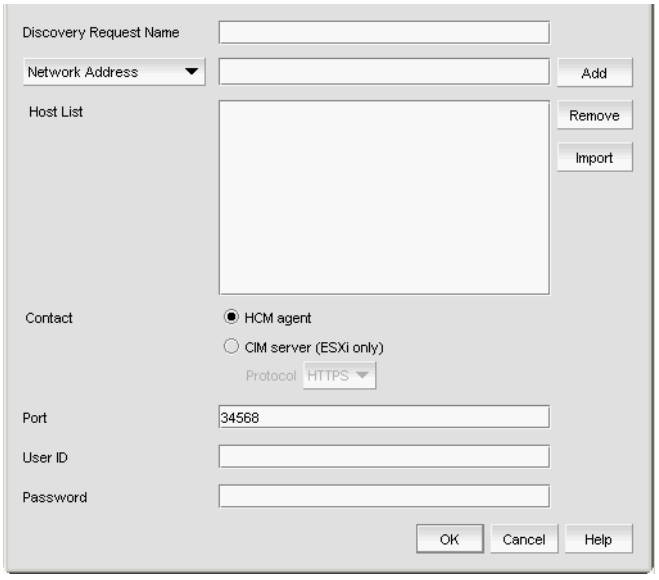


FIGURE 47 Add Host Adapters dialog box

3. Enter a discovery request name (such as, MyFabric) in the **Discovery Request Name** field.
4. Select **Hosts in Fabrics** from the list.
5. Select **All fabrics** or an individual fabric from the list.

6. Click **Add**.

   All hosts which are part of a managed fabric and have a registered host name display in the list. If no host with a registered host name exists, an error message displays. Click **OK** to close the error message.

7. Configure Host credentials by choosing one of the following options:

   - To configure HCM agent credentials, select the **HCM agent** option. Go to step 9.
   - To configure CIM server credentials, select the **CIM server (ESXi only)** option. Continue with step 8.

   If you do not need to configure Host credentials, skip to step 12.

8. Configure discovery authentication by choosing one of the following options:

   - To configure discovery with authentication, select the **HTTPS** from the **Protocol** list.
   - To configure discovery without authentication, select the **HTTP** from the **Protocol** list.

9. Enter the port number in the **Port** field.

   HCM agent default is 34568. CIM server HTTPS default is 5989. CIM server HTTP default is 5988.

10. Enter your username in the **User ID** field.

    HCM agent default is admin. Leave this field blank for the CIM server.

11. Enter your password **Password** field.

    HCM agent default is password. Leave this field blank for the CIM server.

12. Click **OK** on the **Add Host Adapters** dialog box.

    If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

    A Host Group displays in **Discovered Hosts** table with pending status. To update the status from pending you must close and reopen the **Discover Host Adapters** dialog box.

13. Click **Close** on the **Discover Host Adapters** dialog box.

Importing Hosts from a VM manager

To discover Hosts from a discovered VM manager, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Click **Add**.

   The **Add Host Adapters** dialog box displays.

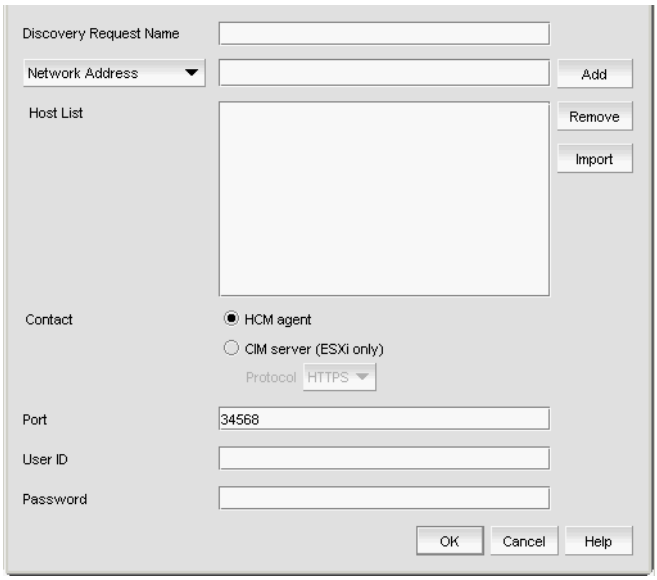


FIGURE 48 Add Host Adapters dialog box

3. Enter a discovery request name (such as, MyVMManager) in the **Discovery Request Name** field.
4. Select **Hosts from VM Manager** from the import by list.
5. Select **All VM** or an individual VM from the list.
6. Click **Add**.

   All hosts which are part of a discovered VM manager and have a registered host name display in the list. If no host with a registered host name exists, an error message displays. Click **OK** to close the error message.
7. Configure Host credentials by choosing one of the following options:
   - To configure HCM agent credentials, select the **HCM agent** option. Go to step 9.
   - To configure CIM server credentials, select the **CIM server (ESXi only)** option. Continue with step 8.

   If you do not need to configure Host credentials, skip to step 12.
8. Configure discovery authentication by choosing one of the following options:
   - To configure discovery with authentication, select the **HTTPS** from the **Protocol** list.
   - To configure discovery without authentication, select the **HTTP** from the **Protocol** list.
9. Enter the port number in the **Port** field.

   HCM agent default is 34568. CIM server HTTPS default is 5989. CIM server HTTP default is 5988.
10. Enter your username in the **User ID** field.

    HCM agent default is admin. Leave this field blank for the CIM server.
11. Enter your password **Password** field.

    HCM agent default is password. Leave this field blank for the CIM server.

12. Click **OK** on the **Add Host Adapters** dialog box.

    If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

    A Host Group displays in **Discovered Hosts** table with pending status. To update the status from pending you must close and reopen the **Discover Host Adapters** dialog box.

13. Click **Close** on the **Discover Host Adapters** dialog box.

Editing Host adapter credentials

To edit Host credentials, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Select the Host in the **Discovered Hosts** list and click **Edit**.

   The **Edit Host Adapters** dialog box displays.

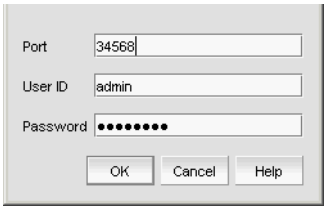


FIGURE 49 Edit Host Discovery dialog box

3. Configure Host credentials by choosing one of the following options:
   - To configure HCM agent credentials, select the **HCM agent** option. Go to step 5.
   - To configure CIM server credentials, select the **CIM server (ESXi only)** option. Continue with step 4.

   If you do not need to configure Host credentials, skip to step 8.

4. Configure discovery authentication by choosing one of the following options:
   - To configure discovery with authentication, select the **HTTPS** from the **Protocol** list.
   - To configure discovery without authentication, select the **HTTP** from the **Protocol** list.

5. Enter the port number in the **Port** field.

   HCM agent default is 34568. CIM server HTTPS default is 5989. CIM server HTTP default is 5988.

6. Enter your username in the **User ID** field.

   HCM agent default is admin. Leave this field blank for the CIM server.

7. Enter your password **Password** field.

   HCM agent default is password. Leave this field blank for the CIM server.

8. Click **OK** on the **Edit Host Adapters** dialog box.

   If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

9. Click **Close** on the **Discover Host Adapters** dialog box.

Removing a host from active discovery

If you decide you no longer want the Management application to discover and monitor a specific host, you can delete it from active discovery. Deleting a host also deletes the host data on the server (both system collected and user-defined data) except for user-assigned names for the device port, device node, and device enclosure information.

To delete a host from active discovery, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Select the host you want to delete from active discovery in the **Discovered Hosts** table.
3. Click **Delete**.
4. Click **OK** on the confirmation message.

   The deleted host displays in the **Previously Discovered Addresses** table.

5. Click **Close** on the **Discover Host Adapters** dialog box.

Rediscovering a previously discovered fabric

To return a host to active discovery, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Select the host you want to return to active discovery in the **Previously Discovered Addresses** table.
3. Click **Discover**.
4. Click **OK** on the confirmation message.

   The rediscovered host displays in the **Discovered Hosts** table.

5. Click **Close** on the **Discover Host Adapters** dialog box.

Deleting a host adapter from discovery

To delete a host permanently from discovery, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Select the host you want to delete permanently from discovery in the **Previously Discovered Addresses** table.
3. Click **Delete**.
4. Click **OK** on the confirmation message.
5. Click **Close** on the **Discover Host Adapters** dialog box.

Viewing the host discovery state

The Management application enables you to view device discovery status through the **Discover Host Adapters** dialog box.

To view the discovery status of a device, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Right-click the Hosts node select **Expand All** to show all devices.

   The **Name** field displays the discovery status icons in front of the device name. The following table illustrates and describes the icons that indicate the current status of the discovered devices.

TABLE 14 Discovery Status Icons

Icon	Description
	Displays when the fabric or host is managed and the management status is okay.
	Displays when the fabric or host is not managed.

The **Discovery Status** field details the actual status message text, which varies depending on the situation. The following are samples of actual status messages:

- Discovered
- New Discovery Pending
- Created host structure differs from discovered host; Discovery ignored
- Brocade HBA Discovery Failed: HCM Agent connection failed
- HCM Agent collection failed
- CIM Server Authentication failed
- CIM Server connection failed

Troubleshooting host discovery

If you encounter discovery problems, complete the following checklist to ensure that discovery was set up correctly. For more complete information about troubleshooting adapters, refer to the *Adapters Troubleshooting Guide*.

1. Verify IP connectivity by issuing a ping command to the host.
   a. Open the command prompt.
   b. From the Server, type `ping Host_IP_Address`.

2. If the host is responding to ping, but discovery still fails, verify that HCM agent is up or not by browsing to the following URL:

   https://*Host_IP_Address*:34568/JSONRPCServiceApp/JSON-RPC

   If HCM agent is running and reachable, you should receive a prompt of credentials and then show an Error 500 (No Reason) result page.

3. Verify that firewall port 34568 is open.

   There are firewall issues with the HCM Agent on Windows 2008 and VMware systems. When installing the driver package on these systems, open TCP/IP port 34568 to allow agent communication with the Management application.

   - For VMware, use the following commands to open port 34568:
     - `esxcfg-firewall –o 34568,tcp,in,https`
     - `esxcfg-firewall –o 34568,udp,out,https`
   - For Windows, use Windows Firewall and Advanced Service (WFAS) to open port 34568.

VM Manager discovery

The Management application enables you to discover VM managers. VM Manager discovery requires vCenter Server 4.0 or later.

NOTE
vCenter discovery time is dynamically determined based on the number of hosts being managed by the vCenter. For every 50 hosts managed, the vCenter collection period increases 30 minutes. For 0-50 hosts managed, the collection duration is 30 minutes; for 50-100 hosts managed, the collection duration is one hour, and so on.

VM Manager discovery requirements

- Discovery of a vCenter server (refer to "Discovering a VM manager" on page 103, step 4 and step 5), requires a vCenter user with read-only or read-write privilege on the vCenter server node and all objects in the inventory below the vCenter server.
- Enabling the vSphere client plug-in registration (refer to "Discovering a VM manager" on page 103, step 6), requires a vCenter user with, at minimum, the following read-write privileges on the vCenter server node and all objects in the inventory below the vCenter server:
  - Extension > Register extension
  - Extension > Unregister extension
  - Extension > Update extension

Discovering a VM manager

Before you discover a VM Manager, make sure you meet the discovery requirements (refer to "VM Manager discovery requirements" on page 103).

To discover a VM manager, complete the following steps.

1. Select **Discover > VM Managers**.

   The **Discover VM Managers** dialog box displays.

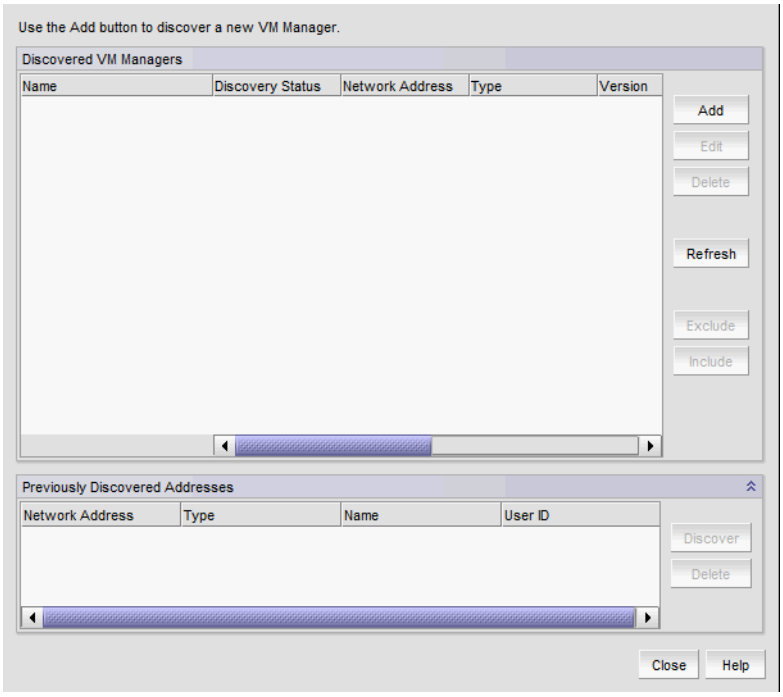


FIGURE 50 **Discover VM Managers dialog box**

2. Click **Add**.

   The **Add VM Manager** dialog box displays.

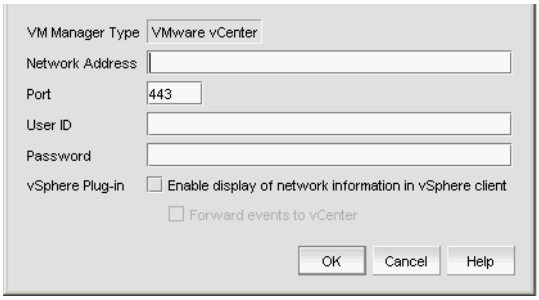


FIGURE 51 **Add VM Manager dialog box**

3. Enter the IP address or host name in the **Network Address** field.
4. Enter the VM manager port number in the **Port** field.
5. Enter the VM manager username in the **User ID** field.
6. Enter the VM manager password **Password** field.
7. Select the **Enable display of network information in vSphere client** check box to enable vSphere client plug-in registration.

   Clear to disable vSphere client plug-in registration.

8. Select the **Forward event to vCenter** check box to enable event forwarding from the Management application to vCenter.

   Clear to disable event forwarding.

9. Click **OK** on the **Add VM Manager** dialog box.

   If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

   A VM manager displays in **Discovered VM Managers** table with pending status. To update the status from pending you must close and reopen the **Discover VM Managers** dialog box.

10. Refresh the **Discover VM Managers** list by clicking **Refresh**.
11. Click **Close** on the **Discover VM Managers** dialog box.

Editing a VM manager

To edit VM manager discovery, complete the following steps.

1. Select **Discover > VM Managers**.

   The **Discover VM Managers** dialog box displays.

2. Select the Host in the **Discovered VM Managers** list and click **Edit**.

   The **Edit VM Manager** dialog box displays.

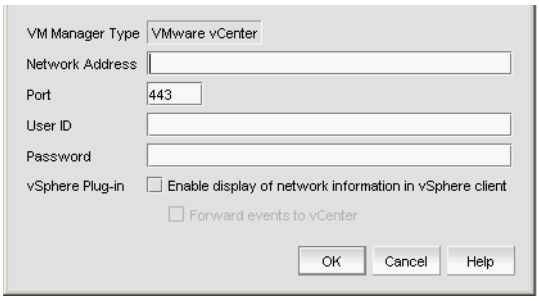


FIGURE 52 Edit VM Manager dialog box

3. Change the VM manager port number in the **Port** field.
4. Enter the VM manager username in the **User ID** field.
5. Enter the VM manager user password **Password** field.
6. Select the **Enable display of network information in vSphere client** check box to enable vSphere client plug-in registration.

   Clear to disable vSphere client plug-in registration.

7. Select the **Forward event to vCenter** check box to enable event forwarding from the Management application to vCenter.

   Clear to disable event forwarding.

8. Click **OK** on the **Edit VM Manager** dialog box.

   If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

9. Refresh the **Discover VM Managers** list by clicking **Refresh**.

10. Click **Close** on the **Discover VM Managers** dialog box.

Excluding a host from VM manager discovery

To exclude host from VM manager discovery complete the following steps.

1. Select **Discover > VM Managers**.

   The **Discover VM Managers** dialog box displays.

2. Select the Host you want to exclude in the **Discovered VM Managers** list and click **Exclude**.
3. Click **Close** on the **Discover VM Managers** dialog box.

Including a host in VM manager discovery

To include host in VM manager discovery complete the following steps.

1. Select **Discover > VM Managers**.

   The **Discover VM Managers** dialog box displays.

2. Select a Host you want to include in the **Discovered VM Managers** list and click **Include**.
3. Click **Close** on the **Discover VM Managers** dialog box.

Removing a VM manager from active discovery

If you decide you no longer want the Management application to discover and monitor a specific VM manager, you can delete it from active discovery. Deleting a VM manager also deletes the data on the server (both system collected and user-defined data) except for user-assigned names for the device port, device node, and device enclosure information.

To delete a VM manager from active discovery, complete the following steps.

1. Select **Discover > VM Managers**.

   The **Discover VM Managers** dialog box displays.

2. Select the VM manager you want to delete from active discovery in the **Discovered VM Managers** table.
3. Click **Delete**.
4. Click **OK** on the confirmation message.

   The deleted VM manager displays in the **Previously Discovered Addresses** table.

5. Refresh the **Discover VM Managers** list by clicking **Refresh**.
6. Click **Close** on the **Discover VM Managers** dialog box.

Rediscovering a previously discovered VM manager

To return a VM manager to active discovery, complete the following steps.

1. Select **Discover > VM Managers**.

   The **Discover VM Managers** dialog box displays.

2. Select the VM manager you want to return to active discovery in the **Previously Discovered Addresses** table.
3. Click **Discover**.
4. Click **OK** on the confirmation message.

   The rediscovered VM manager displays in the **Discovered VM Managers** table.
5. Refresh the **Discover VM Managers** list by clicking **Refresh**.
6. Click **Close** on the **Discover VM Managers** dialog box.

Deleting a VM manager from discovery

To delete a host permanently from discovery, complete the following steps.

1. Select **Discover > VM Managers**.

   The **Discover VM Managers** dialog box displays.
2. Select the VM manager you want to delete permanently from discovery in the **Previously Discovered Addresses** table.
3. Click **Delete**.
4. Click **OK** on the confirmation message.
5. Refresh the **Discover VM Managers** list by clicking **Refresh**.
6. Click **Close** on the **Discover VM Managers** dialog box.

Viewing the VM manager discovery state

The Management application enables you to view device discovery status through the **Discover VM Managers** dialog box.

To view the discovery status of a device, complete the following steps.

1. Select **Discover > VM Managers**.

   The **Discover VM Managers** dialog box displays.
2. Right-click the Hosts node select **Expand All** to show all devices.

   The **Discovery Status** field details the actual status message text, which varies depending on the situation.

   The following are samples of actual VMM status messages:

   - Active
   - Failed – Not reachable
   - Failed – Authentication failure

   The following are samples of actual ESX host status messages:

   - Active
   - Discovery pending,
   - Excluded,
   - Conflict – Existing Host <hostname>

3. Refresh the **Discover VM Managers** list by clicking **Refresh**.
4. Click **Close** on the **Discover VM Managers** dialog box.

Troubleshooting VM manager discovery

If you encounter discovery problems, complete the following checklist to ensure that discovery was set up correctly.

Verify IP connectivity by issuing a ping command to the switch.

1. Open the command prompt.
2. From the Server, type `ping` *`Device_IP_Address`*.

IP Rediscovery

When you change device configuration using the CLI or Web Management Interface, the updated configuration information does not automatically update in the Management application. You must rediscover devices to update configuration information.

For VCS devices, if you do not have the **All IP Products** AOR (area of responsibility) in your user account, you can not rediscover missing fabric members.

When you rediscover an IP device, the Management application captures and stores all changes to its configuration since the last Discovery or Rediscovery cycle. Once Rediscovery completes, configuration updates display in Network Object view.

Rediscovering IP devices

To rediscover one or more IP devices, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Select the IP devices you want to rediscover in the **Discovered Products** table.

   For VCS devices, if you do not have the **All IP Products** AOR (area of responsibility) in your user account, you can not rediscover missing fabric members.

   Select multiple devices by holding down the CTRL key and clicking more than one device. You can select up to 32 devices for rediscovery.

   If you select to rediscover multiple devices, you should configure a discovery profile to run in the background. For step-by-step instructions, refer to "Configuring a discovery profile" on page 64.

   For VCS devices, rediscovery depends on what part of the fabric you select to rediscover.

   - If you select the VCS fabric, rediscovery refreshes the membership information.
   - If you select a VCS member, rediscovery refreshes the asset data for the selected member.
   - If you select a missing VCS member, rediscovery triggers the discovery of a new fabric (VCS-enabled) or a standalone VDX switch (VCS-disabled).

3. Click **Rediscover**.

   The **Rediscover product** dialog box displays. If you selected more than 10 devices, the client only sends the first 10 devices to the server. When rediscovery is complete on the first device and the server returns the status to the client, the client sends the next device to the server. This process continues until rediscovery is complete.

   The **Rediscover product** dialog box displays the progress status for each product in the **Progress Status** column. If an error occurs the status displays as 'Failed" and an error message displays in the **Description** column.

   Click **Abort** to stop rediscovery for any pending devices. Note that rediscovery continues for all devices already sent to the server. The **Rediscover product** dialog box closes when rediscovery is complete for the active rediscovery devices.

4. Click **OK** on the **Rediscover product** dialog box when rediscovery completes.

Rediscovering IP devices from the Product List

For VCS devices, if you do not have the **All IP Products** AOR (area of responsibility) in your user account, you can not rediscover missing fabric members.

To rediscover one or more IP devices from the Product List, complete the following steps.

1. Select the **IP** tab.
2. Select the IP devices you want to rediscover in the Product List.

   Select multiple devices by holding down the CTRL key and clicking more than one device. You can select up to 32 devices for rediscovery.

   If you select to rediscover a multiple devices, you should configure a discovery profile to run in the background. For step-by-step instructions, refer to "Configuring a discovery profile" on page 64.

3. Click **Rediscover** on the Product List toolbar.

   The **Rediscover product** dialog box displays. If you selected more than 10 devices, the client only sends the first 10 devices to the server. When rediscovery is complete on the first device and the server returns the status to the client, the client sends the next device to the server. This process continues until rediscovery is complete.

   The **Rediscover product** dialog box displays the progress status for each product in the **Progress Status** column. If an error occurs the status displays as 'Failed" and an error message displays in the **Description** column.

   Click **Abort** to stop rediscovery for any pending devices. Note that rediscovery continues for all devices already sent to the server. The **Rediscover product** dialog box closes when rediscovery is complete for the active rediscovery devices.

4. Click **OK** on the **Rediscover product** dialog box when rediscovery completes.

Rediscovering a group

To rediscover all devices in a group, complete the following steps.

1. Select the **IP** tab.
2. Select the group you want to rediscover in the Product List.

   You can select one group at a time.
3. Click **Rediscover** on the Product List toolbar.

   The **Rediscover product** dialog box displays. If you selected more than 10 devices, the client only sends the first 10 devices to the server. When rediscovery is complete on the first device and the server returns the status to the client, the client sends the next device to the server. This process continues until rediscovery is complete.

   The **Rediscover product** dialog box displays the progress status for each product in the **Progress Status** column. If an error occurs the status displays as 'Failed" and an error message displays in the **Description** column.

   Click **Abort** to stop rediscovery for any pending devices. Note that rediscovery continues for all devices already sent to the server. The **Rediscover product** dialog box closes when rediscovery is complete for the active rediscovery devices.
4. Click **OK** on the **Rediscover product** dialog box when rediscovery completes.

Enabling password validation on rediscovery

To define global setting preferences, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Global Settings** tab.
3. Click the **Preferences** tab.
4. Select the **Enable password validation on rediscover** check box to enable password validation when rediscovering devices.
5. Click **Apply** to close the **Discover Setup - IP** dialog box.
6. Click **Close** to close the **Discover Setup - IP** dialog box.

Chapter

4

Management Groups

In this chapter

Management groups overview

The Management application enables you to group multiple devices or ports so that you can configure common configurations and perform common monitoring functions for them. You configure management groups through the Network Objects view.

The Network Object view lists the discovered products, default and user-defined product groups, and user-defined port groups. You can use Network Object view to do the following:

- Add devices to product groups.
- Remove devices from product groups.
- Add ports to port groups.
- Remove ports from port groups.
- Synchronize the device configuration with the Management application database before the next Discovery process runs.

The number of devices, device groups, and port groups that Network Object view can manage depends on the disk space available to the Management application. However, adding many devices and groups could affect system performance.

Displaying Network Object view

To display the Network Object view, select **Network Objects** from the view list on the Product List toolbar.

The Management application displays a list of discovered products as well as any product and port groups in a table (Product List). For more information about the Network Object view, refer to "Network Objects view" on page 307.

You can perform the following actions from the Network Object view:

- To configure product groups, refer to "Product group overview" on page 112.
- To configure port groups, refer to "Port Groups" on page 122.
- To search for a product in the Network Object view, refer to "Searching for a device" on page 299.

- To filter the Network Objects Product List, refer to "Filtering devices in the Network Objects Product List" on page 308.
- To update device configuration information on the Network Object view, refer to "IP Rediscovery" on page 108.

Product group overview

Once devices display in the Network Object view, you can associate the devices with a group. Product groups allow you to monitor and manage multiple devices at one time. Once configured you can use product groups to perform the following:

- Deploy common configurations to all devices in a group
- Implement common monitoring facilities for all devices in a group.
- Identify which MPLS configured devices can be managed by MPLS.

The Management application provides pre-defined System Groups and allows you to create user-defined groups.

- System Groups — Groups pre-defined by the Management application. Discovered devices automatically display in these groups. You can see all system groups; however, under each group, you can only see devices that belong to your area of responsibility (AOR). The system groups include the following:
  - Fixed Configuration Products
  - Layer 2 Switch Products
  - Other Products
  - Wireless Standalone APs
  - All IP Products
  - Load Balancer Products
  - Wireless Controllers
  - IP Wired Products
  - Chassis Products
  - Router Products
  - MPLS Licensed and Configured Products

- User-Defined Groups — Groups created by users. All users can see user-defined product groups; however, you can only see products in the group that belong to your AOR. You can create two type of groups - static and dynamic.

  NOTE
  You can add a standalone VDX product or a VCS fabric to a user-defined Product Group; however, the VCS fabric members are not included with the group.

  - Static — You can define a product group by selecting the product you want to include inthe group.
  - Dynamic — You can define a product group using the following product attributes:
    - Name
    - IP Address
    - Product Type
    - Serial #
    - Status
    - Vendor
    - Model
    - Firmware
    - Build Label
    - Location
    - Contact
    - Description
    - *User_defined_property1* (up to 3)

Static product groups

You can define a static product group by selecting the product you want to include in the group.

Creating a static product group

To create a product group, complete the following steps.

1. Select **Network Objects** from the view list on the Product List toolbar.
2. Select **Add Product Group > Static** from the **Grouping** list on the Product List toolbar.

   The **Add Product Group** dialog box displays.

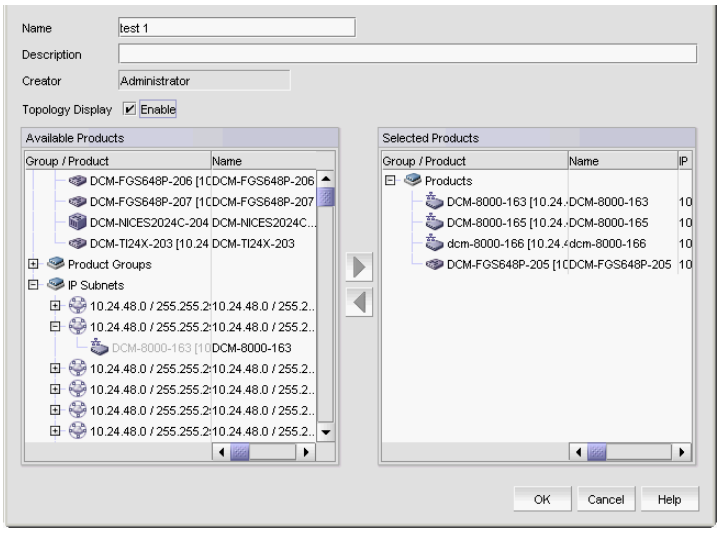


FIGURE 53 Add Product Group dialog box

3. Enter a unique name (maximum 64 characters) for the product group in the **Name** field.
4. Enter a description (maximum 255 characters) for the product group in the **Description** field.
5. Select the **Topology Display Enable** check box to display the product group in theL2 Topology view.
6. Add products to the group by selecting the product in the **Available Products** list and clicking the right arrow button.

NOTE
You can add a standalone VDX product or a VCS fabric to a user-defined Product Group; however, the VCS fabric members are not included with the group.

   The selected products move from the **Available Products** list to the **Selected Products** list.
7. Remove products from the group by selecting the product in the **Selected Products** list and clicking the left arrow button.

   The selected products move from the **Selected Products** list to the **Available Products** list.
8. Click **OK**.

   The new group displays in the User-Defined Groups folder of the Product list.

Editing a static product group

To create a product group, complete the following steps.

1. Select **Network Objects** from the view list on the Product List toolbar.
2. Right-click the product group you want to edit in the Product List and select **Edit Group**.

   The **Edit Product Group** dialog box displays.
3. Edit the name for the product group in the **Name** field.
4. Edit the description for the product group in the **Description** field.

5. Select the **Topology Display Enable** check box to display the product group in the L2 Topology view.
6. Add products to the group by selecting the product in the **Available Products** list and clicking the right arrow button.

   NOTE
   You can add a standalone VDX product or a VCS fabric to a user-defined Product Group; however, the VCS fabric members are not included with the group.

   The selected products move from the **Available Products** list to the **Selected Products** list.
7. Remove products from the group by selecting the product in the **Selected Products** list and clicking the left arrow button.

   The selected products move from the **Selected Products** list to the **Available Products** list.
8. Click **OK**.

Duplicating a static product group

To duplicate a product group, complete the following steps.

1. Select **Network Objects** from the view list on the Product List toolbar.
2. Right-click the product group you want to duplicate in the Product List and select **Duplicate Group**.

   The **Add Product Group** dialog box displays.
3. Edit the name for the product group in the **Name** field.
4. Edit the description for the product group in the **Description** field.
5. Select the **Topology Display Enable** check box to display the product group in the L2 Topology view.
6. Add products to the group by selecting the product in the **Available Products** list and clicking the right arrow button.

   NOTE
   You can add a standalone VDX product or a VCS fabric to a user-defined Product Group; however, the VCS fabric members are not included with the group.

   The selected products move from the **Available Products** list to the **Selected Products** list.
7. Remove products from the group by selecting the product in the **Selected Products** list and clicking the left arrow button.

   The selected products move from the **Selected Products** list to the **Available Products** list.
8. Click **OK**.

   The duplicated group displays in the User-Defined Groups folder of the Product list.

Dynamic product groups

You can define a dynamic product group using the following product attributes:

- Name — The name of the product.
- IP Address — The IP address (IPv4 or IPv6 format) of the product.
- Product Type — The type of product.
- Serial # — The serial number of the product.
- Status — The status for the product and the port.
- Vendor — The name of the product's vendor
- Model — The model number of the product.
- Firmware — The firmware version of the product.
- Build Label — The firmware build number.
- Location — The physical location of the product.
- Contact — The name of the person or group you should contact about the product.
- Description — The description of the product.
- *User_defined_property1* (up to 3) — A user-defined product property value. You can create up to 3 user-defined properties (refer to "Properties customization" on page 1329).

Creating a dynamic product group

To create a dynamic product group, complete the following steps.

1. Select **Network Objects** from the view list on the Product List toolbar.
2. Select **Add Product Group > Dynamic** from the **Grouping** list on the Product List toolbar.

   The **Add Product Group - Dynamic** dialog box displays.

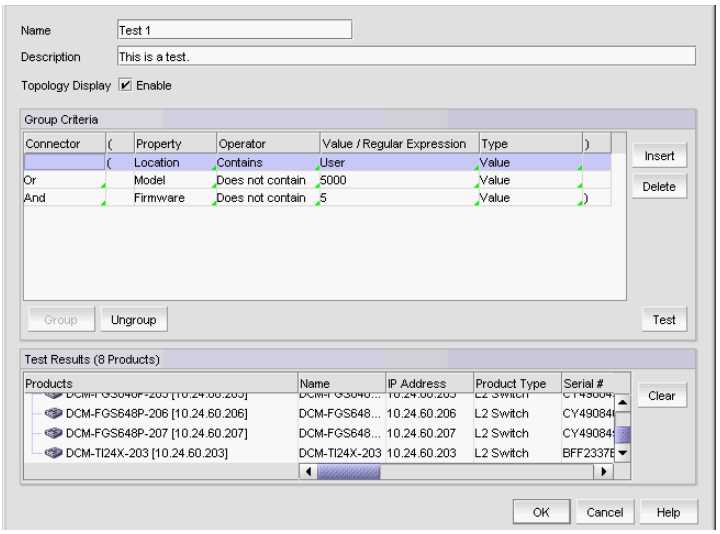


FIGURE 54 **Add Product Group - Dynamic dialog box**

3. Enter a unique name for the product group in the **Name** field.
4. Enter a description for the product group in the **Description** field.

5. Select the **Topology Display Enable** check box to display the product group in the L2 Topology view.
6. Click **Insert**.

   A new row displays in the **Group Criteria** table.
7. Select one of the following from the **Property** list.
   - Name
   - IP Address
   - Product Type
   - Serial #
   - Status
   - Vendor
   - Model

     NOTE
     You can add a standalone VDX product or a VCS fabric to a user-defined Product Group; however, the VCS fabric members are not included with the group.

   - Firmware
   - Build Label
   - Location
   - Contact
   - Description
   - *User_defined_property1* (up to 3)
8. Select one of the following from the **Operator** list.
   - **Equals** (valid for Regular Expression or Value type)
   - **Not Equals** (valid for Regular Expression or Value type)
   - **Starts With** (only valid for Value type)

     Not available if you select Status or Product Type from the **Property** list.
   - **Ends With** (only valid for Value type)

     Not available if you select Status or Product Type from the **Property** list.
   - **Contains** (only valid for Value type)

     Not available if you select Status or Product Type from the **Property** list.
   - **Does not contain** (only valid for Value type)

     Not available if you select Status or Product Type from the **Property** list.

9. Enter a value or regular expression in the **Value/Regular Expression** cell.

   This field is case sensitive.

   If you selected Status from the **Property** list, the following predefined values are populated in the **Value/Regular Expression** cell:

   - Reachable
   - Not Reachable
   - Down
   - Healthy
   - Marginal
   - Degraded Link
   - Unhealthy

   If you selected Product Type from the **Property** list, the following predefined values are populated in the **Value/Regular Expression** cell:

   - L2 Switch
   - Load Balancer
   - Router
   - Wireless Controller
   - Wireless Standalone AP

   To fetch products that have an empty value for a property, select the operator **Equals** from the **Operator** list and leave the **Value/Regular Expression** field blank.

10. Select **Value** or **Regular Expression** from the **Type** list

    To enter another set of criteria, click **Insert**. A new row displays in the **Group Criteria** table. Continue with step 11.

    To test the group criteria, click **Test**. The Management application uses the group criteria to search the available products in your AOR. The products that meet the criteria display in the **Test Results**. table. For detailed information about the test results, refer to "Viewing test results" on page 120.

    To group the criteria, go to step 12.

11. Select a connector (**And**/**Or**) from the **Connector** list and repeat step 8 thorugh step 11.

12. Highlight the rows you want to group and click **Group**.

    An open paren and close paren display in the Group Criteria table to deliniate the new group. You can create up to three groups.

    To ungroup a group, select a row and click **Ungroup**. If the selected row is part of 2 groups, only the inner group ungroups.

13. Click **OK**.

    The new group displays in the **User-Defined Groups** folder of the Product list.

Editing a dynamic product group

To edit a dynamic product group, complete the following steps.

1. Select **Network Objects** from the view list on the Product List toolbar.
2. Right-click the product group you want to edit in the Product List and select **Edit Group**.

   The **Edit Product Group - Dynamic** dialog box displays.
3. Change the name for the product group in the **Name** field.
4. Change the description for the product group in the **Description** field.
5. Select the **Topology Display Enable** check box to display the product group in the L2 Topology view.
6. To add a new row, complete step 6 through step 11 of "Creating a dynamic product group" on page 116.
7. To delete a row, select the row and click **Delete**.
8. To ungroup the criteria, select a row in the group and click **Ungroup**.
9. To create a group, highlight the rows you want to group and click **Group**.

   An open paren and close paren display in the **Group Criteria** table to deliniate the new group. You can create up to three groups.

   To ungroup a group, select a row and click **Ungroup**. If the selected row is part of 2 groups, only the inner group ungroups.
10. Click **OK**.

    The new group displays in the **User-Defined Groups** folder of the Product list.

Duplicating a dynamic product group

To copy a dynamic product group, complete the following steps.

1. Select **Network Objects** from the view list on the Product List toolbar.
2. Right-click the product group you want to edit in the Product List and select **Duplicate Group**.

   The **Add Product Group - Dynamic** dialog box displays.
3. Change the name for the product group in the **Name** field.
4. Change the description for the product group in the **Description** field.
5. Select the **Topology Display Enable** check box to display the product group in the L2 Topology view.
6. To add a new row, complete step 6 through step 11 of "Creating a dynamic product group" on page 116.
7. To delete a row, select the row and click **Delete**.
8. To ungroup the criteria, select a row in the group and click **Ungroup**.

9. To create a group, highlight the rows you want to group and click **Group**.

   An open paren and close paren display in the **Group Criteria** table to deliniate the new group. You can create up to three groups.

   To ungroup a group, select a row and click **Ungroup**. If the selected row is part of 2 groups, only the inner group ungroups.

10. Click **OK**.

    The new group displays in the **User-Defined Groups** folder of the Product list.

Viewing test results

To test the group criteria, click **Test**. The Management application uses the group criteria to search the available products in your AOR. The products that meet the criteria display in the **Test Results**. table. This table includes the following details:

- **Group/Product** — The name of the product or product group.
- **Name** — The name of the product.
- **IP Address** — The IP address (IPv4 or IPv6 format) of the product.
- **Product Type** — The type of product.
- **Serial #** — The serial number of the product.
- **Status** — The status for the product and the port.
- **Vendor** — The name of the product's vendor
- **Model** — The model number of the product.
- **Port Count** — The number of ports on the product.
- **Firmware** — The firmware version of the product.
- **Build Label** — The firmware build number.
- **Location** — The physical location of the product.
- **Contact** — The name of the person or group you should contact about the product.
- **Description** — The description of the product.
- *User_defined_property1* (up to 3) — A user-defined product property value. You can create up to 3 user-defined properties (refer to "Properties customization" on page 1329).

Viewing product group properties

To view group properties, complete the following steps.

1. Select **Network Objects** from the view list on the Product List toolbar.
2. Right-click the product group you want to view properties for in the Product List and select **Properties**.

   The **Product Group Properties** dialog box displays.

3. Review the information:

TABLE 15

Field/Component	Description
Properties tab	Select to display information about the group.
Name	The unique name (maximum 64 characters) for the product group.
Description	The description (maximum 255 characters) for the product group.
Creator	The user name of the creator (for example, Administrator).
Topology Display	Whether or not topology display is enabled.
Dynamic Group	Whether or not this is a dynamic group.
Products tab	Select to display information about products in the group.
Product Count	The number of products in the group.
Performance list	Select to launch the real time or historical performance.
Name	The name of the product.
Alias	The alias.
Host Name	The host name.
System Name	The system name.
IP Address	The IP address (IPv4 or IPv6 format) of the product.
System OID	The system's object identifier.
Device Type	The type of device.
Serial #	The serial number of the product.
Status	The status for the product and the port.
Admin Status.	The admin status of the product. Options include: Normal mode Troubleshooting mode
Memo	Additional information about the product.
Vendor	The name of the product's vendor.
Model	The model number of the product.
Port Count	The number of ports on the product.
Firmware	The firmware version of the product.
Build Label	The firmware build number.
Location	The physical location of the product.
Contact	The name of the person or group you should contact about the product.
Description	The description of the product.
Connected AP Count	The number of connected AP.
User_defined_property (up to 3)	A user-defined product property value. You can create up to 3 user-defined properties (refer to "Properties customization" on page 1329).

4. Click **OK** to close the dialog box.

Deleting a product group

You can delete more than one group at a time.

NOTE
You cannot delete a system group.

To delete a product group, complete the following steps.

1. Select **Network Objects** from the view list on the Product List toolbar.
2. Right-click the product group you want to delete in the Product List and select **Delete Group**.

   Ctrl and click to select more than one group to delete.

   A confirmation message displays.
3. Click **Yes**.

   The group is deleted from the **User-Defined Groups** folder of the Product list.

Port Groups

Port groups allow you to group ports together across network devices to perform common port-based configuration and monitoring activities.

Once configured you can use port groups to perform the following:

- Deploy common configurations to all ports in a group.
- Collect port usage data for all ports in a group.

You can see all port groups; however, under each group, you can only see devices that belong to your area of responsibility (AOR). You can only see user-defined port groups that belong to your AOR.

Creating a port group

To create a port group, complete the following steps.

1. Select **Network Objects** from the view list on the Product List toolbar.
2. Select **Add Port Group** from the **Grouping** list on the Product List toolbar.

   The **Add Port Group** dialog box displays.
3. Enter a unique name for the port group in the **Name** field.
4. Enter a description for the port group in the **Description** field.
5. Select one of the following options:
   - **All Ports** — Select to display all ports.
   - **Ports Connected to APs** — Select to display only ports connected to an access point (AP).

6. Add ports to the group by selecting the port in the **Available Port**s list and clicking the right arrow button.

NOTE
The Management port, peri port, and stack ports are not included in the **Available Port**s list.

The selected ports move from the **Available Port**s list to the **Selected Port**s list.

For VDX 6740 or VDX 6740-T devices, if you create a port group with a 40 GbE port and then the 40 GbE port is broken out into 4 10 GbE ports, the 40 GbE port is automatically removed from the port group. You must manually add the 4 10 GbE ports back into the port group. This also occurs when you merge 4 10 GbE ports into a single 40 GbE port. If you create a port group with 4 10 GbE ports and then merge the 4 10 GbE ports into a 40 GbE port, the 4 10 GbE ports are automatically removed from the port group. You must manually add the 40 GbE port back into the group.

7. Remove ports from the group by selecting the port in the **Selected Port**s list and clicking the left arrow button.

   The selected ports move from the **Selected Port**s list to the **Available Port**s list.

8. Click **OK**.

   The new group displays in the Port Groups folder of the Product list.

Editing a port group

To edit a port group, complete the following steps.

1. Select **Network Objects** from the view list on the Product List toolbar.
2. Right-click the port group you want to edit in the Product List and select **Edit Group**.

   The **Edit Port Group** dialog box displays.

3. Edit the name for the port group in the **Name** field.
4. Edit the description for the port group in the **Description** field.
5. Select one of the following options:
   - **All Ports** — Select to display all ports.
   - **Ports Connected to APs** — Select to display only ports connected to an access point (AP).
6. Add ports to the group by selecting the port in the **Available Port**s list and clicking the right arrow button.

NOTE
The Management port, peri port, and stack ports are not included in the **Available Port**s list.

The selected ports move from the **Available Port**s list to the **Selected Port**s list.

For VDX 6740 or VDX 6740-T devices, if you create a port group with a 40 GbE port and then the 40 GbE port is broken out into 4 10 GbE ports, the 40 GbE port is automatically removed from the port group. You must manually add the 4 10 GbE ports back into the port group. This also occurs when you merge 4 10 GbE ports into a single 40 GbE port. If you create a port group with 4 10 GbE ports and then merge the 4 10 GbE ports into a 40 GbE port, the 4 10 GbE ports are automatically removed from the port group. You must manually add the 40 GbE port back into the group.

7. Remove ports from the group by selecting the port in the **Selected Ports** list and clicking the left arrow button.

   The selected ports move from the **Selected Ports** list to the **Available Ports** list.

8. Click **OK**.

Duplicating a port group

To duplicate a port group, complete the following steps.

1. Select **Network Objects** from the view list on the Product List toolbar.
2. Right-click the port group you want to duplicate in the Product List and select **Duplicate Group**.

   The **Add Port Group** dialog box displays.

3. Edit the name for the port group in the **Name** field.
4. Edit the description for the port group in the **Description** field.
5. Select one of the following options:
   - **All Ports** — Select to display all ports.
   - **Ports Connected to APs** — Select to display only ports connected to an access point (AP).
6. Add ports to the group by selecting the port in the **Available Ports** list and clicking the right arrow button.

   NOTE
   The Management port, peri port, and stack ports are not included in the **Available Port**s list.

   The selected ports move from the **Available Port**s list to the **Selected Port**s list.

   For VDX 6740 or VDX 6740-T devices, if you create a port group with a 40 GbE port and then the 40 GbE port is broken out into 4 10 GbE ports, the 40 GbE port is automatically removed from the port group. You must manually add the 4 10 GbE ports back into the port group. This also occurs when you merge 4 10 GbE ports into a single 40 GbE port. If you create a port group with 4 10 GbE ports and then merge the 4 10 GbE ports into a 40 GbE port, the 4 10 GbE ports are automatically removed from the port group. You must manually add the 40 GbE port back into the group.

7. Remove ports from the group by selecting the port in the **Selected Ports** list and clicking the left arrow button.

   The selected ports move from the **Selected Ports** list to the **Available Ports** list.

8. Click **OK**.

Viewing port group properties

To view port group properties, complete the following steps.

1. Select **Network Objects** from the view list on the Product List toolbar.
2. Right-click the port group you want to view properties for in the Product List and select **Properties**.

   The **Port Group Properties** dialog box displays.
3. Review the information:

TABLE 16

Field/Component	Description
Properties tab	Select to display information about the group.
Name	The unique name (maximum 64 characters) for the product group.
Description	The description (maximum 255 characters) for the product group.
Creator	The user name of the creator (for example, Administrator).
Ports tab	Select to display information about products in the group.
Port Count	The number of ports in the group.
Port Actions list	Select one of the following options: • Enable • Disable • Display Attached Port Properties
Performance list	Select to launch the real time or historical performance.
Identifier	The identifier of the port.
Name	The name of the port.
MAC Address	The MAC Address of the port.
Port Status	The status of the port.
Port State	The state of the port.
Type	The port type.
Speed	The Speed of the port.
L2/Tag Mode	Indicates whether L2 tag mode is enabled or disabled. If enabled, indicates whether the port is tagged, untagged, or dual.
Untagged VLAN ID	The untagged VLAN identifier of the port.
Duplex Mode	The duplex mode of the port, such as auto-sense, full-duplex, or none.
Stacking Port	Whether or not the port stacked.
Role	The role of the device, such as Edge.
Product	The name of the product.
User_defined_property (up to 3)	A user-defined port property value. You can create up to 3 user-defined properties (refer to "Properties customization" on page 1329).

4. Click **OK** to close the dialog box.

Deleting a port group

You can delete more than one group at a time.

To delete a port group, complete the following steps.

1. Select **Network Objects** from the view list on the Product List toolbar.
2. Right-click the port group you want to delete in the Product List and select **Delete Group**.

   Ctrl and click to select more than one group to delete.

   A confirmation message displays.
3. Click **Yes**.

   The group is deleted from the Ports Groups folder of the Product list.

Chapter

5

Application Configuration

In this chapter

Configurable preferences

You can use the **Options** dialog box to configure the following preferences in the Management application:

- Event Storage — Use to configure the maximum number of historical events saved to the repository as well as the retention period for the events. For more information, refer to "Event storage settings" on page 139.
- Flyovers — Use to customize the properties display in product and connection flyovers. For more information, refer to "Flyover settings" on page 140.
- Look and Feel — Use to customize the Management application interface to mimic your system settings as well as define the size of the font. For more information, refer to "Look and feel customization" on page 16.
- Performance Graph Style — Use to configure the color scheme and to display data points for all performance graphics in the management application. For more information, refer to "Performance Data" on page 969.
- Miscellaneous Security — Use to configure server security configurations and the login banner. For more information, refer to "Miscellaneous security settings" on page 149.

- Server Backup — Use to configure backup settings. Backup is a service process that periodically copies and stores application files to an output directory. The output directory is relative to the server and must use a network share format to support backup to the network. If you use a network path as the output directory, you must add network credentials. For more information, refer to "Server Data backup" on page 128 and "Server Data restore" on page 134.
- Syslog Registration — Use to automatically register the server as the syslog recipient on products. For more information, refer to "Syslog Registration settings" on page 151.
- Trap Registration — Use to automatically register the server as the trap recipient on products. If SAN products have Informs enabled, the registration is for the Informs. For more information, refer to "SNMP Trap Registration settings" on page 152.
- Trap Forwarding Credentials — Use to configure SNMP credentials for the traps forwarded by the server. For more information, refer to "SNMP Trap forwarding credential settings" on page 153.
- Client/Server IP — Use to configure IP address of the Management application server. For more information, refer to "Client/Server IP" on page 155.
- IP Preferences — Use to configure IP preferences. For more information, refer to "IP preferences" on page 159.
- Memory Allocation — Use to configure memory allocation for the client and server. For more information, refer to "Memory allocation settings" on page 166.
- Product Communication — Use to configure HTTP or HTTP over SSL for connecting to the server. For more information, refer to "Product communication settings" on page 169.
- FTP/SCP/SFTP servers — Use to configure internal or external FTP, SCP, or SFTP server settings. For more information, refer to "FTP/SCP/SFTP server settings" on page 172.
- Server Port — Use to configure server port settings. For more information, refer to "Server port settings" on page 177.
- Support Mode — Use to configure support settings to enable enhanced diagnostics. For more information, refer to "Support mode settings" on page 178.

Server Data backup

The Management application helps you to protect your data by backing it up automatically. Backup is a service process that periodically copies and stores application files to an output directory. The output directory is relative to the server and must use a network share format to support backup to the network. The data can then be restored, as necessary.

NOTE
Backing up data takes some time. It is possible that, in a disaster recovery situation, configuration changes made after the last backup interval will be missing from the backup.

The Management application allows you to view the backup status at a glance, initiate immediate backup, enable or disable automatic backup, reconfigure the backup directory, interval, and start time, and retrieve backup events.

What is backed up?

The data is backed up to the following directories:

- Backup\databases — contains database and log files.
- Backup\data — contains IP product firmware and configurations.
- Backup\conf – contains the Management application configuration files.

Management server backup

There are three options for backing up data to the Management server:

- Configuring backup to a CD drive
- Configuring backup to a hard drive
- Configuring backup to a network drive

The Management server is backed up to D:\Backup (Windows systems) by default. If there is not second hard disk, this is a rewritable (CD-RW) compact disk. Make sure you have a CD-RW disk in the CD recorder drive to ensure that backup can occur. Critical information from the Management application is automatically backed up to the CD-RW when the data directory contents change or when you restart the Management application.

Note that backing up to CD is not the recommended method. The usable capacity of a CD is approximately 700 MB and needs to be replaced when full. Also, CD media has a limited number of re-writes before the medium is exhausted, and write errors occur. It is recommended that you configure the backup system to target a hard drive or a network drive as described in the procedures below.

Back up directory structure overview

The Management server backs up data to two alternate folders. For example, if the backup directory location is D:\Backup, the backup service alternates between two backup directories, D:\Backup\Backup and D:\Backup\BackupAlt. The current backup is always D:\Backup and contains a complete backup of the system. The older backup is always D:\BackupAlt.

If a backup cycle fails, the cause is usually a full CD-RW. When the backup cycle fails, there may only be one directory, D:\Backup. There may also be a D:\BackupTemp directory. Ignore this directory because it may be incomplete.

Configuring backup

To configure backup, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Server Backup** in the **Category** list.

   The **Server Backup** pane displays (Figure 55) with the currently defined directory displays in the **Backup Output Directory** field.

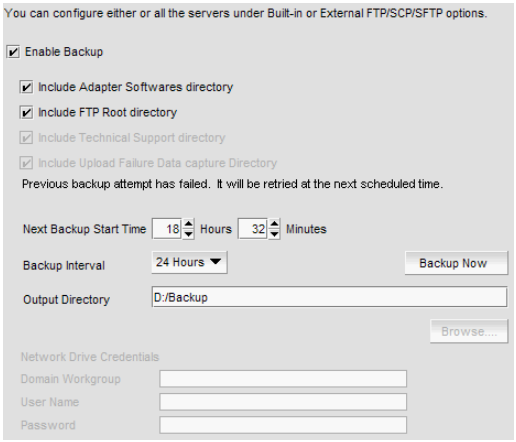


FIGURE 55 Options dialog box (Server Backup pane)

3. Select the **Enable Backup** check box, if necessary.
4. Enter the time (using a 24-hour clock) you want the backup process to begin in the **Next Backup Start Time Hours** and **Minutes** fields.
5. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.
6. Back up data to a hard drive by browsing to the hard drive and directory to which you want to back up your data.

NOTE
This requires a hard drive. The drive should not be the same physical drive on which your Operating System or the Management application is installed.

7. Back up data to a network drive by completing the following steps.

   To back up to a network drive, your workstation can be either in the same domain or in the same workgroup. However, you must have rights to copy files for the network drive.

NOTE
The Management application should not directly access local or network resources through mapped drive letters. When the Management application must access a remote resource (or any process that is running in a different security context), you should use the Universal Naming Convention (UNC) name to access the resource. For more information about services and redirected drives, refer to http://support.microsoft.com/kb/180362/en-us.

NOTE
Configuring backup to a network drive is not supported on UNIX systems.

NOTE
It is recommended that this configuration be completed on the Local client (the client application running on the Server) so that the backup path and location can be confirmed.

a. Browse to the network share and directory to which you want to back up your data.

NOTE
You must specify the directory in a network share format (for example, \\network-name\share-name\directory). Do not use the drive letter format (C:\directory).

b. (Windows only) Enter the name of the Windows domain or workgroup in which you are defined in the **Domain Workgroup** field.

NOTE
You must be authorized to write to the network device.

c. (Windows only) Enter your Windows login name in the **User Name** field.

d. (Windows only) Enter your Windows password in the **Password** field.

8. Back up data to a CD by completing the following steps.

NOTE
This is not recommended on a permanent basis. CDs have a limited life, and may only last a month. An error message occurs if your Management application can no longer back up to the disc.

a. Verify that the CD backup directory is correct (default directory is D:\Backup).

It is assumed that drive D is a CD-RW drive.

You can change the directory or use the **Browse** button to select another directory.

b. Install the formatted disc into the CD drive.

To back up to a writable CD, you must have CD-writing software installed. The disc must be formatted by the CD-writing software so that it behaves like a drive.

9. Click **Apply** or **OK**.

The application verifies that the backup device exists and that the server can write to it.

For back up to a hard drive or writable CD, if the device does not exist or is not writable, an error message displays that says you have entered an invalid device.

For back up to a network drive, if the device does not exist or you are not authorized to write to the network drive, an error message displays that states you have entered an invalid device path or invalid network credentials.

Click **OK** to go back to the **Options** dialog box and fix the error.

Backup occurs, if needed, at the interval you specified.

Enabling backup

Backup is enabled by default. However, if it has been disabled, complete the following steps to enable the function.

1. Select **Server > Options**.

The **Options** dialog box displays.

2. Select **Server Backup** in the **Category** list.

3. Select the **Enable Backup** check box.
4. Click **Apply** or **OK**.

Disabling backup

Backup is enabled by default. If you want to stop the backup process, you need to disable backup. To disable the backup function, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **Server Backup** in the **Category** list.
3. Clear the **Enable Backup** check box.
4. Click **Apply** or **OK**.

Viewing the backup status

The Management application enables you to view the backup status at a glance by providing a backup status icon on the Status Bar. The following table illustrates and describes the icons that indicate the current status of the backup function.

TABLE 17 Backup status

Icon	Description
	Backup in Progress — displays the following tooltip: “Backup started at hh:mm:ss, in progress... *XX* directories are backed up.”
	Countdown to Next Scheduled Backup — displays the following tooltip: “Next backup scheduled at hh:mm:ss.”
	Backup Disabled — displays the following tooltip: “Backup is disabled.”
	Backup Failed — displays the following tooltip: “Backup failed at hh:mm:ss mm/dd/yyyy.”

Changing the backup interval

When the backup feature is enabled, your SAN is protected by automatic backups. The backups occur every 24 hours by default. However, you can change the interval at which backup occurs.

NOTE
Do NOT modify the backup.properties file.

To change the backup interval, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **Server Backup** in the **Category** list.

3. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.
4. Click **Apply** or **OK**.

   The minimum value is 6 hours and the maximum value is 24 hours.

Starting immediate backup

NOTE
You must have backup privileges to use the Backup Now function. For more information about privileges, refer to "User Privileges" on page 1283.

To start the backup process immediately, complete one of the following procedures:

Using the Backup Icon, right-click the **Backup** icon and select **Backup Now**.

The backup process begins immediately.

OR

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **Server Backup** in the **Category** list.
3. Click **Backup Now**.

   Click **Yes** on the confirmation message. The backup process begins immediately.
4. Click **Apply** or **OK**.

Reviewing backup events

The Master Log, which displays in the lower left area of the main window, lists the events that occur on the Fabric.

If you do not see the Master Log, select **View > Show Panels > All Panels**.

The following backup events appear in the Master Log:

- Backup started
- Backup error
- Backup Enabled
- Backup Disabled
- Backup Now
- Backup destination change
- Backup interval change
- Backup start time change
- Domain workgroup change
- User name change
- User password change
- Number of files backed up on completion

- Network share access problem when backup starts or during backup (not when the backup configuration is changed)

Server Data restore

NOTE
You cannot restore data from a previous version of the Management application.

NOTE
You cannot restore data from a higher or lower configuration (Trial or Licensed version) of the Management application.

NOTE
You cannot restore data from a different package of the Management application.

The Management application helps you to protect your data by backing it up automatically. The data can then be restored, as necessary.

The data in the following directories is automatically backed up to disk. The data includes the following items:

- Backup\databases — contains database and log files.
- Backup\data — contains IP product firmware and configurations.
- Backup\conf – contains the Management application configuration files.

In a disaster recovery situation, it is possible that configuration changes made less than 45 minutes before Server loss (depending on the backup interval you set) could be missing from the backup.

Restoring data

NOTE
The restore data files must use the exact directory structure as the backup directory structure (refer to "Back up directory structure overview" on page 129).

1. (Windows) Open the **Server Management Console** from the **Start** menu on the Management application server.

   OR

   (UNIX) Open *Install_Home/bin* from the Management application server and type `./smc.sh` at the command line.

2. Click the **Services** tab.

   The tab lists the Management application services.

3. Click **Stop Services** to stop all of the services.

4. Click the **Restore** tab.

5. Browse to the backup location.

Browse to the location specified in the **Output Directory** field on the **Options** dialog box - Backup pane.

6. Click **Restore**.

   Upon completion, a message displays the status of the restore operation. Click **OK** to close the message and the Server Management Console. For the restored data to take effect, re-launch the Configuration Wizard using the instructions in "Launching the Configuration Wizard" on page 5.

Restoring data to a new server

NOTE
The restore data files must use the exact directory structure as the backup directory structure (refer to "Back up directory structure overview" on page 129).

If your Management application server fails and you must recover information to a new server, restore the data (Refer to "Restoring data" on page 134 for complete instructions).

SAN data collection

NOTE
SAN data collection is only supported on Fabric OS devices.

The Management application uses collectors to gather data from switches, persist the switches in the database, and to publish the collected data to the client. Each collector polls data for one feature area using HTTP or HTTPS (web pages or CAL calls) to communicate with the switch. For a given switch, only one collector runs at a time. When you first discover a switch, all collectors associated with that switch type run to gather data on the switch. After that, the Management application schedules each collector to run independently. Since this is a fairly repetitive task, the Management application has a collection framework which schedules these collectors to run periodically (using lazy polling).

When a data collector fails, the Management application automatically retries the collection after the short tick interval. However, there are two exceptions to this retry rule:

- If collection failure is due to an ACL rule blocking access to the switch, the Management application retries collection after the lazy polling interval (not the short tick interval).
- If collection failure is due to incorrect switch credentials in the Management application, the Management application retries collection three times after which all communication with the switch is stopped to prevent lock out of the Fabric OS user due to too many failed login attempts.

In addition to the automatic collection retry, you can configure adaptive asset collection to trigger specific collectors to run when a particular event occurs. For example, when the Management application receives an SNMP trap that a port has been disabled, the Management application triggers the TopologyCollector (which collects ISL information) and the SwitchAssetCollector to make sure that the client reflects the changes due to the port going down. Adaptive asset collection occurs within the short tick interval.

The Management application uses the short tick interval to ping the switch for a periodic reachability check. If the reachability check succeeds, then the Management application runs pending collectors triggered by an event. When no SNMP traps or syslog events occur, the Management application uses the lazy polling interval to schedule collection of configuration and status changes. The lazy polling interval process schedules any pending collectors for the next short tick. Therefore, the interval between collections when there are no SNMP traps or syslog events is the lazy polling interval plus the short tick interval. To increase polling efficiency, you can configure both the short tick interval (**Check for state change every** option) and the lazy polling interval (**If no state change, poll switch every** option) on the **Options** dialog box. For step-by-step instructions, refer to "Configuring asset polling" on page 168.

There are two types of collectors, fabric-level collectors and switch-level collectors. Fabric-level collectors gather fabric-level information. The Management application collects fabric-level data from the seed switch, for example, the NameServerCollector gathers data about all end devices present in the fabric.

The Management application uses the following Fabric-level collectors:

- DeviceFDMICollector – Collects FDMI-related information for end devices in the fabric.
- NameServerInfoCollector – Collects data about end devices in the fabric.
- ActiveZoneInfoCollector – Collects the active zone configuration in the fabric.
- ZoneInfoCollector – Collects the defined zone configuration in the fabric.
- TopologyCollector – Collects data about the ISLs in the fabric.
- TrunkInfoCollector – Collects data about trunks in the fabric.
- WtJarsCollector – Downloads the jar files needed to launch WebTools from the Management application.

Switch-level collectors gather individual switch-level information (such as, port details and so on). The Management application also uses specialty collectors which run only for switches that have a particular feature. For example the EncryptionBaseCollector only runs for encryption switches. The Management application uses the following Switch-level collectors:

- BottleneckConfigCollector – Collects data about bottleneck configuration on the switch.
- BottleneckStatusCollector – Collects data about the bottleneck status (whether or not a port is bottlenecked) for each port on the switch.
- EncryptionBaseCollector – Collects all encryption related data.
- GroupConfigChangeCollector – Collects encryption data related to HA Cluster, Target Containers, Crypto Host, and Crypto LUN.
- GroupConfigCollector – Collects group member and group collection data.
- FabricCollector – Collects the fabric members (switches) and persists the members in the application. This is the main collector that organizes fabric discovery.
- CeeSwitchCalCollector – Collects the association of a device port to a 10 G physical port on the DCB switch.
- DCBCollector – Collects data specific to the DCB switch.
- FportTrunkCollector – Collects data about F-port trunks present on the switch.
- GigePortCollector – Collects GigE-port data on the switch.
- LicenseCollector – Collects data about licenses on the switch.
- LiteSwitchAssetCollector – Collects the FMS mode setting on the switch.

- SwitchAssetCollector – Collects data about the switch including, inventory details, port level data, any blades that may be present (on directors), AG-port mapping, and auto trace dump settings. This is the major collector for switch data.
- FCIPCollector – Collects FCIP-related data on the older FCIP switches.
- XFCIPCollector – Collects extended FCIP-related data on the newer FCIP switches.
- MapsPolicyCollector – Collects data about MAPS policies configured on the switch.
- MetaSANCollector – Collects data about the IFLs (Inter Fabric Links) on the switch.
- FlowCollector – Collects data about the flow definitions on the switch. Also collects the subflows for each flow definition. This collector requires the Fabric Insight license on the switch.
- VPWwnInfoCollector – Collects data about the VPWWN (Virtual Port World Wide Name) on the switch.

The Management application collects performance monitoring data via SNMP. Performance monitoring data is collected asynchronously and is not affected by the collector scheduling. Performance data (mostly port statistics) is collected every 5 minutes.

Product communication protocols

Table 18 details the protocols that the Management application uses for communication between products and the Management application server.

TABLE 18 Product communication protocols

Protocol	Description	Management application use	Communicates with device type
ICMP	The Internet Control Message Protocol (ICMP) is part of the Internet Protocol Suite, as defined in RFC 792. ICMP messages are typically used for diagnostic or control purposes or generated in response to errors in IP operations.	Used during initial discovery. For IronWare devices, used for every subsequent polling cycle. You can edit the IronWare polling interval on the **Options** dialog box (refer to "Configuring polling service preferences" on page 163).	Fabric OS IronWare Network OS
SNMP	Simple Network Management Protocol (SNMP) is an internet-standard protocol for managing devices on IP networks. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.	Used during discovery, performance polling, and operation status polling. You can edit the IronWare operating polling interval on the **Options** dialog box (refer to "Configuring polling service preferences" on page 163). Note that performance polling (including data collection for dashboards) completely relies on SNMP. For Historical data collection, the minimum time interval is 1 minute for IronWare and Network OS devices and 5 minutes for Fabric OS devices. For real time graphs, the minimum time interval is 10 seconds.	Fabric OS IronWare Network OS

TABLE 18 Product communication protocols

Protocol	Description	Management application use	Communicates with device type
NETCONF	The Network Configuration Protocol (NETCONF), is an IETF network management protocol. NETCONF provides mechanisms to install, manipulate, and delete the configuration of network devices. Its operations are realized on top of a simple Remote Procedure Call (RPC) layer. The NETCONF protocol uses an Extensible Markup Language (XML) based data encoding for the configuration data as well as the protocol messages. The protocol messages are exchanged on top of a secure transport protocol..	Used to discover all the information on VDX including Device, Ports, Zoning details and so on. Also used for configuring various parameters to VDX devices.	Network OS
HTTP/HTTPS	The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. Hypertext Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.	Used to collect all information required to manage Fabric OS devices. Used to launch web element manager for IronWare devices. You can configure the HTTP/HTTPS protocol from the **Options** dialog box (refer to "Product communication settings" on page 169).	Fabric OS IronWare
SSH/Telnet	Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers that connects, via a secure channel over an insecure network, a server and a client. Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).	Used to send configurations to IronWare devices. For Network OS and IronWare products, used to deploy CLI templates created through the CLI Configuration Manager. You can configure this protocol on the Options dialog box (refer to "Configuring IP communication" on page 171.	IronWare Network OS
FTP	File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host to another host over a TCP-based network	Used for firmware download. For Fabric OS and Network OS devices, used to collect technical support information. For Network OS devices, used for configuration management (backup and restore). For more information, refer to "FTP/SCP/SFTP server settings" on page 172.	Fabric OS Network OS

TABLE 18 Product communication protocols

Protocol	Description	Management application use	Communicates with device type
SCP	Secure copy (SCP) is a means of securely transferring computer files between a local host and a remote host or between two remote hosts. It is based on the Secure Shell (SSH) protocol.	Used for firmware download. For Fabric OS and Network OS devices, used to collect technical support information. For Network OS devices, used for configuration management (backup and restore). For more information, refer to "FTP/SCP/SFTP server settings" on page 172.	Fabric OS IronWare Network OS
SFTP	Secure File Transfer Protocol (SFTP) or SSH File Transfer Protocol is a network protocol that provides file access, file transfer, and file managementfunctionalities over any reliable data stream.	Used for firmware download. For Fabric OS and Network OS devices, used to collect technical support information. For Network OS devices, used for configuration management (backup and restore). For more information, refer to "FTP/SCP/SFTP server settings" on page 172.	Fabric OS Network OS

Event storage settings

You can configure the maximum number of historical events save to the repository, how long the events will be retained, as well as whether to store historical events to a file before purging them from the repository.

Configuring event storage

To configure event storage, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Event Storage** in the **Category** list (Figure 56).

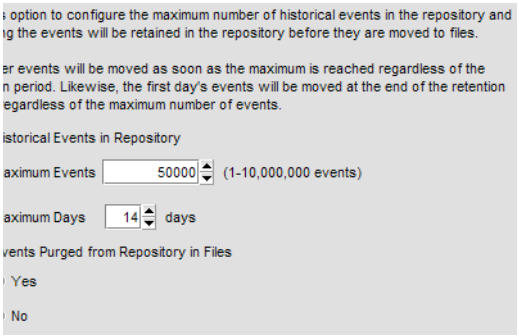


FIGURE 56 Options dialog box (Event Storage pane)

3. Enter the maximum number of events you want to be retained in the repository in the **Maximum Events** field.

   Depending on your installation, the maximum number of events stored are as follows:

- Professional — 1 through 100,000
- Enterprise — 1 through 10,000,000

Default is 50,000. Older events are purged at midnight on the date the maximum event limit is reached regardless of the retention days.

4. Enter then number of days (1 through 365) you want to store events in the **Maximum Days** field.

   The events are purged at midnight on the last day of the retention period regardless of the number of maximum events.

5. Choose one of the following options:
   - Select the **Yes** option to store all historical events from the repository to a file while purging occurs.
   - Select the **No** option to purge historical events from the repository without storing them as a file.
6. Click **OK**.

Storing historical events purged from repository

To store historical events purged from the repository, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Event Storage** in the **Category** list.
3. Select the **Yes** option.
4. Click **OK**.

   Purged events from the master log table are stored in the *Install_Home*\data\archive\events directory using the format event_*MMDDYYY*.zip (for example, event_04052011.zip. These files are retained for a maximum of 30 days. The zip file contains multiple archive text files that use the format event_*MMDDYYY_N*.txt (for example, event_04052011_1.txt).

Flyover settings

You can configure your system to display information for products and connections in a pop-up window on the Connectivity Map.

Configuring flyovers

To display product and connection information in a pop-up window, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Flyovers** in the **Category** list.

3. Select the **Enable flyover display** check box to enable flyover display on your system.
4. Select the **Include labels** check box to include labels on flyover displays.
5. Add product properties you want to display on flyover by selecting the **Product** tab (Figure 57) and completing the following steps.

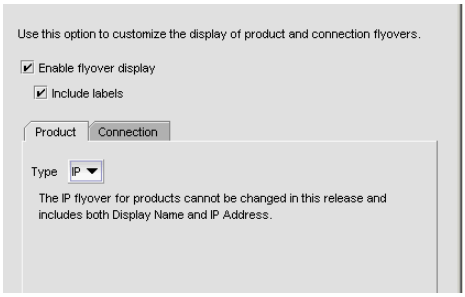


FIGURE 57 Options dialog box (Flyovers pane, Product tab)

   a. Select the protocol type from the **Type** list, if necessary.
   b. Select each property you want to display in the product flyover from the **Available Properties** table.

      Depending on which protocol you select, some of the following properties may not be available:

      IP

- Display Name
- IP Address
- Status

   c. Click the right arrow to move the selected properties to the **Selected Properties** table.
   d. Use the **Move Up** and **Move Down** buttons to reorder the properties in the **Selected Properties** table, if necessary.

      The properties displayed in the **Selected Properties** table appear in the flyover display.

6. Remove product properties you do not want to display on flyover by selecting the property in the **Selected Properties** table and clicking the left arrow.
7. Add connection properties you want to display on flyover by selecting the **Connection** tab (Figure 58) and completing the following steps.

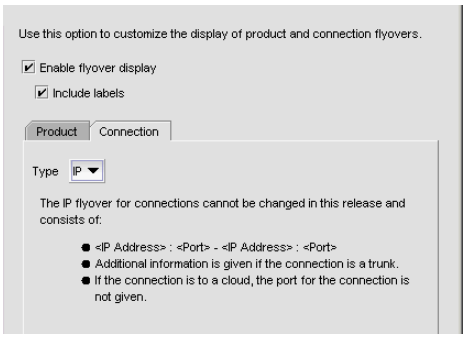


FIGURE 58 Options dialog box (Flyovers pane, Connection tab)

a. Select the protocol type from the **Type** list, if necessary.

   Depending on which protocol you select, some properties may not be available for all protocols.

b. Select each property you want to display in the connection flyover from the **Available Properties** table.

   Depending on which protocol you select, some of the following properties may not be available for all protocols:

   IP

   - *IP_Address:Port-IP_Address:Port*

c. Click the right arrow to move the selected properties to the **Selected Properties** table.

d. Use the **Move Up** and **Move Down** buttons to reorder the properties in the **Selected Properties** table.

   The properties displayed in the **Selected Properties** table appear in the flyover display.

8. Remove connection properties you do not want to display on flyover by selecting the property in the **Selected Properties** table and clicking the left arrow.
9. Click **Apply** or **OK** to save your work.

Turning flyovers on or off

Flyovers display when you place the cursor on a product. They provide a quick way to view a product's properties.

To turn flyovers on or off, select **Enable Flyover Display** from the **View** menu.

Viewing flyovers

On the Topology Map, rest the pointer over a product icon, port, or connection.

The pop-up window containing the product, port, or connection information displays.

For the product icon, the pop-up window displays the display name and IP address of the device.

For the connection, the pop-up window displays the IP address and port number for each device at either end of the connection. If one of the connections is a cloud, the port number does not display.

Name settings

You can use Names as a method of providing familiar simple names to products and ports in your SAN. Using your Management application you can:

- Set names to be unique or non-unique.
- Fix duplicate names.
- Associate a name with a product, port WWN, or Fabric Assigned WWN currently being discovered.
- Add a WWN and an associated name for a product or port that is not yet being discovered.
- Remove or disassociate a name from a WWN.

Fixing duplicate names

To fix duplicated names, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Click **Fix Duplicates**.

   The **Duplicated Names** dialog box displays (Figure 59).

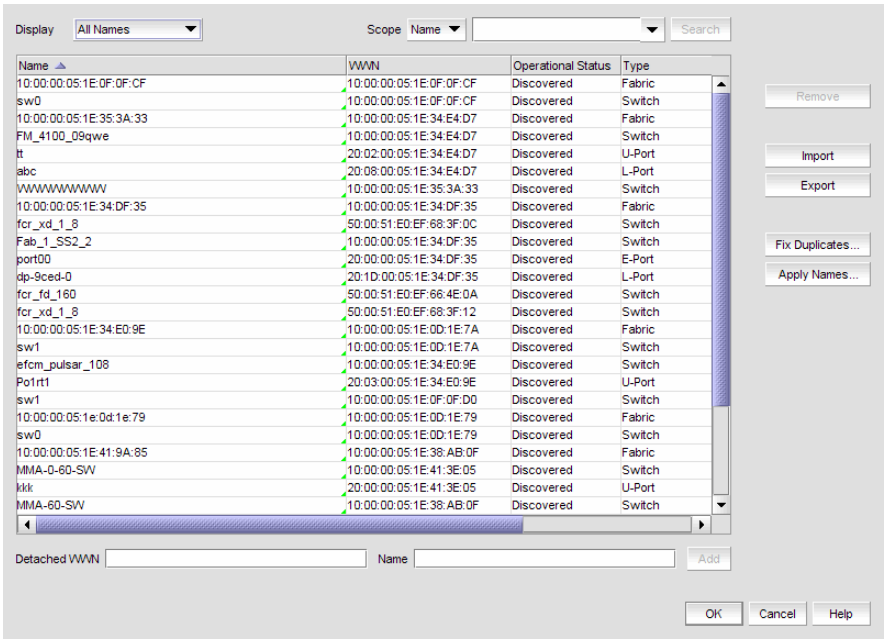


FIGURE 59 Duplicated Names dialog box

The **Duplicated Names** dialog box contains the following information:

- **Description** — A description of the device.
- **Duplicate Names** table — Every instance of duplicate names.
  - **Fabric** — The fabric name.
  - **FC Address** — The Fibre Channel address.
  - **Names** — The current name of the device.
    If you selected the **Append Incremental numbers for all repetitive names** option, the names display with the incremental numbering.
    If you selected the **I will fix them myself** option, this field becomes editable.
  - **Operational Status** — The operational status of the device. There are four possible values:
    - Up — Operation is normal.
    - Down — The port is down or the route to the remote destination is disabled.
    - Disabled — The connection has been manually disabled.
    - Backup Active — The backup TCP port is active due to a failover.
  - **Port #** — The port number.
  - **Type** — The type of device.

3. Select one of the following options.
   - If you select **Append Incremental numbers for all repetitive names**, the names are edited automatically using incremental numbering.
   - If you select **I will fix them myself**, edit the name in the **Name** field.
4. Click **OK** on the **Duplicated Names** dialog box.
5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

Viewing names

To view names associated with devices, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays (Figure 60).

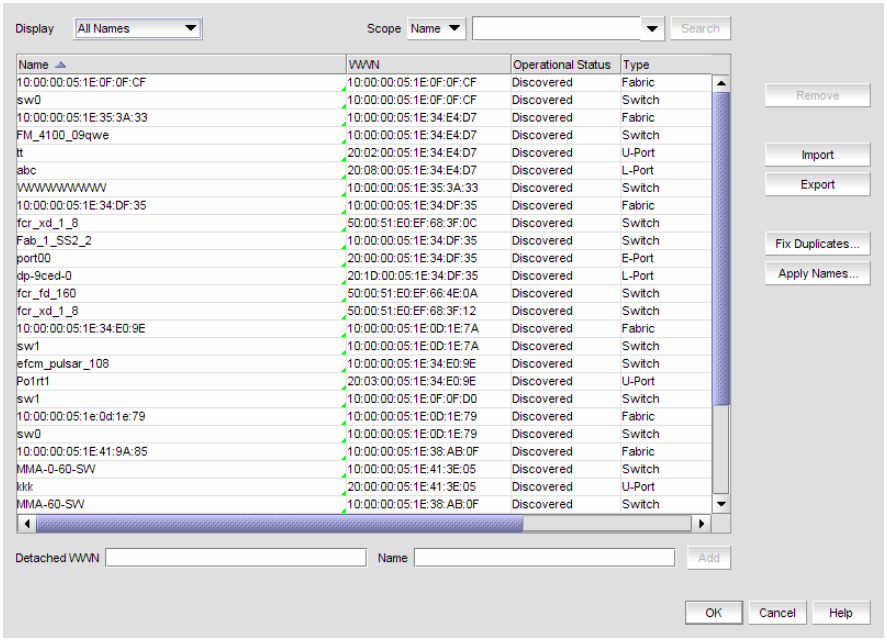


FIGURE 60 Configure Names dialog box

2. Select **All Names** from the **Display** list.

   Only devices with a name display. The table displays the following information.
   - **Scope** list — Select a search value (Name or WWN) from the list.
   - **Search text box** — Enter the name or WWN of the device for which you are searching.
   - **Search** button — Click to search on the value in the Search field. For more information, refer to "Searching for a device by name" on page 148.

- **Display** table — This table displays the following information:
  - **Description**–A description of the device.
  - **Name**–The name of the device. Enter a name for the device.
  - **Operational Status**–The operational status of the device (discovered, operational, and unknown).
  - **Type**–The type of device (port, node, Fabric Assigned WWN, and unknown).
  - **WWN**–The world wide node (WWN) of the device. Enter a WWN for the device. Click a column head to sort the list. Click a column head again to reverse the sort order.
- **Remove** button — Click to remove a device from the Display table. For more information, refer to "Removing a name from a device" on page 147.
- **Import** button — Click to import name data. For more information, refer to "Importing Names" on page 148.
- **Export** button — Click to export the name data. Depending on your operating system, the default export location are as follows:
  - Desktop\My documents (Windows)
  - \root (Linux)

  For more information, refer to "Exporting names" on page 147.
- **Fix Duplicates** button — Click to launch the Fix Duplicates dialog box. For more information, refer to "Fixing duplicate names" on page 143.
- **Apply Names** button — Click to apply unassigned (detached) names to newly discovered devices. For more information, refer to "Applying a name to a detached WWN" on page 146.
- **Detached WWN text box —** Enter the WWN of the device you want to add.
- **Name text box —** Enter a name for the device you want to add.
- **Add** button — Click to add a device by detached WWN and Name to the table. For more information, refer to "Adding a name to a new device" on page 146.

3. Click **OK** to close the **Configure Names** dialog box.

Adding a name to an existing device

To add a name to an existing device, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Select how you want to display devices from the **Display** list.

   You can display devices by **All Names**, **All WWNs**, **Fabric Assigned WWNs**, **Only Fabrics**, **Only Products**, **Only Ports**, or **Switch and N Ports**.

   All discovered devices display.

3. Select the device to which you want to assign a name in the **Display** table.
4. Double-click in the **Name** column for the selected device or port and enter a name for the device or port.

If you set names to be unique on the **Options** dialog box and the name you entered already exists, the entry is not accepted. To search for the device already using the name, refer to "Searching for a device by name" on page 148 or "Searching for a device by WWN" on page 149 in the **Configure Names** dialog box or "Searching for a device" on page 299 in the connectivity map.

NOTE
If you segment a fabric, the Fabric's name follows the assigned principal switch.

5. Click **OK** on the confirmation message.
6. Click **OK** to close the **Configure Names** dialog box.

Adding a name to a new device

To add a new device and name it, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.
2. Enter the WWN of the device in the **Detached WWN** field.
3. Enter a name for the device in the **Name** field.
4. Click **Add**.

   The new device displays in the table.

   If you set names to be unique on the **Options** dialog box and the name you entered already exists, a message indicating the name already in use displays. Click **OK** to close the message and change the name.
5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

Applying a name to a detached WWN

To apply a name to a detached wwn, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.
2. Click **Apply Names**.

   If there are any detached WWNs in a discovered state, the **Apply Names** dialog box displays.
3. Select or clear the check box for the associated switch or switch port.

   Select a check box to apply the detached name as the switch or switch port name and remove the duplicated WWN entry (detached) in the **Configure Names** dialog box.

   Clear a check box to remove the duplicated WWN entry (detached) in the **Configure Names** dialog box.
4. Click **OK** on the **Apply Names** dialog box.
5. Click **OK** on the **Configure Names** dialog box.

Removing a name from a device

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. In the **Display** table, select the name you want to remove.
3. Click **Remove**.

   An application message displays asking if you are sure you want clear the selected name.

4. Click **Yes**.
5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

Editing names

To edit the name associated with a device, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Select **All Names** from the **Display** list.

   Only devices with a name display. The table displays the Name, WWN, Operational Status, Type, and a Description of the device.

3. Click the name you want to edit in the **Name** column.
4. Edit the name and press **Enter**.
5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

Exporting names

To export the names associated with devices, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Click **Export.**

   The **Export Files** dialog displays.

3. Browse to the location where you want to save the export file.

   Depending on your operating system, the default export location are as follows:

   - Desktop\My documents (Windows)
   - \root (Linux)

4. Enter a name for the file and click **Save.**
5. Click **OK** to close the **Configure Names** dialog box.

Importing Names

If the name length exceeds the limitations detailed in the following table, you must edit the name (in the CSV file) before import. Names that exceed these limits will not be imported. If you migrated from a previous version, the .properties file is located in the *Install_Home*\migration\data folder.

TABLE 19

Device	Character limit
Fabric OS switch 6.2 or later	30 (24 character limit when in FICON mode)
Fabric OS switch 6.1.X or earlier	15
Fabric OS switch port 7.0 or later	128 (24 character limit when in FICON mode)
Fabric OS switch port 6.4.X or earlier	32 (24 character limit when in FICON mode)
HBA	256
HBA port	256
Others names	128

To import names, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Click **Import.**

   The **Import Files** dialog displays.

3. Browse to the import (.csv) file location.
4. Select the file and click **Import.**
5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

Searching for a device by name

You can search for objects (switch, fabric, product, ports, or N Ports) by name. To search for a name in the Connectivity Map, refer to "Searching for a device" on page 299.

To search by name, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Select **All Names** from the **Display** list.
3. Select **Name** from the **Scope** list.
4. Enter the name you want to search for in the **Search** field.

   You can search on partial names.

NOTE
To search for a device, the device must be discovered and display in the topology.

5. Click **Search**.

   All devices with the specified name (or partial name) are highlighted in the **Display** table. You may need to scroll to see all highlighted names.

   If the search finds no devices, a 'no item found' message displays.

6. Click **OK** to close the **Configure Names** dialog box.

Searching for a device by WWN

You can search for objects (switch, fabric, product, ports, or N Ports) by WWN (world wide name). To search for a WWN in the Connectivity Map, refer to "Searching for a device" on page 299.

To search by WWN, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Select **All Names** from the **Display** list.

3. Select **WWN** from the **Scope** list.

4. Enter the WWN you want to search for in the **Search** field.

   You can search on partial WWNs.

   NOTE
   To search for a device, the device must be discovered and display in the topology.

5. Click **Search**.

   All devices with the specified WWN (or partial WWN) are highlighted in the **Display** table. You may need to scroll to see all highlighted WWNs.

   If the search finds no devices, a 'no item found' message displays.

6. Click **OK** to close the **Configure Names** dialog box.

Miscellaneous security settings

You can configure the Server Name, login banner, modify whether or not to allow clients to save passwords, and modify whether or not to enforce the MD5 checksum during import. When the login banner is enabled, each time a client connects to the server, the login banner displays with a legal notice provided by you. The client's users must acknowledge the login banner to proceed, otherwise they are logged out.

NOTE
M-EOS device support is no longer available in the Management application; therefore, the **CHAP Secret** and **Retype Secret** fields are no longer required.

Configuring the server name

To configure the server name, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Security Misc** in the **Category** list.

   The **Security Misc** pane displays (Figure 61).

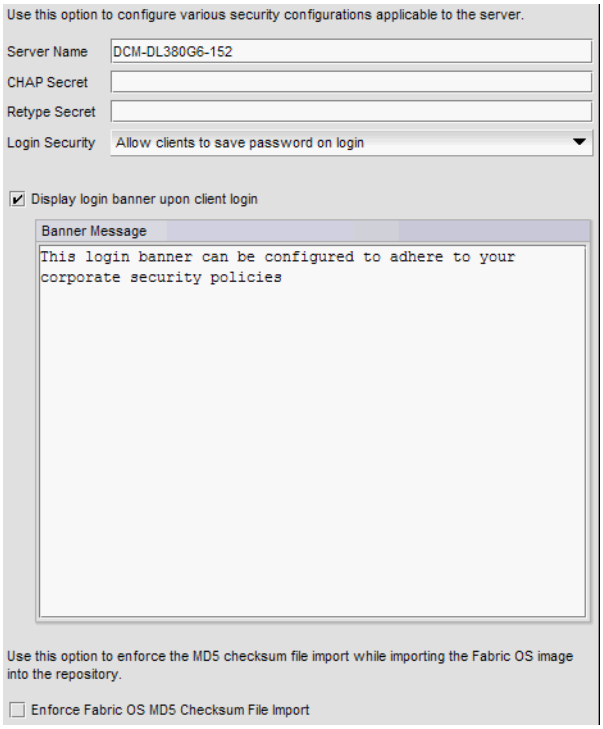


FIGURE 61 Options dialog box (Security Misc pane)

3. Enter the server name in the **Server Name** field.

   The **Server Name** field cannot be empty.

4. Click **OK** on the confirmation message.
5. Click **Apply** or **OK** to save your work.

Configuring login security

To configure login security, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Security Misc** in the **Category** list.
3. Choose one of the following options:

- To allow users to save their password in the **Login Security** list, select **Allow clients to save password on login**.
- To not allow users to save their password in the **Login Security** list, select **Do NOT allow clients to save password on login**.

4. Click **Apply** or **OK** to save your work.

Configuring the login banner display

To configure the login banner display, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Security Misc** in the **Category** list.
3. Select the **Display login banner upon client login** check box.
4. Enter the message you want to display every time a user logs into this server in the **Banner Message** field.

   This field contains a maximum of 2048 characters.

5. Click **Apply** or **OK** to save your work.

Disabling the login banner

To disable the login banner display, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Security Misc** in the **Category** list.
3. Clear the **Display login banner upon client login** check box.

   NOTE
   Users logging into the client will not see the banner when logging in to this Server.

4. Click **Yes** on the confirmation message.
5. Click **Apply** or **OK** to save your work.

Syslog Registration settings

You can automatically register the server as the syslog recipient on products.

Registering a server as a Syslog recipient automatically

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Syslog Registration** in the Category pane.

The **Syslog Registration** pane displays (Figure 62).

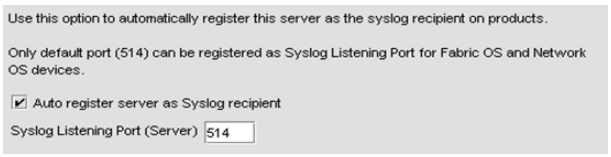


FIGURE 62 Options dialog box (Syslog Registration pane)

3. Select the **Auto register server as Syslog recipient** check box, if necessary.

   This check box is selected by default.

4. Click **Apply** or **OK** to save your work.

Configuring the Syslog listing port number

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Syslog Registration** in the Category pane.

   The **Syslog Registration** pane displays (Figure 62).

3. Enter the Syslog listening port number of the Server in the **Syslog Listening Port (Server)** field, if necessary.

   The default Syslog listening port number is 514 and is automatically populated.

   For Network OS devices, only the default port (514) can be registered as the Syslog Listening Port.

4. Click **Apply** or **OK** to save your work.

SNMP Trap Registration settings

You can automatically register the server as the trap recipient on products. If SAN products have Informs enabled, the registration is for the Informs.

Registering a server as a SNMP trap recipient automatically

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Trap Registration** in the Category pane.

   The **Trap Registration** pane displays (Figure 63).

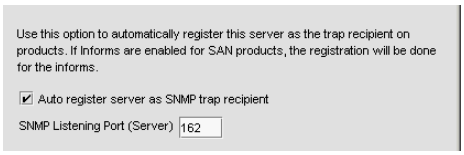


FIGURE 63 Options dialog box (Trap Registration pane)

3. Select the **Auto register server as SNMP trap or informs recipient** check box, if necessary.

   This check box is selected by default.

4. Click **Apply** or **OK** to save your work.

Configuring the SNMP trap listing port number

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Trap Registration** in the Category pane.
3. Enter the SNMP listening port number of the Server in the **SNMP Listening Port (Server)** field, if necessary.

   The default SNMP listening port number is 162 and is automatically populated.

4. Click **Apply** or **OK** to save your work.

SNMP Trap forwarding credential settings

You can configure SNMP credentials for the traps forwarded by the server.

Configuring SNMP v1 and v2c credentials

To configure a SNMP v1 or v2c credentials, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Trap Forwarding Credentials** in the Category pane.

   The **Trap Forwarding Credentials** pane displays (Figure 64).

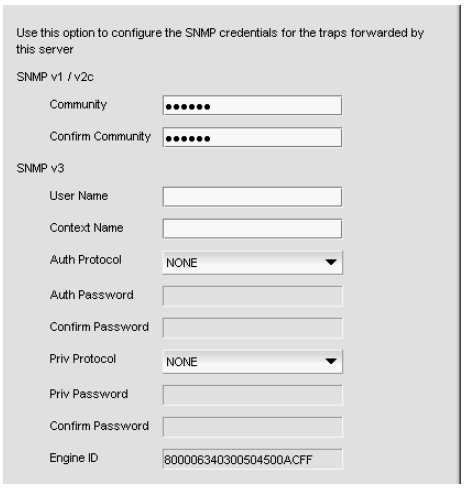


FIGURE 64 Options dialog box (Trap Forwarding Credentials pane)

3. Enter the unique community string (case sensitive, 1 to 16 characters). in the **Community** and **Confirm Community** fields.

   Displays as asterisks. Allows all printable ASCII characters.

4. Click **Apply** or **OK** to save your work.

Configuring SNMP v3 credentials

To configure a SNMP v1 or v2c credentials, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Trap Forwarding Credentials** in the Category pane.

   The **Trap Forwarding Credentials** pane displays (Figure 64).

3. Enter the SNMP v3 name (case sensitive, 1 to 16 characters) to identify the credentials in the **User Name** field.

   Allows all printable ASCII characters.

4. Select on of the following authentication protocols from the **Auth Protocol** list.

   - HMAC_MD5 (continue with step 5)
   - HMAC_SHA (continue with step 5)
   - NONE (go to step 6)

5. Enter the SNMP v3 authentication password (case sensitive, 1 to 16 characters) in the **Auth Password** and **Confirm Password** fields.

   Displays as asterisks. Allows all printable ASCII characters.

6. Select one of the following privacy protocol types from the **Priv Protocol** list.

   - CBC-DES (continue with step 7)
   - CFB_AES-128 (continue with step 7)

- NONE (go to step 8)

7. Enter the privacy password (case sensitive, 8 to 16 characters) in the **Priv Password** and **Confirm Password** fields.

   Displays as asterisks. Allows all printable ASCII characters.

8. Click **Apply** or **OK** to save your work.

Software Configuration

The Management application allows you to configure the following software settings:

- Client/Server IP — IP configuration settings.
- IP preferences — IP settings specific to IP product managemental.
- Memory allocation settings — Memory allocation for the client and server.
- Product communication settings — Connections between the server and SAN switches or IP products.
- FTP/SCP/SFTP server settings — Internal or external FTP or SCP server settings.
- Server port settings — Server port settings.
- Support mode settings — Support settings to allow enhanced diagnostics.

Client/Server IP

You can configure connections between the client or switches and the Management application server.

Configuring the server IP address

If your Operating System is IPv4-enabled or IPv6-enabled (running in dual mode), the server binds using an IPv4 address. IPv6 only mode does not support server to client communication (the IPv6 address cannot be bound to the server).

NOTE
If the Management server or client has multiple Network Interface Cards and if any of these interfaces are not plugged in, you must disable them; otherwise, the following features do not work properly:

Server impact

- Configuration wizard (does not display all IP addresses)
- Trap and Syslog auto registration
- Report content (Ipconfiguration element does not display all server IP addresses)
- Network OS configuration backup through FTP
- Trace dump through FTP

Client impact

- Options dialog box (does not display all IP addresses)
- Firmware import and download dialog box

- Firmware import for Fabric OS and Network OS products
- FTP button in Technical Support Repository dialog box
- Technical supportSave of Fabric OS, Network OS, and Host products through FTP

To configure the IP address used by the server for client-server communications, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Client/Server IP** in the **Category** list to set the IP address.

   The **Client/Server IP** pane displays (Figure 65).

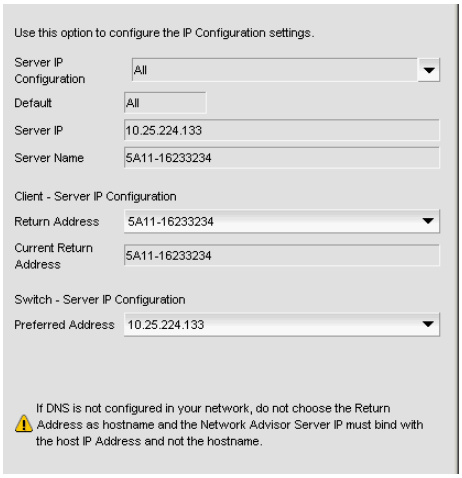


FIGURE 65 Options dialog box (Client/Server IP option)

3. Choose one of the following options in the **Server IP Configuration** list.
   - Select **All**. Go to step 4.
   - Select a specific IP address. Continue with step 5.
   - Select **localhost**. Continue with step 5.

   When **Server IP Configuration** is set to **All**, you can select any available IP address as the **Return Address**. If you select a specific IP address, the **Return Address** list shows the same IP address and you cannot change it.

4. Select the return IP address in the **Client - Server IP Configuration Return Address** list.
5. Select the preferred IP address in the **Switch - Server IP Configuration Preferred Address** list.

   If DNS is not configured for your network, do not select the 'hostname' option from either the **Return Address** or **Preferred Address** list. Selecting the 'hostname' option prevents clients and devices from communicating with the Server.

6. Click **Apply** or **OK** to save your work.

NOTE
Changes to this option take effect after an application restart.

NOTE
You can only restart the server using the Server Management Console (**Start > Programs >** *Management_Application_Name* **12.X.X > Server Management Console**).

7. Click **OK** on the "changes take effect after application restart" message.

Configuring an explicit server IP address

If you selected a specific IP address from the **Server IP Configuration** screen during installation and the selected IP address changes, you will not be able to connect to the server. To connect to the new IP address, you must manually update the IP address information.

To change the IP address, complete the following steps.

1. Choose one of the following options:
   - On Windows systems, select **Start > Programs >** *Management_Application* **12.X.X >** *Management_Application* **Configuration**.
   - On UNIX systems, execute `sh` *`Install_Home`*`/bin/configwizard` on the terminal.
2. Click **Next** on the **Welcome** screen.
3. Click **Yes** on the confirmation message.
4. Click **Next** on the **FTP Server** screen.
5. Complete the following steps on the **Server IP Configuration** screen (Figure 66).

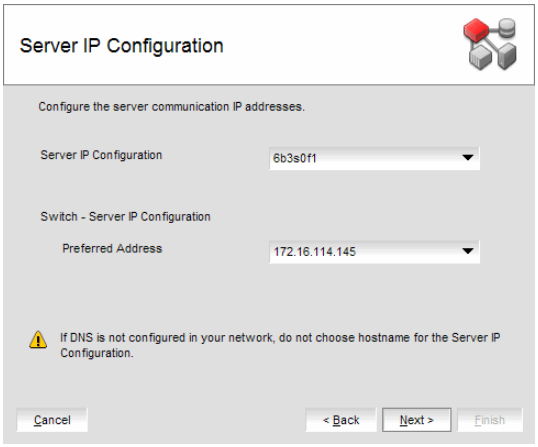


FIGURE 66 Server IP Configuration screen

   a. Select an address from the **Server IP Configuration** list.
   b. Select an address from the **Switch - Server IP Configuration Preferred Address** list.

NOTE
If the "hostname" contains invalid characters, the host name does not display in the list. Valid characters include alphanumeric and dash (-) characters. The IP address is selected by default. If the an IPv6 address is selected, server start up will fail.

If DNS is not configured for your network, do not select the 'hostname' option from either the **Server IP Configuration** or **Switch - Server IP Configuration Preferred Address** list. Selecting the 'hostname' option prevents clients and devices from communicating with the Server.

c. Click **Next**.

6. Click **Next** on the **Server Configuration** screen.
7. Click **Next** on the **SMI Agent Configuration** screen.
8. Verify the IP address on the **Server Configuration Summary** screen and click **Next**.
9. Click **Finish** on the **Start Server** screen.
10. Click **Yes** on the restart server confirmation message.
11. Choose one of the following options:
    - If you configured authentication to CAC, enter your PIN in the CAC PIN field.
    - If you configured authentication to the local database, an external server (RADIUS, LDAP, or TACACS+), or a switch, enter your user name and password.

      The defaults are **Administrator** and **password**, respectively.

      NOTE
      Do not enter *Domain\User_Name* in the **User ID** field for LDAP server authentication.
12. Click **Login**.
13. Click **OK** on the **Login Banner**.

Configuring the application to use dual network cards

Issues with Client-to-Server connectivity can be due to different reasons. Some examples are:

- The computer running the Server has more than one network interface card (NIC) installed.
- The computer running the Server is behind a firewall that performs network address translation.

To make sure that Clients can connect to the Server, you may need to edit the IP configuration setting in the **Options** dialog to manually specify the IP address that the Server should use to communicate to its Clients.

NOTE
If your Operating System is IPv4-enabled or IPv6-enabled (dual mode), the server binds using IPv4 address by default.

NOTE
IPv6 only mode does not support server to client communication (the IPv6 address cannot be bound to the server).

To configure the IP address to override the default RMI server host IP address, complete the following steps.

NOTE
This configuration option replaces the -Djava.rmi.server.hostname value used in previous releases.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Client/Server IP** in the **Category** list to set the IP address.

3. Choose one of the following options in the **Server IP Configuration** list.

   - Select **All**. Go to step 4.
   - Select a specific IP address. Continue with step 5.
   - Select **localhost**. Continue with step 5.

4. Select the return IP address in the **Client - Server IP Configuration Return Address** list.

   When **Server IP Configuration** is set to **All**, you can select any available IP address as the **Return Address**. If you select a specific IP address, the **Return Address** field shows the same IP address and you cannot change it.

5. Click **Apply** or **OK** to save your work.

   NOTE
   Changes take effect after you restart the Management Server.

   NOTE
   You can only restart the server using the Server Management Console (**Start > Programs >** *Management_Application_Name* **12.X.X > Server Management Console**).

6. Click **OK** on the "changes take effect after "application restart" message.

IP preferences

You can configure the following preferences for IP products.

Configuring change manager preferences

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **IP Preferences from the Software Configurations list** in the **Category** pane.

   The **IP Preferences** pane displays (Figure 67).

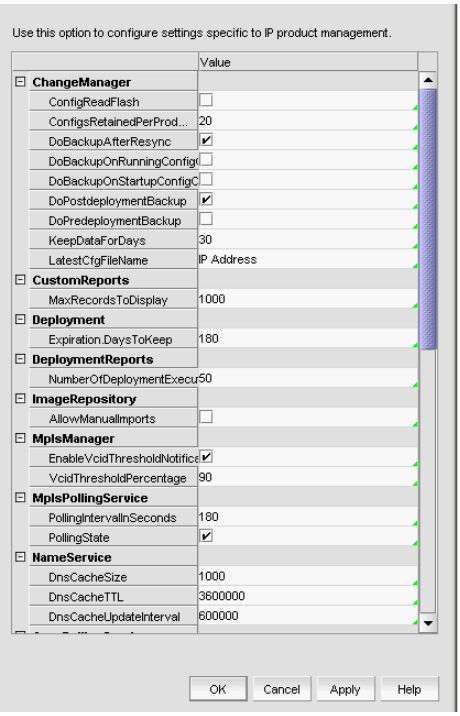


FIGURE 67 Options dialog box (IP Preferences pane)

3. Select the **ConfigReadFlash** check box to obtain configuration back up from flash.

   Clear to obtain configuration back up from DRAM. Default is clear (disabled).

4. Enter the number of configurations to retain per product in the **ConfigsRetainedPerProduct** field.

   Default is 20. Maximum is 30. Minimum is 5. When the system reaches the maximum limit for a product, the oldest configuration is deleted and the new configuration is saved. However, if a Baselined configuration becomes the oldest configuration, the baselined configuration is retained.

5. Select the **DoBackupAfterResync** check box to turn on product configuration backup after re-synch is performed from the client.

6. Select the **DoBackupOnRunningConfigChangeTrap** check box to turn on product configuration backup after receiving a running configuration change trap.

7. Select the **DoBackupOnStartupConfigChangeTrap** check box to turn on product configuration backup after receiving a startup configuration change trap.

8. Select the **DoPostdeploymentBackup** check box to turn on product configuration backup after a payload is deployed using the Configuration Wizard.
9. Select the **DoPredeploymentBackup** check box to turn on product configuration backup before a payload is deployed using the Configuration Wizard.
10. Enter the number of days to keep product configuration backup files on the server in the **KeepDataForDays** field.

    Minimum duration is 7 days. Maximum duration is 365. Default is 30.

    Reducing this parameter may result in expiring a large number of records on server restart and lead to reduced performance. If millions of records are impacted, this might last several hours.
11. Click **Apply** or **OK** to save your work.

Configuring custom report preferences

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **IP Preferences from the Software Configurations list** in the **Category** pane.
3. Enter the maximum number of records to display in HTML Reports in the **MaxRecordsToDisplay** field.

   By default, 1000 records display, even if the event count is greater than 1000. You can enter a value of from 10 (minimum) through 2000 (maximum) records.
4. Enter the maximum number of records to obtain from the database in the **MaxRecordsToFromDatabase** field.
5. Click **Apply** or **OK** to save your work.

Configuring deployment preferences

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **IP Preferences from the Software Configurations list** in the **Category** pane.
3. Enter the number of days to retain deployment records in the **Expiration.DaysToKeep** field.

   Minimum is 1. Maximum is 366. Default is 180.
4. Click **Apply** or **OK** to save your work.

Configuring deployment report preferences

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **IP Preferences from the Software Configurations list** in the **Category** pane.
3. Enter the number of Deployment Executions to show in a Deployment Report in the **NumberOfDeploymentExecutionsToDisplay** field.

   Minimum is 10. Maximum is 10000. Default is 50.

4. Click **Apply** or **OK** to save your work.

Configuring IP device manager preferences

This configuration is only applicable to the Ethernet router series switch running firmware version 5.4 or later.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **IP Preferences from the Software Configurations list** in the **Category** pane.
3. Enter the number of Element Managers that can be launched from the Management application in the **LaunchLimitforElementManagerGUI** field.

   The default is 4. The minimum is 1. The maximum is 6.

4. Click **Apply** or **OK** to save your work.

Configuring image repository preferences

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **IP Preferences from the Software Configurations list** in the **Category** pane.
3. Select the **AllowManualImports** check box to turn on launching the Manual Image Import dialog box when you select an image that is not recognized as valid image format.
4. Click **Apply** or **OK** to save your work.

Configuring MPLS management preferences

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **IP Preferences from the Software Configurations list** in the **Category** pane.
3. Select the **EnableVcidThresholdNotification** check box to enable notification when the VCID pool usage crosses a threshold.
4. Enter a threshold percentage for the VCIDs pool usage in the **VcidThresholdPercentage** field.

   Once this threshold is reached, a trap is generated to notify you that the VCID pool is running out of IDs.

5. Click **Apply** or **OK** to save your work.

Configuring MPLS polling service preferences

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **IP Preferences from the Software Configurations list** in the **Category** pane.
3. Enter the frequency of MPLS polling in the **PollingIntervalInSeconds** field.

   Default is 180 seconds.

4. Select the **PollingState** check box to enable MPLS polling.
5. Click **Apply** or **OK** to save your work.

Configuring name service preferences

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **IP Preferences from the Software Configurations list** in the **Category** pane.
3. Enter the maximum cache size for the DNS Lookup Manager in the **DnsCacheSize** field.
4. Enter the time (in milliseconds) for the DNS cache to stay in the cache without being accessed in the **DnsCacheTTL** field.
5. Enter the time (in milliseconds) interval between each DNS Cache refresh in the **DnsCacheUpdateInterval** field.
6. Click **Apply** or **OK** to save your work.

Configuring polling service preferences

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **IP Preferences from the Software Configurations list** in the **Category** pane.
3. Select the **EnablePingsForSwitches** check box to enable Ping for wired IP devices.
4. Enter the polling interval in seconds in the **PollingIntervalInSeconds** field.
5. Select the **PollingState** check box to enable the polling state for IP device health.
6. Click **Apply** or **OK** to save your work.

Configuring sFlow accounting preferences

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **IP Preferences from the Software Configurations list** in the **Category** pane.
3. Select the **LogReportsToFile** check box to enable sFlow accounting log reports to file.
4. Enter the maximum number of rows to display in the log report in the **MaxRowsToShow** field.

   Default is 200.
5. Click **Apply** or **OK** to save your work.

Configuring sFlow data collector preferences

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **IP Preferences from the Software Configurations list** in the **Category** pane.

3. Select the **EnableReverseDNSLookup** check box to enable reverse DNS Look up on the L3/L4 IP Address so that the host name is displayed together with the IP Address.
4. Enter the number of days to retain the SFlow hourly data in the **KeepDataForDays** field.

   Minimum duration is 7 days. Maximum duration is 65 days. Reducing this parameter may result in expiring a large number of records on server restart and lead to reduced performance. If millions of records are impacted, this might last several hours.
5. Select the **ProcessTCPFlagsData** check box to monitor TCP traffic.
6. Enter the port number for the SFlow data collector in the **ReceiveSFlowPktsOnPortNum** field.
7. Click **Apply** or **OK** to save your work.

Configuring sFlow monitoring preferences

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **IP Preferences from the Software Configurations list** in the **Category** pane.
3. Enter a list of IP ports for which the application treats the port used for the opposite side of the connection as 'ephemeral' (shown in reports as 'various') in the **IPPortsForEphemeralWatch** field.

   For example: FTP-DATA=20, FTP=21, SSH=22, TELNET=23, SMTP=25, DNS=53, HTTP=80, POP2=109, POP3=110, NNTP=119, IMAP4=143, SNMP=161, SSL=443.
4. Enter the maximum pairs to be displayed in the report table in the **MaxPairsToShow** field.
5. Enter the maximum number of rows to be displayed in the report table in the **MaxRowsToShow** field.
6. Enter the monitoring chart auto refresh rate in minutes in the **RefreshRate** field.
7. Enter two control bits separated by a hyphen (for example, FIN-SYN) to define an invalid combination in the **TCPFlags_InvalidCombos** field.

   To enter multiple combinations, separate them with commas (for example, FIN-SYN, ACK-RST). Control bit options include:

   - ACK — Acknowledgement field significant bit
   - URG — Urgent pointer field significant bit
   - PSH — Push function bit
   - RST — Reset connection bit
   - SYN — Synchronize sequence number bit
   - FIN — No more data from sender
8. Click **Apply** or **OK** to save your work.

Configuring SSL certificates preferences

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **IP Preferences from the Software Configurations list** in the **Category** pane.

3. Enter a number of days to display a warning for an expiring certificate in the **DaysUntilExpiryWarning** field.

   When the certificate reaches this value, the certificate displays orange. Default is 31. Minimum is 0.

4. Enter a number of days to display the next warning for an expiring certificate in the **DaysUntilNextExpiryWarning** field.
5. Click **Apply** or **OK** to save your work.

Configuring SNMP preferences

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **IP Preferences from the Software Configurations list** in the **Category** pane.
3. Enter the number of retries after first attempt to read in the **Retries.Read** field.
4. Enter the number of retries after first attempt to write in the **Retries.Write** field.
5. Enter the time-out period in seconds between Read retry attempts in the **Timeout.Read** field.
6. Enter the time-out period in seconds between Write retry attempts in the **Timeout.Write** field.
7. Click **Apply** or **OK** to save your work.

Configuring syslog file reader preferences

To configure syslog file reader preferences, compete the following steps.

1. Enter a name for the file in the FileName field.
2. Select the **KeepFileOpenBetweenPolls** check box to keep the file open between polls.
3. Enter the message filter type in the **MessageFilter field.**

   For example, ^snort.

4. Enter the polling interval in the **PollingIntervalMilliSeconds field.**

   The default is 5000.

5. Select the **ReadNewEventsOnly** check box to only read new events.

Configuring TFTP preferences

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **IP Preferences from the Software Configurations list** in the **Category** pane.
3. Enter the number of retries before aborting a read or write transfer in the **maxRetries** field.
4. Enter the time-out period in milliseconds between retry attempts in the **timeout** field.
5. Click **Apply** or **OK** to save your work.

Memory allocation settings

You can configure memory allocation for the client and server to improve performance. You can trigger switch polling when a state changes or you can poll at intervals when no state change occurs.

NOTE
SAN size is a consideration in selection of polling periods.

Configuring memory allocation settings

To configure memory allocation settings, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Memory Allocation** in the **Category** list to set the memory allocation for the server and client.

   The **Memory Allocation** pane displays (Figure 68).

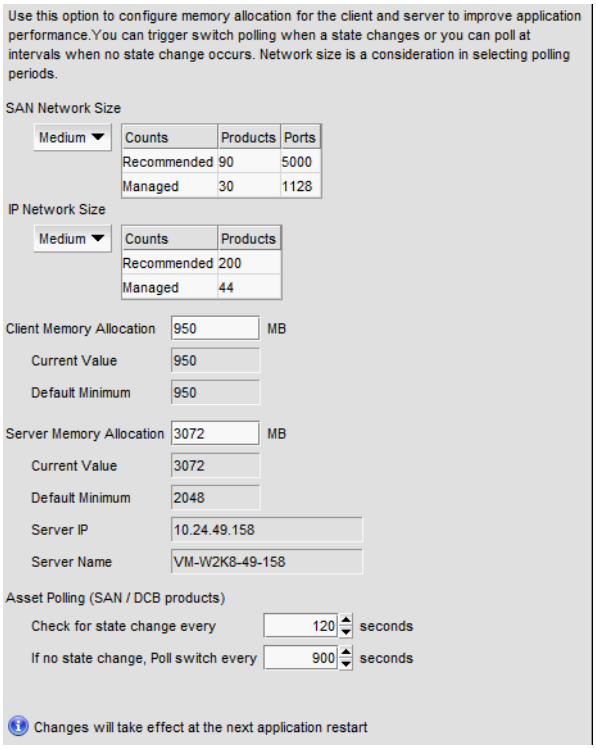


FIGURE 68 Options dialog box (Memory Allocation pane)

3. (Enterprise only) In the **IP Network Size is** list, complete the following steps:

   For other editions, the IP Network size is medium. You cannot change the IP size.

   a. Select the size of the IP (small, medium, or large) you want to configure.

      Product recommended counts change to the new default values when you change the IP Network size. Recommended counts are as follows:

- Small — 20 products (recommended)
- Medium — 200 products (recommended)
- Large — 5,050 products (recommended)

Memory and asset polling values change to the new default values when you change the IP Network size. You may increase these values. For default values, refer to step 4 and step 5.

b. Click **OK** on the confirmation message.

4. Enter the memory allocation (MB) for the client in the **Client Memory Allocation** field.

   If you enter an invalid value, an error message displays with the minimum value allowed. Click **OK** and edit the value again.

   The current configured number of megabytes for client memory allocation displays in the **Current Value** field. The default minimum number of megabytes for client memory allocation displays in the **Default Minimum** field.

   For all network sizes, the default minimum Client Heap Size is 950 MB.

   NOTE
   There is no restriction on the Client Heap Size value. The correct Client Heap Size value should be given according to the RAM present in the server where it is launched.

   NOTE
   For a 32-bit server, configuring a value higher than 1024 MB impacts the client launch.

5. Enter the memory allocation (MB) for the server in the **Server Memory Allocation** field.

   If you enter an invalid value, an error message displays with the minimum value allowed. Click **OK** and edit the value again.

   The current configured number of megabytes for server memory allocation displays in the **Current Value** field. The default minimum number of megabytes for server memory allocation displays in the **Default Minimum** field. The IP address of the server displays in the **Server IP** field. The server name displays in the **Server Name** field.

   To support more than 8 clients on a 64-bit server, increase the memory allocation for the server to 3076 MB.

   Minimum values are as follows:

   For a 32-bit Windows/Linux Server

   - Professional: 768 MB
   - Professional Plus: 1024 MB
   - Enterprise Small : 768 MB
   - Enterprise Medium : 1024 MB
   - Enterprise Large : 1024 MB

   Default values for IP only Server

   Server Heap Size

   For a 32-bit Windows/Linux Server

   - Small : 768 MB
   - Medium : 1024 MB

- Large : 1024 MB

For all 64-bit servers, the default minimum Server Heap Size for all network sizes is 2048 MB.

NOTE
There is no restriction on the maximum value for Server Heap Size in a 64-Bit Server. The correct server heap size value must be given according to the RAM present in the server.

6. Click **Apply** or **OK** to save your work.

NOTE
Changes to this option take effect after an application restart.

NOTE
You can only restart the server using the Server Management Console (**Start > Programs >** *Management_Application_Name* **12.X.X > Server Management Console**).

7. Click **OK** on the "changes take effect after application restart" message.

Configuring asset polling

NOTE
Asset polling is only applicable for Fabric OS DCB products discovered from the IP tab.

Asset polling allows you set the length of time between state change polling. To maximize the efficiency of the polling feature (balance the amount of possible information with any possible performance impact), base your settings on the size of the SAN.

To configure asset polling, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Memory Allocation** in the **Category** list to set the memory allocation for the server and client.

   The **Memory Allocation** pane displays (Figure 68).

3. Enter how often you want to check for state changes in the **Check for state change every** field.

   Valid values are from 1 through 600 seconds. You cannot enter a value lower than the default minimum value.

   Default minimum values are as follows:

   - Small (Professional): 60 seconds
   - Medium: 120 seconds
   - Large: 180 seconds

4. Enter how often you want to check for state changes in the **If no state change, Poll switch every** field.

   Valid values are from 1 through 3,600 seconds. Default values are as follows:

   - Small (Professional): 120 seconds
   - Medium: 900 seconds

- Large: 1800 seconds

5. Click **Apply** or **OK** to save your work.

NOTE
Changes to this option take effect after an application restart.

NOTE
You can only restart the server using the Server Management Console (**Start > Programs >** *Management_Application_Name* **12.X.X > Server Management Console**).

6. Click **OK** on the "changes take effect after application restart" message.

Viewing the network size status

The Management application enables you to view the network size status at a glance by providing a status icon on the Status Bar. Double-click the icon to launch the **Memory Allocation** pane of the **Options** dialog box.

NOTE
If you exceed the recommended count, the network size status icon refreshes when the License is refreshed (every three hours) or after a client restart.

NOTE
The recommended count is the supported scalability limit based on the network size. If the maximum license count is less than the recommended count, the license count displays as the recommended count.

The following table illustrates and describes the icons that indicate the current network size status.

TABLE 20

Icon	Description
	This icon displays when the network size is within the recommended count.
	This icon displays when the network size exceeds the recommended count. This icon displays when any of the following counts are exceeded: • IP Product Count • IP Port Count

Product communication settings

You can configure HTTP or HTTPS connections between the products and the Management application server.

Configuring SAN communication

To configure connections between the SAN devices and the Management application server, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Product Communication from the Software Configurations list** in the **Category** pane.

   The **Product Communication** pane displays (Figure 69).

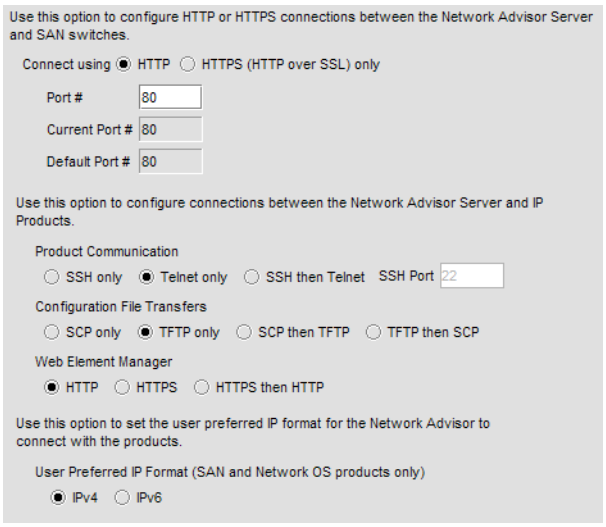


FIGURE 69 Options dialog box (Product Communication pane)

3. To connect using HTTP, complete the following steps.
   a. Select the **Connect using HTTP** option.
   b. Enter the connection port number in the **Port #** field. Go to step 5.

      The default HTTP port number is 80.

NOTE
To manage FIPS-enabled Fabric OS fabrics, you must configure Product Communication using the **Connect using HTTPS (HTTP over SSL) only** option.

4. To connect using HTTPS (HTTP over SSL), complete the following steps.
   a. Select the **Connect using HTTPS (HTTP over SSL) only** option.
   b. Enter the connection port number in the **Port #** field. Continue with step 5.

      The default HTTPS port number is 443.

5. (Fabric OS and Network OS products only) Select **IPv4** or **IPv6** to set the preferred IP format.
6. Click **Apply** or **OK** to save your work.

   Changes to this option take effect after an application restart.

7. Click **OK** on the “changes take effect after application restart” message.

Configuring the preferred IP format

To configure the preferred IP format for the Management application server to connect with Fabric OS and Network OS devices, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Product Communication from the Software Configurations list** in the **Category** pane.

   The **Product Communication** pane displays (Figure 69).

3. (Fabric OS and Network OS products only) Select **IPv4** (default) or **IPv6** to set the preferred IP format.

4. Click **Apply** or **OK** to save your work.

   Changes to this option take effect after an application restart.

5. Click **OK** on the "changes take effect after application restart" message.

Configuring IP communication

To configure communication between IP product and the Management application server, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Product Communication from the Software Configurations list** in the **Category** pane.

   The **Product Communication** pane displays (Figure 70).

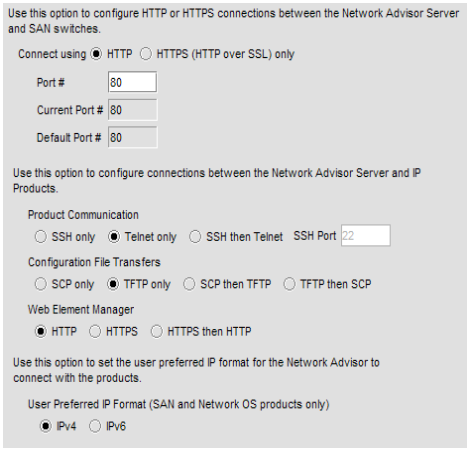


FIGURE 70 Options dialog box (Product Communication pane)

3. To connect to products using SSH, complete the following steps.
   a. Select the **SSH only** option.
   b. Enter the connection port number in the **SSH Port** field. Go to step 6.

      The default SSH port number is 22.

4. To connect to products using Telnet, select the **Telnet only** option. Go to step 6.
5. To connect to products using SSH then Telnet, complete the following steps.
   a. Select the **SSH then Telnet** option.
   b. Enter the connection port number in the **SSH Port** field. Continue with step 6.

6. Select one of the following options to determine configuration file transfer communication:
    - SCP only
    - TFTP only
    - SCP then TFTP
    - TFTP then SCP
7. Select one of the following options to configure the web element manager communication:
    - HTTP
    - HTTPS (HTTP over SSL)
    - HTTPS then HTTP
8. Click **Apply** or **OK** to save your work.

FTP/SCP/SFTP server settings

NOTE
For FIPS-enabled Fabric OS switches, you must configure the FTP/SCP/SFTP server communication to an external SCP server to download firmware and allow technical support.

File Transfer Protocol (FTP) is a network protocol used to transfer data from one computer to another over a TCP computer network. During installation, a built-in FTP server and its services are installed. Other FTP servers on your system are recognized by the application as external FTP servers.

For Windows systems, the built-in FTP server is the default configuration and installation starts the FTP service if port 21 is not used by any other FTP server. For UNIX systems, built-in FTP is the default for UNIX systems during installation; the external FTP server is the default only if port 21 is busy.

Note that when uninstalling the application the built-in FTP server is removed with all other services even if the FTP service is used by firmware upgrade or supportSave features.

NOTE
FTP is supported on all Fabric OS devices.

Secure Copy (SCP) is a means of securely transferring computer files between a local and a remote host or between two remote hosts, using the Secure Shell (SSH) protocol. You must configure SCP on your machine to support Technical Support and firmware download.

NOTE
SCP is supported on Fabric OS devices running 5.3 and later.

SSH File Transfer Protocol (SFTP) is a network protocol used to transfer data from one computer to another over a secure channel. You must configure SCP on your machine to support Technical Support and firmware management.

NOTE
SFTP is supported on Fabric OS devices running 7.0 and later.

The built-in SCP/SFTP servers use the port 22 by default.

To view the port status for the FTP and SCP/SFTP servers, refer to "Viewing port status" on page 10.

Accessing the FTP server folder

Choose from one of the following options to access the FTP server folder:

- To access the internal FTP folder, select **Monitor > Techsupport > View Repository**.
- To access the external FTP folder, type the following in a browser window: ftp://*Username@External_FTP_Server_IP_Address* (for example, ftp://admin@10.1.1.1) and press **Enter**. Type your password in the pop-up window and press **Enter**. The external FTP folder displays.

Configuring an internal FTP server

To configure the internal FTP server settings, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **FTP/SCP/SFTP** in the **Category** list.

   The **FTP/SCP/SFTP** pane displays (Figure 71).

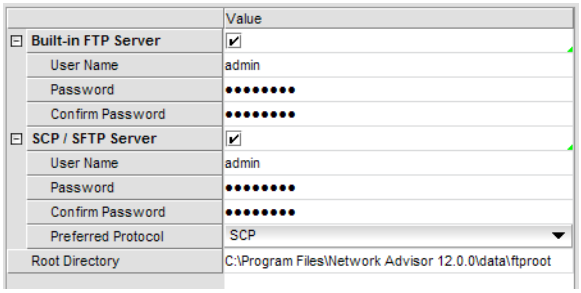


FIGURE 71 Options dialog box (FTP/SCP/SFTP pane)

3. Select the **Use built-in FTP/SCP/SFTP Server** option to use the default built-in FTP server.

   All active fields are mandatory. The default user name is admin. The full path to the built-in FTP directory displays in the **Root Directory** field.

4. Select the **Built-in FTP Server** check box.
5. Change your password by entering a new password in the **Password** and **Confirm Password** fields.

   The default password is passw0rd (where 0 is a zero).

6. Click **Test** to test the FTP server.

   An "FTP Server running successfully" or an error message displays.

   If you receive an error message, make sure your credentials are correct, the server is running, the remote directory path exists, and you have the correct access permission; then try again.

7. Click **Apply** or **OK** to save your work.

Configuring an internal SCP or SFTP server

NOTE
SCP is supported on Fabric OS devices running 5.3 and later.

NOTE
SFTP is supported on Fabric OS devices running 7.0 and later.

To configure the internal SCP or SFTP server settings, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **FTP/SCP/SFTP** in the **Category** list.

   The **FTP/SCP/SFTP** pane displays (Figure 71).

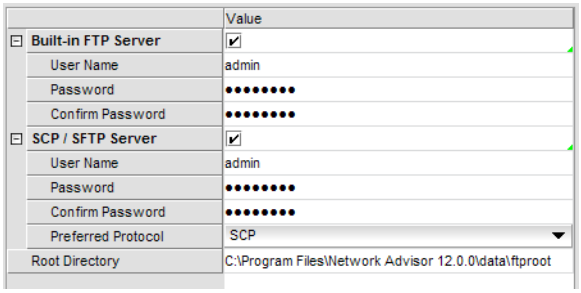


FIGURE 72 Options dialog box (FTP/SCP/SFTP pane)

3. Select the **Use built-in FTP/SCP/SFTP Server** option to use the default built-in SCP or SFTP server.

   All active fields are mandatory. The default user name is admin. The full path to the built-in SCP or SFTP directory displays in the **Root Directory** field.

4. Select the **SCP/SFTP Server** check box.

5. Change your password by entering a new password in the **Password** and **Confirm Password** fields.

   The default password is passw0rd (where 0 is a zero).

6. Select the protocol (**SCP** or **SFTP**) from the **Preferred Protocol** list.

7. Click **Test** to test the server.

   An “SCP/SFTP Server running successfully” or an error message displays.

   If you receive an error message, make sure your credentials are correct, the SCP/SFTP server is stopped, the remote directory path exists, and you have the correct access permission; then try again.

8. Click **Apply** or **OK** to save your work.

Configuring an external FTP, SCP, or SFTP server

NOTE
For FIPS-enabled Fabric OS switches, you must configure the FTP/SCP/SFTP server communication to an external SCP or SFTP server to download firmware and allow technical support.

NOTE
SCP is supported on Fabric OS devices running 5.3 and later.

NOTE
SFTP is supported on Fabric OS devices running 7.0 and later.

To configure external FTP, SCP, or SFTP server settings, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **FTP/SCP/SFTP** in the **Category** list.

   The **FTP/SCP/SFTP** pane displays (Figure 73).

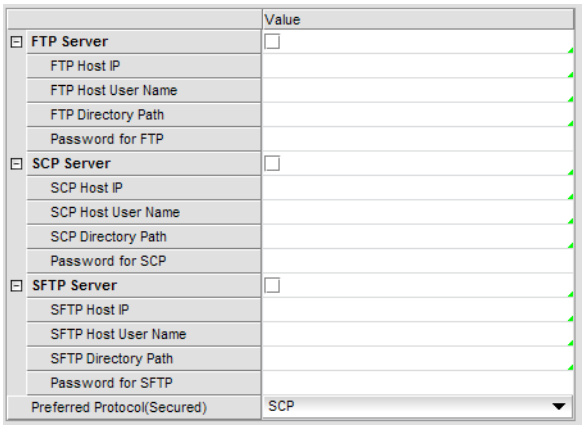


FIGURE 73 Options dialog box (FTP/SCP/SFTP pane)

3. Select the **Use External FTP Server and/or SCP Server** option.
4. To configure an external FTP server, complete the following steps.
   a. Select the **FTP Server** check box to configure the external FTP server.

      All fields are mandatory.

   b. Enter the IP address for the remote host in the **Remote Host IP** field.
   c. Enter a user name in the **Remote Host User Name** field.
   d. Enter the path to the remote host in the **Remote Directory Path** field.

      Use a slash (/) or period (.) to denote the root directory.

   e. Enter the password in the **Password Required for FTP** field.
5. To configure an external SCP server, complete the following steps.

a. Select the **SCP Server** check box to configure the external SCP server.

   All fields are mandatory.

b. Enter the IP address for the remote host in the **SCP Host IP** field.

c. Enter a user name in the **SCP Host User Name** field.

d. Enter the path to the remote host in the **SCP Directory Path** field.

   Use a slash (/) or period (.) to denote the root directory.

e. Enter the password in the **Password Required for SCP** field.

f. Select **SCP** from the **Preferred Protocol (Secured)** list.

6. To configure an external SFTP server, complete the following steps.

   a. Select the **SFTP Server** check box to configure the external SCP server.

      All fields are mandatory.

   b. Enter the IP address for the remote host in the **SFTP Host IP** field.

   c. Enter a user name in the **SFTP Host User Name** field.

   d. Enter the path to the remote host in the **SFTP Directory Path** field.

      Use a slash (/) or period (.) to denote the root directory.

   e. Enter the password in the **Password Required for SFTP** field.

   f. Select **SFTP** from the **Preferred Protocol (Secured)** list.

7. Click **Test** to test the server.

   A "Server running successfully" or an error message displays.

   If you receive an error message, make sure your credentials are correct, the server is running, the remote directory path exists, and you have the correct access (read and write) permissions; then try again.

8. Click **OK** on the message.

9. Click **Apply** or **OK** to save your work.

Testing the FTP, SCP, and SFTP server

To test the FTP, SCP, or SFTP server, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **FTP/SCP/SFTP** in the **Category** list.

3. Choose one or more of the following options:

   - If you are using the internal FTP server, select the **Use built-in FTP/SCP/SFTP Server** option.

     For step-by-step instructions about configuring the built-in server, refer to "Configuring an internal FTP server" on page 173.

   - If you are using the external FTP server, select the **Use external FTP/SCP/SFTP Server** option.

For step-by-step instructions about configuring the built-in server, refer to "Configuring an external FTP, SCP, or SFTP server" on page 175.

4. Click **Test**.

   An "FTP, SCP, or SFTP Server running successfully" or an error message displays.

   If you receive an error message, make sure your credentials are correct, the server is running, the remote directory path exists, and you have the correct access permission; then try again.

5. Click **OK** on the message.
6. Click **OK** to close the **Options** dialog.

Server port settings

You can configure the server port settings so that you can assign a web server port number and set the server port to be SSL-enabled.

Configuring the server port

To configure server settings, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Server Port** in the **Category** list.

   The **Server Port** pane displays (Figure 74).

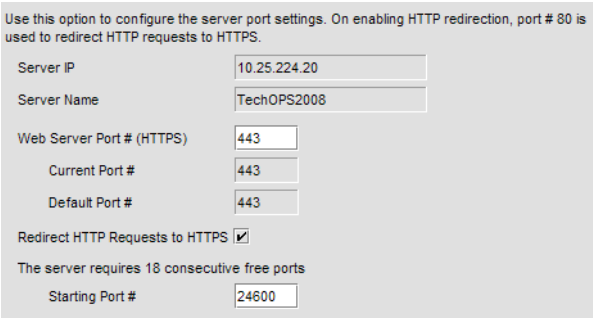


FIGURE 74 Options dialog box (Server Port pane)

3. Enter a port number in the **Web Server Port # (HTTPS)** field.

   The default is 443.

4. Enable HTTP redirection to HTTPS by selecting the **Redirect HTTP Requests to HTTPS** check box.

   When you enable HTTP redirection, the server uses port 80 to redirect HTTP requests to HTTPS. Make sure that port 80 is available before you enable HTTP redirection.

5. Enter a port number in the **Starting Port #** field.

   The default is 24600.

For Professional, the server requires 15 consecutive free ports beginning with the starting port number.

For Trial and Licensed versions, the server requires 18 consecutive free ports beginning with the starting port number.

6. Click **Apply** or **OK** to save your work.

NOTE
Changes to this option take effect after application restart.

7. Click **OK** on the "changes take effect after application restart" message.

Support mode settings

You can configure support settings to allow enhanced diagnostics.

Configuring support mode settings

To configure support mode settings, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays (Figure 75).

2. Select **Support Mode** in the **Category** list.

NOTE
Only use this option when directed to by customer support.

   The **Support Mode** pane displays (Figure 74).

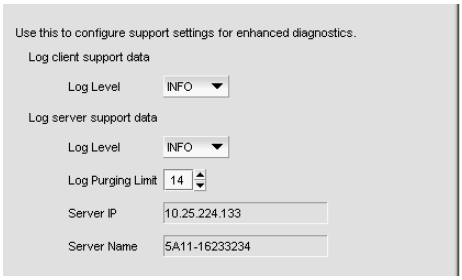


FIGURE 75 Options dialog box (Support Mode pane)

3. Select the **Log client support data - Log Level** list, and select the type of log data you want to configure.

   Log level options include: **All**, **Fatal**, **Error**, **Warn**, **Info**, **Debug**, **Trace**, and **Off**. Default is **Info**.

4. Select the **Log server support data - Log Level** list, and select the type of log data you want to configure.

   Log level options include: **All**, **Fatal**, **Error**, **Warn**, **Info**, **Debug**, **Trace**, and **Off**. Default is **Info**.

5. Click **Apply** or **OK** to save your work.

NOTE
Changes to the server log levels reset to the default (INFO) after a server restart.

NOTE
Changes to the **Log client support data** log level is persisted on all clients launched from the same machine for the same server.

client. log file properties

- Client logs are collected separately for each server. After successful login, a log file is created and prefixed with the network address provided in the **Login** dialog box.

  For example, 172.26.1.1.client.log or localhost.client.log

  Each log file is limited to 5 MB. When a file reaches the maximum size, and there are less than 5 log files for the Client, a new file is created.

- For local clients, log files (*network_address*.client.log.1 through *network_address*.client.log.5) are created in the *User_Home/Product_Name/localhost* directory.
- For web start clients, log files (*network_address*.client.log.1 through *network_address*.client.log.5) are created in the *User_Home/Product_Name/Server_IP_Address* directory.

server. log file properties

- There is only one server.log file each day with no log size limit.
- The server.log file rolls over at 12:00 midnight everyday.
- When the log file rolls over, it is compressed and renamed using the following file name format:

  server.yyyy-mm-dd.log.zip
  for example, server.2010-04-14.log.zip, server.2010-04-15.log.zip, and so on

- For servers, log files are created in the *Install_Home*/logs/server directory.

Configuring the server log file purge limit

To configure server log file purging, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Support Mode** in the **Category** list.

   NOTE
   Only use this option when directed to by customer support.

3. Select the maximum number of days to retain the server log file in the **Log Purging Limit** field.

   Valid values are 1 through 90. Default is 14.

   The log files are purged at 1:00 AM on the day after the retention period ends.

4. Click **Apply** or **OK** to save your work.

FIPS Support

To manage FIPS-enabled Fabric OS fabrics and switches, make sure you complete the following configuration requirements:

- Configure Product Communication to HTTPS (refer to "Configuring SAN communication" on page 169) to allow communication between the server and the Fabric OS switches.
- Configure an external SCP server (refer to "Configuring an external FTP, SCP, or SFTP server" on page 175) to allow firmware download, product technical support, and supportSave.

Chapter

6

User Account Management

In this chapter

Users overview

The Management application allows you to manage accounts of users who manage devices on the network. When a user logs in to the Management application, the user name and password can be authenticated and authorized by the local server or by a supported external server.

User accounts are assigned privileges, which you define within roles. Each privilege provides access to a specific feature of the Management application. This enables you to maintain privileges common to a group of administrators within a role, instead of in individual accounts.

You can group devices, access points, and their groups in areas of responsibilities (AORs), then assign one or more AORs to a user's privilege. When you assign a user an AOR, that user will be able to manage only the devices in that AOR. Devices in a user's AOR are the only devices that user sees in device trees and on the **Dashboard** tab. You can place selected devices, device groups, port groups, access points, access point groups, and access point port groups in an AOR.

Users who create a device group are the only users who can manage the devices in that group. Other users may view the groups, but do not have the ability to add, delete, or modify the groups.

Configuration requirements

To administer accounts on the Management application server, you must have an administrative login on the platform on which the Management application is running. Use the "Administrator" login to create other logins with administrative permissions.

Viewing configured users

To view configured users, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Click the **Users** tab, if necessary.

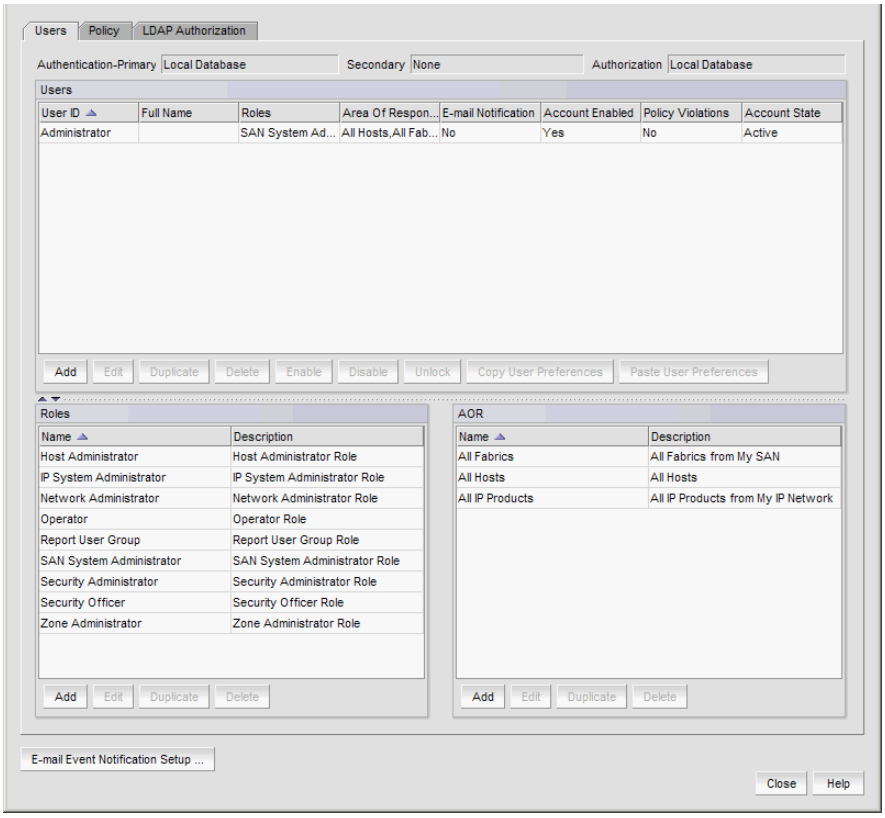


FIGURE 76 **Users dialog box - Users tab**

The **Users** dialog box contains the following fields and components:

- Authentication-Primary — The primary authentication server type configured through the Server Management Console.
- Secondary — The secondary authentication server type configured through Server Management Console.
- Authorization — The authorization source configured through the Server Management Console.

- **Users** table — The configured users.
  - **User ID** — The unique name used to identity a user.
  - **Full Name** — The user's full name.
  - **Roles** — List of Roles the user belongs to separated by comma.
  - **Area Of Responsibility** — List of AORs the user belongs to separated by comma.
  - **E-mail Notification** — Whether e-mail notification is enabled for user.
  - **Account Enabled** — Whether the user account status is enabled.
  - **Policy Violations** — Whether there is a current policy violation for the user.
  - **Account State** — The current account state for the user. Options include:
    - Active
    - Locked by User manager
    - Password Expired
    - Password format policy violated
    - Password history policy violated
    - Locked Out threshold reached
  - **Add** button — Click to launch the **Add Users** dialog box and configure a new user (refer to "Creating a new user account" on page 185).
  - **Edit** button — Click to launch the **Edit Users** dialog box for the selected user (refer to "Editing a user account" on page 187).
  - **Duplicate** button — Click to launch the Duplicate Users dialog box for the selected user (refer to "Copying a user account" on page 187).
  - **Delete** button — Click to delete the selected users (refer to "Deleting a user account" on page 190).
  - **Enable** button — Select to enable the selected users (refer to "Enabling a user account" on page 190). Disabled if the selected user is already enabled.
  - **Disable** button — Select to disable the selected users (refer to "Disabling a user account" on page 189). Disabled if the selected user is already disabled.
  - **Unlock** button — Select to unlock the selected users account (refer to "Unlocking a user account" on page 190).
  - **Copy User Preferences** button — Select to copy user preference from the selected users account (refer to "Copying and pasting user preferences" on page 188).
  - **Paste User Preferences** button — Select to paste user preference from the selected users account (refer to "Copying and pasting user preferences" on page 188).
- **Roles** table — Lists the default system roles and any user-defined roles.
  - **Name** — The unique name of the role.

Default system roles for IP only environments include:

- IP System Administrator
- Network Administrator
- Report User Group
- Default system roles for SAN plus IP environments include:
- SAN System Administrator
- IP System Administrator
- Network Administrator
- Security Administrator
- Zone Administrator
- Operator
- Security Officer
- Host Administrator
- Report User Group

- **Description** — A description of the role.
- **Add** button — Click to add a new role (refer to "Creating a new role" on page 191).
- **Edit** button — Click to edit the selected role (refer to "Editing a role" on page 192).
- **Duplicate** button — Click to copy the selected role (refer to "Copying a role" on page 192).
- **Delete** button — Click to delete the selected role (refer to "Deleting a role" on page 193).

- **AOR** table — Lists the default system AOR and any user-defined AORs.
  - **Name** — The unique name of the AOR. Default system AORs include:
    - **All Fabrics** — all discovered SAN devices.
    - **All Hosts** — all discovered Hosts devices.
    - **All IP Products** — all discovered IP devices.
  - **Description** — A description of the AOR.
  - **Add** button — Click to launch the Add AOR dialog box.
  - **Edit** button — Click to launch the Edit AOR dialog box for the selected AOR. You cannot edit system AORs.
  - **Duplicate** button — Click to launch the Duplicate AOR dialog box for the selected AOR. You cannot duplicate system AORs.
  - **Delete** button — Click to delete the selected AOR. You cannot delete system AORs.
- **E-mail Event Notification Setup** button — Click to configure e-mail event notification (refer to "Configuring e-mail notification" on page 209).

3. Click **Close** to close the **Users** dialog box.

User accounts

NOTE
You must have User Management Read and Write privileges to add new accounts, set passwords for accounts, and apply roles to the accounts. For a list of privileges, refer to "User Privileges" on page 1283.

Management application user accounts contain the identification of the Management application user, as well as privileges, roles, and AORs assigned to the user. Privileges provide access to the features in Management application. A role is a group of selected privileges. A role can be assigned to one or more Management application users who need access to the same menu options.

An AOR contains selected devices, device groups, device port groups, access points, access point groups, and port groups that an Management application user is allowed to manage.

Creating a new user account

To create a new user account, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Click **Add** under the **Users** table.

   The **Add User** dialog box displays.

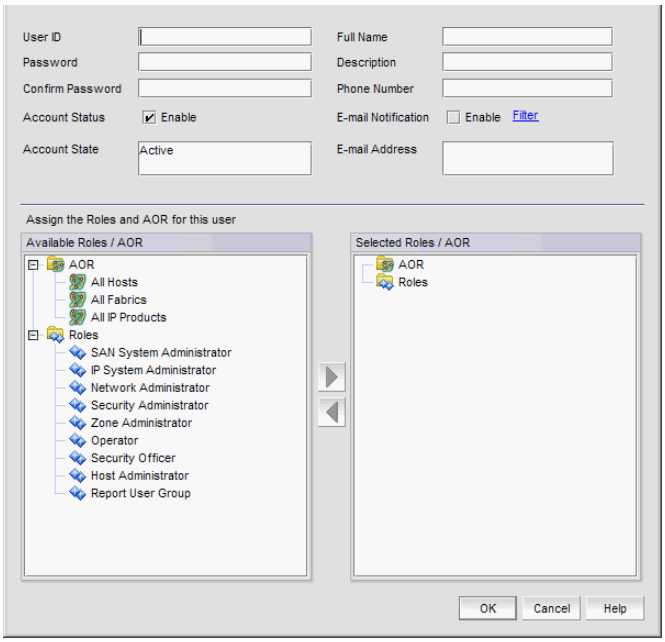


FIGURE 77 Add User dialog box

3. Enter a unique name to identify the user in the **User ID** field.

4. Enter a password for the user in the **Password** and **Confirm Password** fields.

   Passwords displays as dots (.). For password policy details, refer to "Viewing your password policy" on page 208.

5. Select the **Account Status** - **Enable** check box to enable the account of the user.

   Account Status is enabled by default.

6. (Optional) Enter the full name of the user in the **Full Name** field.

7. (Optional) Enter a description for the user in the **Description** field.

8. (Optional) Enter the phone number of the user in the **Phone Number** field.

9. Select the **E-mail Notification** - **Enable** check box to enable e-mail notification for the user.

   E-mail Notification is disabled by default.

10. Click **Filter** to set up basic event filters for the user.

    For step-by-step instructions about setting up basic event filters, refer to "Setting up basic event filtering" on page 1144.

11. Enter the e-mail address of the user in the **E-mail Address** field.

    Enter more than one e-mail address, separating each with a semi-colon. To send a text message or page via e-mail, use the following format *number@carrier.com*, where *number* is your phone number and *carrier.com* is the SMS server. For example, 3035551212@txt.att.net (text message) or 3035551212@page.att.net (page).

    NOTE
    Check with your carrier for the exact e-mail address.

12. Assign roles and AORs by selecting the role or AOR in the **Available Roles / AOR** table and click the right arrow button to move the role or AOR to the **Selected Roles / AOR** table.

    Select multiple roles or AORs by holding down the CTRL key and clicking more than one role or AOR.

13. Remove roles and AORs by selecting the role or AOR in the **Selected Roles / AOR** table and click the left arrow button to move the role or AOR to the **Available Roles / AOR** table.

    Select multiple roles or AORs by holding down the CTRL key and clicking more than one role or AOR.

14. Click **OK** to save the new user and close the **Add User** dialog box.

    The new user account displays in the **Users** table of the **Users** dialog box. You must assign at least one role to a user account. Users without an assigned role cannot log into the client.

15. Click **Close** to close the **Users** dialog box.

Editing a user account

To make changes to an existing user account, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the user account you want to edit and click **Edit** under the **User**s table.

   The **Edit User** dialog box displays.

3. Complete step 3 through step 13 in "Creating a new user account" on page 185.

4. Click **OK** to save the user account and close the **Edit User** dialog box.

   If you make changes to the user's role or AOR while the user is logged in, a confirmation message displays. When you click **OK** on the confirmation message, the user is logged out and must log back in to see the changes.

5. Click **Close** to close the **Users** dialog box.

Copying a user account

You can create a user account by copying an existing one. When you copy an account, you copy the selected roles and AORs of that account. You can then enter a new user name, ID, e-mail address, and telephone number.

To create a new user account from an existing account, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the user account you want to copy and click **Duplicate** under the **User**s table.

   The **Duplicate User** dialog box displays.

3. Complete step 3 through step 13 in "Creating a new user account" on page 185.

4. Click **OK** to save the new user and close the **Duplicate User** dialog box.

   The new user account displays in the **Users** table of the **Users** dialog box.

5. Click **Close** to close the **Users** dialog box.

Copying and pasting user preferences

Enables you to copy user preference settings, such as window and dialog box sizes, table column and sort order, as well as other customizations, and all the user-defined views (including fabrics and hosts) from the selected user account to one or more other user accounts.

If the fabric and hosts from the original user account are not included in the other user's AOR, then the copied fabrics and hosts do not display in the other user's views. To include fabrics and hosts from the original user account, you must add them to the other user's account (refer to "Assigning roles and areas of responsibility to a user account" on page 188).

If a user-created view with the same name already exists in the other user's views, user-defined views with the same name are ignored. For example, user_acct1 (copy) has the following user-defined views: Fabric1, Fabric2, and Host1 and user_acct2 (paste) has the following user-defined views: Fabric1, Fabric_CO, and Hosts. When you paste the user_acct1 user preferences to user_acct2, user_acct2 now has the following user-defined views: Fabric1, Fabric2, Fabric_CO, Host1, and Hosts.

NOTE
You cannot copy user preferences to user accounts that are currently logged in to the Management application.

NOTE
You cannot copy user preferences to the original user account.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the user account you want to copy user preferences from and click **Copy User Preferences** under the **Users** table.

3. Select the user account you want to copy user preferences to and click **Paste User Preferences** under the **Users** table.

   If you need to make any other changes to this user account, refer to "Editing a user account" on page 187.

4. Click **Yes** on the confirmation message.

5. Click **Close** to close the **Users** dialog box.

Assigning roles and areas of responsibility to a user account

To assign roles and AORs to an existing user account, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the user account you want to edit and click **Edit** under the **Users** table.

   The **Edit User** dialog box displays.

3. Assign roles and AORs by selecting the role or AOR in the **Available Roles / AOR** table and click the right arrow button to move the role or AOR to the **Selected Roles / AOR** table.

   Select multiple roles or AORs by holding down the CTRL key and clicking more than one role or AOR.

4. Click **OK** to save the user account and close the **Edit User** dialog box.

   If you make changes to the user's role or AOR while the user is logged in, a confirmation message displays. When you click **OK** on the confirmation message, the user is logged out and must log back in to see the changes.

5. Click **Close** to close the **Users** dialog box.

Removing roles and areas of responsibility from a user account

To remove roles and AORs from an existing user account, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the user account you want to edit and click **Edit** under the **User**s table.

   The **Edit User** dialog box displays.

3. Remove roles and AORs by selecting the role or AOR in the **Selected Roles / AOR** table and click the left arrow button to move the role or AOR to the **Available Roles / AOR** table.

   Select multiple roles or AORs by holding down the CTRL key and clicking more than one role or AOR.

4. Click **OK** to save the user account and close the **Edit User** dialog box.

   If you make changes to the user's role or AOR while the user is logged in, a confirmation message displays. When you click **OK** on the confirmation message, the user is logged out and must log back in to see the changes.

5. Click **Close** to close the **Users** dialog box.

Disabling a user account

To make the user account inactive, but keep it in the database, you can disable the user account.

NOTE
You cannot disable the default "Administrator" account.

To disable a user account, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the enabled user account you want to disable in the **Users** table and click **Disable**.

3. Click **Yes** on the confirmation message.

   If currently accessing the server, the user will be logged out once the user account is disabled. The user cannot log back in until you re-enable the user account.

4. Click **Close** to close the **Users** dialog box.

Enabling a user account

To re-activate a user account, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the disabled user account you want to enable in the **Users** table and click **Enable**.
3. Click **Yes** on the confirmation message.
4. Click **Close** to close the **Users** dialog box.

Deleting a user account

NOTE
You cannot delete the default "Administrator" user account.

To permanently delete a user account from the server, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the user you want to delete in the **Users** table and click **Delete**.
3. Click **Yes** on the confirmation message.

   If currently accessing the server, the user will be logged out once the user account is deleted.

4. Click **Close** to close the **Users** dialog box.

Unlocking a user account

NOTE
You must have User Management Read and Write privileges to unlock a user account.

You can unlock a user account when a user is locked out of the system because of too many invalid login attempts.

To unlock a user account, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the locked user account you want to unlock in the **Users** table and click **Unlock**.
3. Click **Yes** on the confirmation message.
4. Click **Close** to close the **Users** dialog box.

Roles

NOTE
You must have User Management Read and Write privileges to view, add, modify, or delete roles.

A role is a group of Management application tasks or privileges that can be assigned to several users who have similar functions.

When you create a role, it immediately becomes available in the **Users** dialog box.

Creating a new role

To create a new role, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Click **Add** under the **Roles** table.

   The **Add Role** dialog box displays.

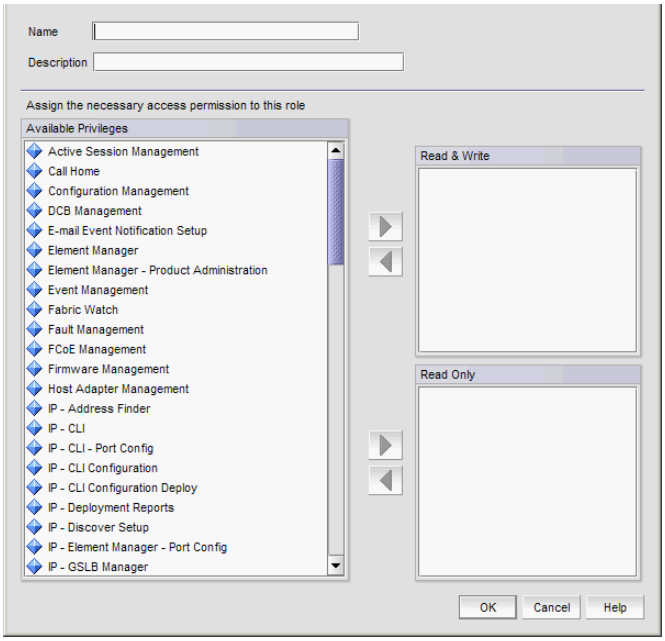


FIGURE 78 Add Role dialog box

3. Enter a name of the role in the **Name** field.
4. (Optional) Enter a short description for the role in the **Description** field.
5. Add or remove privileges as needed.

   For step-by-step instructions, refer to "Adding privileges to a role" on page 193 or "Removing privileges from a role" on page 194.

6. Click **OK** to save the new role and close the **Add Role** dialog box.

   The new role displays in the **Roles** list of the **Users** dialog box. To add users to this role, follow the instructions in "Assigning roles and areas of responsibility to a user account" on page 188.

7. Click **Close** to close the **Users** dialog box

Editing a role

To make changes to an existing role, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the role you want to edit in the **Roles** table and click **Edit**.

   The **Edit Role** dialog box displays.

3. Complete step 3 through step 5 in "Creating a new role" on page 191.

4. Click **OK** to save the role and close the **Edit Role** dialog box.

   If you make changes to the user's role or AOR while the user is logged in, a confirmation message displays. When you click **OK** on the confirmation message, the user is logged out and must log back in to see the changes.

5. Click **Close** to close the **Users** dialog box.

Copying a role

You can create a new role by copying an existing one. When you copy a role, you copy the selected privileges in that role.

To copy an existing role, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the role you want to copy in the **Roles** table and click **Duplicate**.

   The **Duplicate Role** dialog box displays.

3. Complete step 3 through step 5 in "Creating a new role" on page 191.

4. Click **OK** to save the role and close the **Duplicate Role** dialog box.

   The new role displays in the **Roles** list of the **Users** dialog box. To add users to this role, follow the instructions in "Assigning roles and areas of responsibility to a user account" on page 188.

5. Click **Close** to close the **Users** dialog box.

Deleting a role

To delete a role, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the role you want to delete in the **Roles** table and click **Delete**.
3. Click **Yes** on the confirmation message.
4. Click **Close** to close the **Users** dialog box.

Adding privileges to a role

Each option under the Management application main menu corresponds to a privilege. By adding a privilege to a role and assigning that role to a user, you give the user access to a feature of the Management application. When a user logs in to the Management application, the user sees only the options that correspond to the privileges listed in the **Add Roles**, **Edit Roles**, or **Duplicate Roles** dialog box.

To add privileges to a role, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Click **Add**, **Edit**, or **Duplicate** under the **Roles** table.

   The **Add Roles**, **Edit Roles**, or **Duplicate Roles** dialog box displays.

3. Add read and write access by selecting the features to which you want to allow read and write access in the **Available Privileges** list and click the right arrow button to move the features to the **Read & Write Privileges** list.

   Select multiple features by holding down the CTRL key and clicking more than one privilege. The features are moved to the **Read & Write Privileges** list.

4. Add read-only access by selecting the features to which you want to allow read-only access in the **Available Privileges** list and click the right arrow button to move the features to the **Read Only Privileges** list.

   Select multiple features by holding down the CTRL key and clicking more than one privilege. The features are moved to the **Read Only Privileges** list.

5. Click **OK** to save your work.
6. Click **Close** to close the **Users** dialog box.

Removing privileges from a role

You remove privileges from the **Edit** or **Duplicate Users** dialog boxes.

To remove privileges from role, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the role you want to edit in the **Roles** table and click **Edit** or **Duplicate** under the **Roles** table.

   The **Edit Roles** or **Duplicate Roles** dialog box displays.

3. Remove read and write access by selecting the features to which you want to remove read and write access in the **Read & Write Privileges** list and click the left arrow button to move the features to the **Available Privileges** list.

   Select multiple features by holding down the CTRL key and clicking more than one privilege. The features are moved to the **Available Privileges** list.

4. Remove read-only access by selecting the features to which you want to remove read-only access in the **Read Only Privileges** list and click the right arrow button to move the features to the **Available Privileges** list.

   Select multiple features by holding down the CTRL key and clicking more than one privilege. The features are moved to the **Available Privileges** list.

5. Click **OK** to save your work.

6. Click **Close** to close the **Users** dialog box.

Areas of responsibility

NOTE
You must have User Management Read and Write privileges to view, add, modify, or delete operational areas of responsibility.

An area of responsibility (AOR) allows you to place Fabrics, Hosts, Products, Product Groups, Port Groups, and Application products into management groups that can be assigned to an Management application user. Users can manage only the Fabrics, Hosts, Products, Product Groups, Port Groups, and Application products in the AOR assigned to them, because only devices their AOR display in the Product List and Topology Map.

For example, devices 10.10.10.1, 10.10.10.2, and 10.10.14.3 may be placed in AOR Group 1. This AOR group can then be assigned to UserA. When using the Management application, UserA will be able to create configurations, generate reports, and perform backups only to entries in AOR Group 1 (which consists of devices 10.10.10.1, 10.10.10.2, and 10.10.14.3).

Creating an AOR

When creating an AOR, you assign devices or groups to that AOR. After you save the AOR, it can be assigned to one or more user account. Users of those accounts can then view the devices or groups in their assigned AOR. Users can deploy configurations and payloads only to devices in assigned AORs.

When you create an AOR, it immediately becomes available in the **Users** dialog box.

To create an AOR, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Click **Add** under the **AOR** table.

   The **Add AOR** dialog box displays.

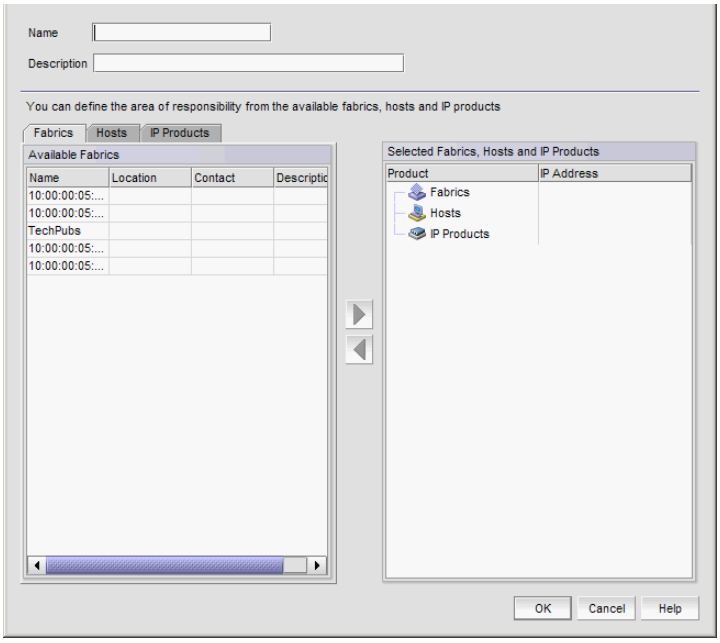


FIGURE 79 **Users dialog box - Users tab**

3. Enter a name of the AOR in the **Name** field.
4. (Optional) Enter a short description for the AOR in the **Description** field.
5. Assign or remove products as needed.

   For step-by-step instructions, refer to "Assigning products to an AOR" on page 197 or "Removing products from an AOR" on page 198.

6. Click **OK** to save the new AOR and close the **Add AOR** dialog box.

   The new AOR displays in the **AOR** list of the **Users** dialog box.

7. Click **Close** to close the **Users** dialog box.

Editing an AOR

NOTE
You cannot edit system AORs.

To make changes to an existing AOR, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the AOR you want to edit in the **AOR** table and click **Edit**.

   The **Edit AOR** dialog box displays.

3. Complete step 3 through step 5 in "Creating an AOR" on page 195.

4. Click **OK** to save the AOR and close the **Edit AOR** dialog box.

   If you make changes to the user's role or AOR while the user is logged in, a confirmation message displays. When you click **Yes** on the confirmation message, the user is logged out and must log back in to see the changes.

5. Click **Close** to close the **Users** dialog box.

Copying an AOR

NOTE
You cannot duplicate system AORs.

To create a new AOR by copying an existing one, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the AOR you want to copy in the **AOR** table and click **Duplicate**.

   The **Duplicate AOR** dialog box displays.

3. Complete step 3 through step 5 in "Creating an AOR" on page 195.

4. Click **OK** to save the new AOR and close the **Duplicate AOR** dialog box.

   The new AOR displays in the **AOR** table of the **Users** dialog box. To add this AOR to a user, follow the instructions in "Assigning roles and areas of responsibility to a user account" on page 188.

5. Click **Close** to close the **Users** dialog box

Deleting an AOR

NOTE
You cannot delete system AORs.

To delete an AOR, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the AOR you want to delete in the **AOR** table and click **Delete**.
3. Click **Yes** on the confirmation message.
4. Click **Close** to close the **Users** dialog box.

Assigning products to an AOR

You can assign hostsIP products to an AOR from the **Add**, **Edit**, or **Duplicate AOR** dialog box.

To assign hostsIP products to an AOR, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Click **Add**, **Edit**, or **Duplicate** under the **AOR** table.

   The **Add AOR**, **Edit AOR**, or **Duplicate AOR** dialog box displays.

3. Click the **Hosts** tab.
4. Select the hosts you want to assign to the AOR in the **Available Hosts** table and click the right arrow button to move the products to the **Selected Products** table.

   Select multiple hosts by holding down the CTRL key and clicking more than one host.

5. Click the **IP Products** tab.
6. Choose one of the following options:
   - Select the IP products you want to assign to the AOR in the **Available IP Products** table and click the right arrow button to move the products to the **Selected Products** table.

     Select multiple products by holding down the CTRL key and clicking more than one product.

   - Select the **System Product Group** or **User-Defined Device Group** you want to assign to the AOR in the **Available IP Products** table and click the right arrow button to move the groups to the **Selected Products** table.

     All products in the group will be assigned to the AOR.

   - (Application products (ServerIron) only) Select the *Application_Product* **Group** you want to assign to the AOR in the **Available IP Products** table and click the right arrow button to move the group to the **Selected Products** table.

     Select multiple products by holding down the CTRL key and clicking more than one product.

NOTE
You must include the Application product to which the real or virtual servers in the AOR for the complete association to display in VIP manager.

NOTE
Virtual or real server IP addresses, configured for an Application product, display as a two FLAT list under the associated Application product tree node in the **Available IP Products** table.

7. Click **OK** to save your work
8. Click **Close** to close the **Users** dialog box.

Removing products from an AOR

You can remove hostsIP products from and AOR from the **Edit AOR** or **Duplicate AOR** dialog box.

To remove hostsIP products from the AOR, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Click **Edit** or **Duplicate** under the **AOR** table.

   The **Edit AOR** or **Duplicate AOR** dialog box displays.

3. In the **Selected Products** table, select the products or groups you want to remove and click the left arrow button.

   Select multiple products or groups by holding down the CTRL key and clicking more than one item.

4. Click **OK** to save your work.
5. Click **Close** to close the **Users** dialog box.

Password policies

NOTE
You must have User Management Read and Write privileges to configure password policy.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. The purpose of the password policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Configuring a password policy

To configure password policies for all user accounts, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Click the **Policy** tab.

3. Configure the password expiration by completing the following steps.
    a. Enter the maximum number of days that can elapse before a password must be changed by the user in the **Password Age** field.

        Valid values are 0 through 999. The default is 0, which means the policy is disabled.

    b. Enter the number of days to warn the user prior to password expiration in the **Warning Period** field.

        Only enabled when the **Password Age** value is greater than zero. Valid values are 0 through 998. The default is 0. The **Warning Period** value must be less than the **Password Age** value.

4. Enter the number of unique passwords you must use before you can reuse a password in the **History Count** field.

    Valid values are 1 through 24. The default is 1. When you update the **History Count** value, the current password history is not cleared.

5. Configure the password format by completing the following steps.
    a. Select the **Empty Password - Allow** check box to allow user accounts to be created or edited with empty passwords or to allow passwords with any format.

        Empty Password is enabled by default.

    b. Enter the minimum password length in the **Minimum Length** field.

        Only enabled when the **Empty Password - Allow** check box is clear. Valid values are 4 through 127. The default is 8.

    c. Enter the minimum number of uppercase characters required in the **Upper Case Characters** field.

        Only enabled when the **Empty Password - Allow** check box is clear. Valid values are 0 through 127. The default is 0.

    d. Enter the minimum number of lowercase characters required in the **Lower Case Characters** field.

        Only enabled when the **Empty Password - Allow** check box is clear. Valid values are 0 through 127. The default is 0.

    e. Enter the minimum number of digits required in the **Number of Digits** field.

        Only enabled when the **Empty Password - Allow** check box is clear. Valid values are 0 through 127. The default is 0.

    f. Enter the minimum number of punctuation characters required in the **Punctuation Required** field.

        Only enabled when the **Empty Password - Allow** check box is clear. Valid values are 0 through 127. The default is 0.

    g. Enter the maximum number that the same character can repeat without a different intervening character in the **Maximum Repeat** field.

        Only enabled when the **Empty Password - Allow** check box is clear. Valid values are 0 through 127. The default is 2.

    h. Enter the maximum number of sequence characters from the ASCII collating series or keyboard sequences in the **Maximum Sequence** field.

For example, 'ab' is a sequence of 2 and '456' is a sequence of 3.

Only enabled when the **Empty Password - Allow** check box is clear. Valid values are 0 through 127. The default is 1.

6. Configure the password lockout support by completing the following steps.
   a. Enter the number of failed login attempts allowed before the user account is locked out in the **Lockout Threshold** field.

      Valid values are 0 through 999. The default is 0 (disabled).

   b. Enter the time frame after which the account automatically unlocks and resumes normal operation in the **Lockout Duration** field.

      Only enabled when the **Lockout Threshold** is greater than zero. If you specify zero, the user account is locked out indefinitely until an administrator manually unlocks it. Valid values are 0 through 99999. The default is 30.

7. Configure the password login policy by completing the following steps.
   a. Select **Concurrent Login** or **Single Login** from the **Login Mode** list.

      Single Login allows only one user to login at a time. If you selected **Single Login**, continue with step b.

      Concurrent Login allows multiple users to login at the same time. If you selected **Concurrent Login**, go to step 8.

   b. Select **Reject New Sessions** or **Logout Existing Sessions** from the **Action** list.

8. To configure the application to use the CLI login credentials of the user for all CLI deployments, select the **Use User CLI Credential** check box in the **CLI Credential** area.

   A confirmation message displays. Click **Yes** on the message.

   Make sure to configure the User CLI Credentials in the User Profile dialog box (refer to "Configuring CLI credentials" on page 209). These credentials will be used for all CLI deployments and will override the CLI credentials configured during discovery or in the CLI template.

9. Click **View Policy Violators** to view the user accounts affected by any policy violations caused by your changes to the **Policy** tab before you save your work.

   If none of the user accounts violate the updated password policy, an empty **View Policy Violators** dialog box displays.

10. Click **Apply**.
11. Click **Yes** on the confirmation message.
12. Click **Close** to close the **Users** dialog box.

Viewing password policy violators

To view password policy violators, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Click the **Policy** tab.

3. Click **View Policy Violators**.

   The **View Policy Violators** dialog box displays.

4. Review the password policy violator details.

   The **View Policy Violators** dialog box includes the following details:

   - **User ID** — Displays the identifier of the user who violated the password policy.
   - **Full Name** — Displays the full name of the user who violated the password policy.
   - **Reason** — Displays the reason the user violated the password policy.

5. Click **Close** on the **View Policy Violators** dialog box.
6. Click **Close** on the **Users** dialog box.

Authentication Server Groups on the Management server

NOTE
You must have User Management Read and Write privileges to map roles and AORs to Active Directory (AD) groups.

NOTE
You must configure an Lightweight Directory Access Protocol (LDAP) server as the primary authentication server and set Authentication Server Groups as the authorization preference (refer to "Configuring LDAP server authentication" on page 382).

Authentication Server Groups enable you to configure user access rights to AD groups (including users, contacts, computers, and other AD groups) by assigning roles and AORs to groups in the Management application. LDAP provides user authentication and authorization using the AD service in conjunction with LDAP on the switch.

Assigning roles and AORs to an AD group

Using Authentication Server Groups, you assign users to groups within the Authentication Server Groups server, and assign roles and AORs to the groups within the Management application.

To assign roles and AORs to an AD group, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Click the **Authentication Server Groups** tab.
3. Select the roles and AORs you want to assign to the AD group in the **Available Roles / AORs** table.

   Select multiple roles and AORs by holding down the CTRL key and clicking more than one role and AOR.

4. Select the AD group to which you want to assign the selected roles and AORs in the **Active Directory Groups** table.

   If the AD group you want does not display in the table, refer to "Loading an AD group" on page 202.

5. Click the right arrow button.

   The selected roles and AORs are moved to the **Active Directory Groups** table.

6. Click **Apply** to save your work

   When you assign roles and AORs to an AD group and save the configurations, when you reopen the **Users** dialog box and select the **Authentication Server Groups** tab, only the configured AD group is available.

Removing roles and AORs from an AD group

To remove roles and AORs from an AD group, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Click the **Authentication Server Groups** tab.
3. Select the roles and AORs you want to remove in the **Active Directory Groups** table.

   Select multiple roles and AORs by holding down the CTRL key and clicking more than one role and AOR.

4. Click the left arrow button.

   The selected roles and AORs are moved to the **Available Roles / AORs** table.

5. Click **OK** to save your work.

Loading an AD group

To load an AD group, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Click the **Authentication Server Groups** tab.
3. Click **Fetch**.

   The **Fetch AD Group** dialog box displays.

4. Select the LDAP server network address from the **Network Address** list.
5. Enter the TCP port number in the **TCP Port** field, if necessary.

   Default is 389 if security is not enabled. Default is 636 if security is enabled.

6. Select the authentication protocol **MD5** from the **Authentication** list.
7. Enter your LDAP server user login name in the **User Name** field.
8. Enter your LDAP server user login password in the **Password** field.
9. Select the **Security Enable** check box to enable the security channel between the Management application server and the LDAP server.

   When you enable security, the TCP port number automatically changes to port 636 and you must enable certificate services on the LDAP server.

10. Click **OK**.

The **Active Directory Groups** table displays with all AD groups available in the specified LDAP server, as well as any AD groups already mapped in the Management server (Local database).

To assign or remove roles and AORs, refer to "Assigning roles and AORs to an AD group" on page 201 or "Removing roles and AORs from an AD group" on page 202.

11. Click **Close** to close the **Users** dialog box.

Deleting an AD group

Deleting an AD group deletes the roles and AORs assigned to the group and removes the group from the **Active Directory Groups** table.

To delete an AD group, complete the following steps.

1. Select one or more AD groups that you want to delete from the **Active Directory Groups** table.
2. Click **Delete**.
3. Click **Yes** on the confirmation message.
4. Click **OK** on the deletion successful message.
5. Click **OK** to save your work.

Creating an AD user account

To create a new user account in Active Directory Users and Computers, complete the following steps. For more information, click **F1** for help or refer to www.microsoft.com.

1. Open the Active Directory Users and Computers console.

   For example, on Windows XP, select **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
2. Right-click the **Users** folder and select **New > User**.
3. Enter a name in the **First name** field.
4. Enter a name in the **Full name** field
5. Enter a logon name in the **User logon name** field.
6. Click **Next**.
7. Select the **Password Never Expires** option and click **Next**.
8. Click **Finish**.
9. Right-click the new user in the **Users** pane and select **Reset Password**.
10. Assign a new password with at least one special character and one number and click **OK**.
11. Close the **Active Directory Users and Computers** dialog box.

Assigning an AD user to an AD group

To assign a new group in Active Directory Users and Computers, complete the following steps. For more information, click **F1** for help or refer to www.microsoft.com

1. Open the Active Directory Users and Computers console.

   For example, on Windows XP, select **Start > Programs > Administrative Tools > Active Directory Users and Computers**.

2. Right-click the new user in the **Users** pane and select **Add to a Group**.
3. Enter the group name in the **Enter the object name to select** text box and click **Check Names**.
4. Click **OK**.

Defining user accounts on the external LDAP server

If you configure the external LDAP server as the primary authentication server in the server management console, you must define roles and AORs in the external LDAP server to match the Management application roles and AORs.

Configuring roles and AORs on the external LDAP server

Open the Management console on the Active Directory installed server and complete the following steps.

1. Select **Start > Run**.
2. Type **mmc** and press **Enter**.
3. Select **File > Add/Remove Snap-in**.
4. Click **Add**.
5. Select **Active Directory Schema** from the **Available standalone snap-ins list** and click **Add**.
6. Click **Close**.
7. Right-click the **Attributes** folder (Console Root/Active Directory Schema/ Attributes) and select **New > Attribute**.
8. Create the NmAors attribute by completing the following steps.
   a. Enter NmAors in the **Common Name** field.
   b. Enter NmAors in the **LDAP Display Name** field.
   c. Enter a unique object identifier in the **Unique x500 Object ID** field.
   d. Enter a description of the attribute in the **Description** field.
   e. Select **Case Insensitive String** in the **Syntax** list.
   f. Click **OK**.
9. Right-click the **Attributes** folder (Console Root/Active Directory Schema/ Attributes) and select **New > Attribute**.
10. Create the NmRoles attribute by completing the following steps.

a. Enter NmRoles in the **Common Name** field.

b. Enter NmRoles in the **LDAP Display Name** field.

c. Enter a unique object identifier in the **Unique x500 Object ID** field.

d. Enter a description of the attribute in the **Description** field.

e. Select **Case Insensitive String** in the **Syntax** list.

f. Click **OK**.

11. Close the Management console.

Configuring authorization details on the external LDAP server

Open the **ADSI Edit** dialog box on the Active Directory installed server.

1. Select **Start > Run**.
2. Type **adsiedit.msc** and press **Enter**.
3. Right-click **CN=***User_Name* in the **CN=Users** directory and select **Properties**.

   Where *User_Name* is the name of the user you created in "Creating an AD user account" on page 203.
4. Select **NmAors** in the **Attributes** list and click **Edit**.
5. Enter the areas of responsibility (such as, All Fabrics, All IP Products) in the **Value** field and click **OK**.
6. Select **NmRoles** in the **Attributes** list and click **Edit**.
7. Enter the Management application user roles (such as Host Administrator, IP System Administrator, Network Administrator, Operator, Report User Group, SAN System Administrator, Security Administrator, Security Officer, and Zone Administrator) in the **Value** field and click **OK**.
8. Close the **ADSI Edit** dialog box.

User profiles

User profiles contain the standard identification information of the user account, such as name, password, phone number, and e-mail address. The Management application enables you to make the following changes to your user profile:

- Change your name
- Change your password
- Change your user account description
- Change your phone number
- Change your e-mail address
- View your account state
- View your password policy
- Reset Management application messages
- Enable e-mail notification
- Configure e-mail notification

- Configure CLI credentials

Viewing your user profile

To view your user profile, complete the following steps. To edit your user profile, refer to "Editing your user profile" on page 207.

1. Select **Server > User Profile**.

   The **User Profile** dialog box displays the following information:

   - **User ID** — Displays your user identifier.
   - **Full Name** — Displays the name if entered while adding a user; otherwise, this field is blank.
   - **Password** — Displays your password as dots (.). If the password policy is configured for an empty password, this field is blank. To change your password, refer to "Changing your password" on page 207.
   - **Confirm Password** — Displays your password as dots (.). If the password policy is configured for an empty password, this field is blank.
   - **Description** — Displays your description if entered while adding a user; otherwise, this field is blank.
   - **Phone Number** — Displays your phone number if entered while adding a user; otherwise, this field is blank.
   - **Account State** — Displays the current state of the account. Valid states include:
     - Active
     - Locked out by user manager
     - Locked out threshold reached
     - Password expired
     - Password format policy violated
     - Password history policy violated
   - **E-mail Notification Enable** check box — Select to enable e-mail notification.
   - **Filter** — Click to configure e-mail notification (refer to "Configuring e-mail notification" on page 209).
   - **E-mail Address** — Displays your e-mail, text message, or page addresses if entered while adding a user; otherwise, this field is blank.
   - **Password Age** — Displays the age of the password in days. Default is zero.
   - **Password Policy View** button — Click to display the current password policy (refer to "Viewing your password policy" on page 208).
   - **CLI Credential Configure** button — Click to display the **CLI Credentials** dialog box (refer to "Configuring CLI credentials" on page 209).
   - **Optional Messages Reset** button — Click to reset all optional messages to the default behavior. For more information, refer to "Resetting optional messages" on page 209.

2. Click **OK** on the **User Profile** dialog box.

Editing your user profile

To edit your user profile, complete the following steps.

1. Select **Server > User Profile**.

   The **User Profile** dialog box displays.

2. Change your name in the **Full Name** field.
3. Change your password in the **Password** and **Confirm Password** fields.

   Passwords display as dots (.).

4. Change your user profile description in the **Description** field.
5. Change your phone number in the **Phone Number** field.
6. Select the **E-mail Notification Enable** check box to enable e-mail notification.

   Clear the **E-mail Notification Enable** check box to disable e-mail notification.

7. Click **Filter** to set up basic event filters.

   For step-by-step instructions about setting up basic event filters, refer to "Setting up basic event filtering" on page 1144.

8. Change your e-mail, text message, or page address in the **E-mail Address** field.

   Enter more than one e-mail address, separating each with a semi-colon. To send a text message or page via e-mail, use the following format *number@carrier.com*, where *number* is your phone number and *carrier.com* is the SMS server. For example, 3035551212@txt.att.net (text message) or 3035551212@page.att.net (page).

   NOTE
   Check with your carrier for the exact e-mail address.

9. To configure the application to use the CLI login credentials of the user for all CLI deployments, **Configure**.

   To configure the User CLI Credentials, refer to "Configuring CLI credentials" on page 209. These credentials will be used for all CLI deployments and will override the CLI credentials configured during discovery or in the CLI template.

10. Click **OK** on the **User Profile** dialog box to save your changes.

Changing your password

To change your password from your user profile, complete the following steps.

1. Select **Server > User Profile**.

   The **User Profile** dialog box displays.

2. Change your password in the **Password** and **Confirm Password** fields.

   Passwords display as dots (.).

3. Click **OK** on the **User Profile** dialog box to save your changes.

If your password expires or your current password violates the password policy, you will be prompted to change your password from the **Change Password** dialog box. To view your password policy, click **Password Policy - View**.

To change your password from the **Change Password** dialog box, complete the following steps.

1. Enter your current password in the **Existing Password** field.
2. Enter your new password in the **New Password** and **Confirm Password** fields.

   Passwords display as dots (.).
3. Click **OK** to save your new password.

Viewing your password policy

To view your password policy, complete the following steps.

1. Select **Server > User Profile**.

   The **User Profile** dialog box displays.
2. Click **Password Policy - View** to display your password policy.

   The **View Password Policy** dialog box displays.

   - **Password History Count** — The number of unique passwords you must use before you can reuse a password.
   - **Empty Password** — Whether or not to allow empty passwords.
   - **Minimum Length** — The minimum length allowed for the password.
   - **Upper Case Characters** — The minimum number of uppercase characters required in the password.
   - **Lower Case Characters** — The minimum number of lowercase characters required in the password.
   - **Number of Digits** — The minimum number of digits required in the password.
   - **Punctuation Required** — The minimum number of punctuation characters required in the password.
   - **Maximum Repeat** — The maximum number that the same character can repeat without a different intervening character in the password.
   - **Maximum Sequence** — The maximum number of sequence characters from the ASCII collating series or keyboard sequences in the password.
3. Click **OK** on the **Password Policy** dialog box.
4. Click **OK** on the **User Profile** dialog box.

Resetting optional messages

To reset all Management application optional messages to their default behaviors, complete the following steps.

1. Select **Server > User Profile**.

   The **User Profile** dialog box displays.

2. Click **Optional Messages Reset**.

   The **Password Policy** dialog box displays.

3. Click **Yes** on the confirmation message.

   A successful reset message displays.

4. Click **OK** on the **User Profile** dialog box.

Configuring e-mail notification

To configure and enable e-mail notification, complete the following steps.

1. Select **Server > User Profile**.

   The **User Profile** dialog box displays.

2. Select the **E-mail Notification - Enable** check box to enable e-mail notification.

3. Click **Filter** to set up basic event filter.

   For step-by-step instructions about setting up basic event filters, refer to "Setting up basic event filtering" on page 1144.

4. Enter your e-mail, text message, or page address in the **E-mail Address** field.

   Enter more than one e-mail address, separating each with a semi-colon. To send a text message or page via e-mail, use the following format *number@carrier.com*, where *number* is your phone number and *carrier.com* is the SMS server. For example, 3035551212@txt.att.net (text message) or 3035551212@page.att.net (page).

   NOTE
   Check with your carrier for the exact e-mail address.

5. Click **OK** on the **User Profile** dialog box.

Configuring CLI credentials

NOTE
This feature requires a Trial or Licensed version.

To configure CLI credentials, complete the following steps.

1. Select **Server > User Profile**.

   The **User Profile** dialog box displays.

2. Click **Configure** to set up basic event filter.

   The **CLI Credential** dialog box displays.

3. Enter the user name for the product in the **Product Login Account - Username** field.
4. Enter the password for the product in the **Product Login Account - Password** field.

NOTE
If Telnet is used to log in to the device and Telnet only requires a password, then enter the password in the **Password** field and leave the **Username** field blank.

5. (IronWare only) Enter the user name assigned to management privilege levels on the device in the **Product Enable Account - Username** field.
6. (IronWare only) Enter the password assigned to management privilege levels on the device in the **Product Enable Account - Password** field.

NOTE
If a device only requires the enable password, then enter the password in the **Password** field and leave the **Username** field blank.

7. Click **OK** on the **CLI Credential** dialog box.
8. Click **OK** on the **User Profile** dialog box.

   Once you configure the CLI credentials, you must turn on the CLI credential policy through the Users dialog box.

Configuring the CLI credential policy

NOTE
You must have User Management Read and Write privileges to configure user accounts.

NOTE
This feature requires a Trial or Licensed version.

To configure the application to use the CLI login credentials of the user for all CLI deployments, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.
2. Click the **Policy** tab.
3. Select the **Use User CLI Credential** check box in the **CLI Credential** area.

   A confirmation message displays. Click **Yes** on the message.

   Make sure to configure the User CLI Credentials in the User Profile dialog box (refer to "Configuring CLI credentials" on page 209). These credentials will be used for all CLI deployments and will override the CLI credentials configured during discovery or in the CLI template.
4. Click **OK** on the **Users** dialog box.

Chapter

Dashboard Management

7

In this chapter

Dashboard overview

NOTE
Only devices in your area of responsibility (AOR) display in the dashboard.

The **Dashboard** tab (Figure 80) displays the status widgets, performance monitors, and the Master Log. You can also display additional status widgets and performance monitors, as needed. The Management application has the following default dashboards: Product Status and Traffic and IP Port Health

The dashboard provides a high-level overview of the network and the current states of managed devices. This allows you to easily check the status of the devices on the network. The dashboard also provides several features to help you quickly access reports, device configurations, and system logs.

The dashboard updates regardless of the currently selected tab (**IP**) or the LAN size. However, data may become momentarily out of sync between the dashboard and other areas of the application. For example, if you remove a product from the network while another user navigates from the dashboard to a more detailed view of the product, the product may not appear in the detailed view.

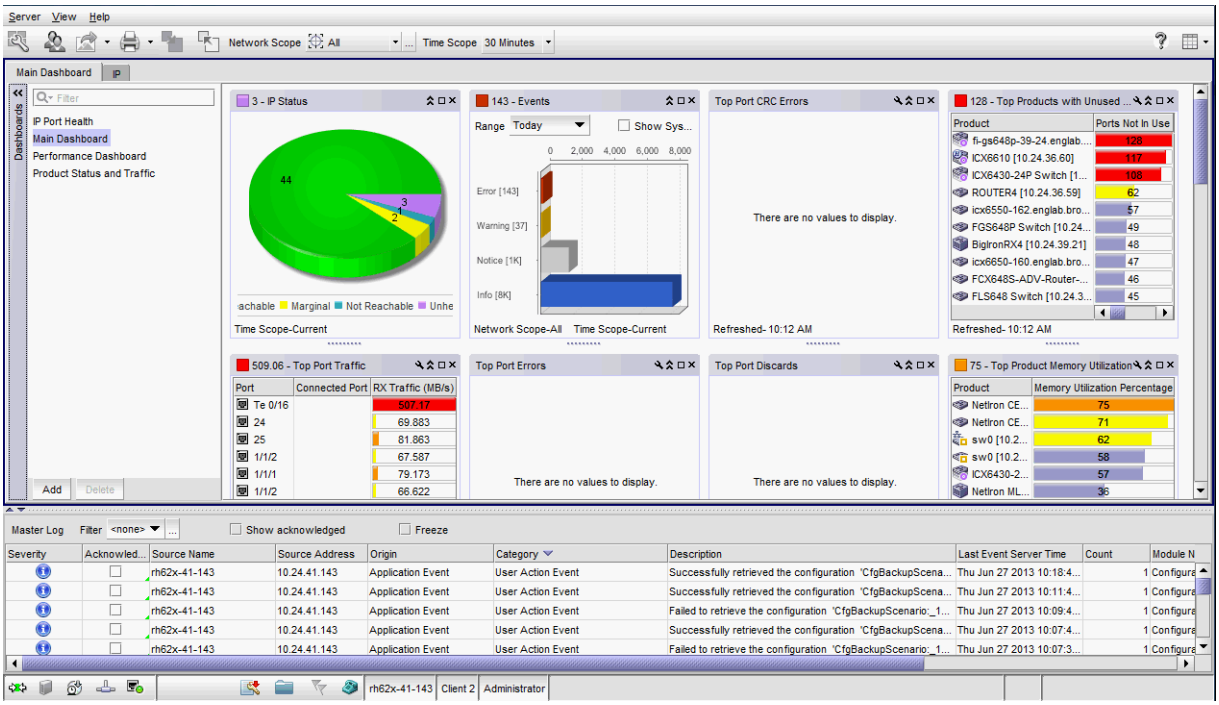


FIGURE 80 **Dashboard tab**

1. **Menu bar** — Lists commands you can perform on the dashboard. For a list of **Dashboard** tab menu commands, refer to "Dashboard main menus" on page 1261.

   The dashboard also provides a shortcut menu to reset the dashboard back to the defaults. Reset the dashboard back to the default settings by right-clicking in the white space and selected **Reset to Default**.

2. **Toolbar** — Provides buttons that enable quick access to dialog boxes and functions. For a list of Dashboard tab toolbar options, refer to "Dashboard toolbar" on page 213.

3. Dashboard tab — Provides a high-level overview of the network managed by Management application server.

4. **IP** tab — Displays the Master Log, Minimap, Connectivity Map (topology), and Product List. For more information, refer to the "IP tab overview".

5. Dashboard expand navigation bar — The expand navigation bar is located left of the status widgets or performance monitors and provides a list of dashboards to choose from as well as buttons to perform add and delete functions. For more information, refer to "Dashboards expand navigation bar" on page 214.

6. **Widgets** — Displays operational status, inventory status, event summary, and overall network or fabric status as well as performance monitors. For more information, refer to "Status widgets" on page 224 and "Performance monitors" on page 237.

7. **Master Log** — Displays all events that have occurred on the Management application. For more information, refer to "Master Log" on page 287.

8. **Status bar —** Displays the connection, port, product, special event, Call Home, and backup status, as well as Server and User data. For more information about the status bar, refer to "Status bar" on page 289.

Dashboard toolbar

The toolbar (Figure 81) is located beneath the menu bar and provides icons and buttons to perform various functions.

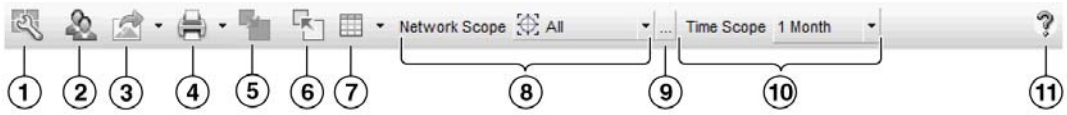


FIGURE 81 Toolbar

The toolbar contains the following icons and buttons:

1. **Customize Dashboard** — Displays the **Customize Dashboard** dialog box. Use to configure which status widgets and performance monitors display on the **Dashboard** tab and **Performance Dashboard**. For more information, refer to "Customizing the dashboard widgets and monitors" on page 217
2. **Users —** Displays the **Users** dialog box. Use to configure users, user groups, and permissions. For more information, refer to "User accounts" on page 185.
3. **Export** list — Saves the current dashboard display (all widgets) or a selected widget in a .png format. For more information, refer to "Exporting the dashboard display" on page 219.
4. **Print** list — Prints the dashboard display (all widgets) or a selected widget. For more information, refer to "Printing the dashboard display" on page 219.
5. **Attach** — Returns the dashboard to the main window. For more information, refer to "Attaching and detaching the Dashboard tab" on page 219.
6. **Detach** — Detaches the dashboard to a separate window. For more information, refer to "Attaching and detaching the Dashboard tab" on page 219.
7. Dashboard display list — Use to select how to display the status widgets and performance monitors in the dashboard. For more information, refer to "Setting the dashboard display" on page 217.
8. **Network Scope** — Use to select the network you want to display in the dashboard. For more information, refer to "Setting the network scope" on page 220.
9. **Network Scope** ellipsis button — Displays the **Edit Scopes** dialog box. Use to configure or delete product and port scopes. For more information, refer to "Creating a customized network scope" on page 221.
10. **Time Scope** list — Use to select the specific duration for which you want to display data. For more information, refer to "Setting the data display time frame" on page 222.
11. **Help** — Displays the online help.

Dashboard messages

The dashboard message bar (Figure 82) only displays when the Network Scope or Time Scope has changed. You can also view all dashboard messages and clear them.

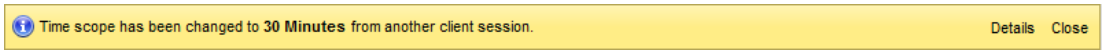


FIGURE 82 Dashboard message bar

The toolbar contains the following fields and components:

1. **Details** button — Use to view dashboard messages.
2. **Close** button — Use to close the dashboard message bar.

Dashboards expand navigation bar

The expand navigation bar (Figure 83) is located left of the status widgets or performance monitors and provides a list of dashboards to choose from as well as buttons to perform add and delete functions.

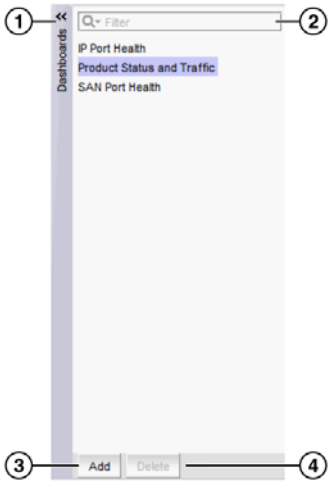


FIGURE 83 Expand navigation bar

The toolbar contains the following fields and components:

1. **Dashboards** expand navigation bar — Use to select the dashboard you want to view from the list. For more information, refer to "Accessing a dashboard" on page 215.
2. **Filter** — Use to search for the dashboard you want to view.
3. **Add** button — Use to create a dashboard. For more information, refer to "Creating a user-defined dashboard" on page 216.
4. **Delete** button — Use to delete the selected user-defined dashboard. For more information, refer to "Deleting a user-defined dashboard" on page 217.

General dashboard functions

The Management application also provides the following general functions which are applicable to all widgets and monitors:

- **Preference persistence —** Any customization you make to the dashboards are persisted in that dashboard. For example, if you customize a dashboard to display the **Events** widget and set the **Range** to **This Hour** in the **Dashboard** tab and set it to **Last 30 Days** in the **Performance Dashboard**, then these preferences persist when you log off and log back in again.
- **Severity** — Most widgets display a severity icon (worst severity of the data shown) next to the widget title. The IP Status and IP and Host Inventory widgets also indicate the number of products with that severity. The Events widget displays a severity icon with the highest severity event color. The Status widget does not display the severity icon.
- **Title bar buttons** — Status widgets have the following three (left to right) title bar buttons: expand/collapse, maximize/minimize, and close. Performance monitors are editable and have the following four (left to right) title bar buttons: edit, expand/collapse, maximize/minimize, and close.
- **Resizing** — All widgets can be resized by dragging the grab bars. Use the vertical grab bars between widget columns to adjust the width of widgets in the adjacent columns. Use the horizontal grab bars to adjust the height of adjacent widget rows.

  Reset the dashboard back to the default size by right-clicking in the white space and selected **Reset to Default**.
- **Zoom in** — Only widgets with a bar graph enable you to zoom in using your mouse. To zoom in, click the upper left of the widget area on which you want to zoom in, drag the mouse to the lower right, and release the mouse button.
- **Zoom out** — Only widgets with a bar graph enable you to zoom out using your mouse. To zoom out, click the lower right widget area on which you want to zoom out, drag the mouse to the upper left, and release the mouse button.
- **Tooltips** — Only widgets with a pie chart or bar graph display tooltips when you pause on a section or bar.
  - For the pie chart widgets, the tooltip displays the name of the category, number of items in that category, and the percentage.
  - For the bar graph widgets, the tooltip displays the count represented by the selected bar.

Accessing a dashboard

From the **Dashboards** expand navigation bar, double-click the dashboard you want to view. Options include:

- **IP Port Health** — Displays preconfigured IP performance monitors. You can display additional status widgets and performance monitors in this dashboard.
- **Product Status and Traffic** — Displays preconfigured status widgets and performance monitors. You can display additional widgets and monitors in this dashboard.
- **SAN Port Health** — Displays preconfigured SAN performance monitors. You can display additional status widgets and performance monitors in this dashboard.
- *User_defined* dashboard — Displays a user-defined dashboard.

The dashboard you selected displays.

Filtering the dashboards list

You can filter the list of dashboards to only display dashboard you need.

1. Click the **Dashboards** expand navigation bar.
2. Enter your filter criteria in the **Filter** text box.
3. To make the filter case sensitive or insensitive, choose one of the following options from the filter icon list:
   - **Case sensitive** — Select to make the filter case sensitive.
   - **Case insensitive** — Select to make the filter case insensitive.
4. To allow wild cards or regular expressions, choose one of the following options from the filter icon list:
   - **Use wildcards** — Select to use wildcards in the **Filter** text box.
   - **Use regular expression** – Select to use a unicode regular expression. Enter a Unicode regular expression in the **Filter** text box.
5. To determine how to match the filter text, choose one of the following options from the filter icon list:
   - **Match from start** — Select to match from the start of the dashboard name.
   - **Match exactly** — Select to match the dashboard name exactly.
   - **Match anywhere** — Select to match text anywhere in the dashboard name.
6. To determine how to handle leaf nodes as well as parent and children nodes, choose one of the following options from the filter icon list:
   - **Match leaf node only** — Select to only include leaf nodes in the filter.
   - **Hide nodes without children** — Select to exclude nodes without children from the filter.
   - **Keep the children if any of their ancestors match** — Select to include children in the filter when any of their ancestors match.
7. Press **Enter**.

   The filter results display in the **Dashboards** expand navigation bar. To stop the filter, click the stop filter (X) icon in the **Filter** text box.

Creating a user-defined dashboard

You can create a dashboard and customize it with the status widgets and performance monitors you need to monitor your network.

1. Click the **Dashboards** expand navigation bar.
2. Click **Add**.

   The **Add Custom Dashboard** dialog box displays.
3. Enter a name and description for the dashboard.
4. Select the **Copy active dashboard widgets** to include all widget in the current dashboard to this dashboard.
5. Click **OK**.

The new dashboard displays in the **Dashboards** expand navigation bar and becomes the active dashboard.

Deleting a user-defined dashboard

You can delete a user-defined dashboard.

1. Click the **Dashboards** expand navigation bar.
2. Select the dashboard you want to delete and click **Delete**.
3. Click **Yes** on the confirmation message.

Setting the dashboard display

You can set the dashboard to minimize or expand all status widgets and performance monitors as well as return to the default settings.

Select one of the following options from the dashboard display list:

- **Collapse All** — Select to minimize all widgets and monitors on the dashboard.
- **Expand All** — Select to expand all widgets and monitors on the dashboard.
- **Reset to Default** — Select to reset the dashboard to the default display settings.

Customizing the dashboard widgets and monitors

1. From the dashboard, click the **Customize Dashboard** icon.

   The **Customize Dashboard** dialog box displays.

2. Click the **Status** tab.

   The preconfigured general status widgets display.

3. Select the **Display** check box in the **General Status Widgets** list for each status widget you want to add to the dashboard.

   Clear the check box to remove the associated status widget from the dashboard.

   The **General Status Widgets** list contains the following additional information:

   - **Title** — The name of the status widget. For more information, refer to "Status widgets" on page 224.
   - **Description** — A general description of the status widget.

4. Click the **Performance** tab (Figure 84).

   The preconfigured performance monitors display. You can create up to 100 performance monitors; however, you can only display up to 30 performance monitors. For more information about performance monitors, refer to "Performance monitors" on page 237.

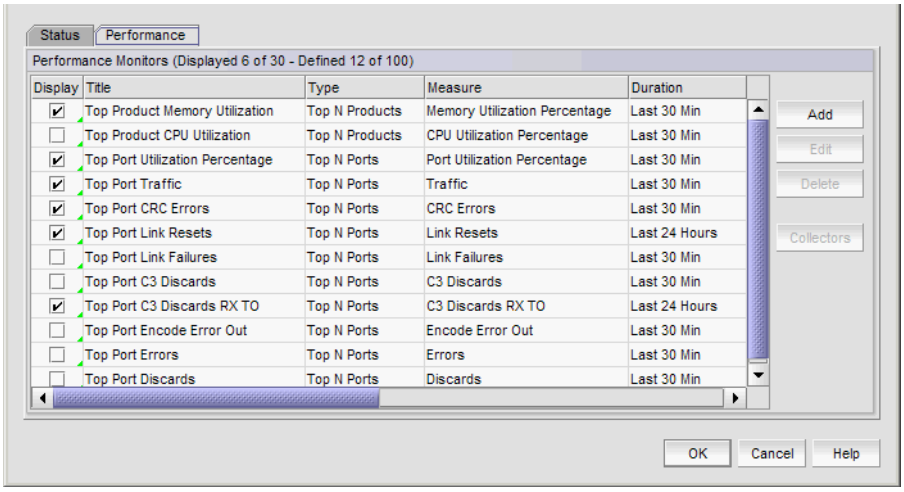


FIGURE 84 **Customize Dashboard dialog box, Performance tab**

5. Select the **Display** check box in the **Performance Monitors** list for each performance monitor you want to add to the dashboard.

   Clear the check box to remove the associated performance monitor from the dashboard.

   The **Performance Monitors** list contains the following additional information:

   - **Title** — The name of the performance monitor. For more information, refer to "Performance monitors" on page 237
   - **Type** — The type of monitor.
   - **Measure** — The performance measures included in the monitor.
   - **Data Collectors —** The data collectors that provide data for the monitor.

6. Click **Add** to add a new performance monitor. For more information, refer to "Configuring a user-defined product performance monitor" on page 270.

7. Click **Edit** to edit an existing performance monitor. For more information, refer to "Configuring a user-defined product performance monitor" on page 270 or "Editing a preconfigured performance monitor" on page 263.

8. Select one or more user-defined monitors and click **Delete** to delete the user-defined performance monitors.

9. Select a monitor and click **Collectors** to launch the **Historical Data Collectors** dialog box. For more information, refer to "Displaying historical data collectors" on page 996.

10. Click **OK** to close the **Customize Dashboard** dialog box.

Exporting the dashboard display

You can export the current dashboard display (all widgets and monitors) or a selected widget or monitor in a .png format.

1. Select one of the following options from the **Export** list:
   - **Dashboard** — Exports the current dashboard.
   - *Name* — Exports the selected widget (where *Name* is the name of the widget or monitor on the dashboard).

   The **Export Dashboard to PNG File** or **Export** *Name* **to PNG File** dialog box displays.
2. Browse to the location you want to save the file.
3. Enter a name for the snapshot in the **File Name** field, if needed.

   Export uses the following naming convention: *Name_yyyy_mm_dd_hh_mm_ss*.png.
4. Click **Save**.

   The file is saved to the location you selected.

Printing the dashboard display

You can print the current dashboard display (all widgets and monitors) or a selected widget or monitor.

1. Select one of the following options from the **Print** list:
   - **Dashboard** — Prints the current dashboard.
   - *Name* — Prints the selected widget (where *Name* is the name of the widget or monitor on the dashboard).

   The **Page Setup** dialog box displays.
2. Change the page setup options, as needed.
3. Click **OK**.

Attaching and detaching the Dashboard tab

You can detach the **Dashboard** tab from the main application to display in a separate window.

To detach the **Dashboard** tab, click the Detach icon. The **Dashboard -** *Dashboard_Name – Application_Name* window displays.

Reattach the **Dashboard** to the main application by clicking the Attach icon or by closing the **Dashboard -** *Dashboard_Name – Application_Name* window. The **Dashboard** tab displays in the main application window.

Setting the network scope

You can configure the dashboard to display all objects in your area of responsibility (AOR) or a subset of objects (fabrics, devices, or groups).

NOTE
Network scope does not affect the Events widget. The Events widget always includes all objects in your AOR.

From the dashboard, select a network from the **Network Scope** list. Options include:

- All
- Any SAN fabric
- Any Ethernet fabric
- Any system-defined group
- Any user-defined group
- Any user-defined customized network

If you select a fabric scope, violation counts display for all products and ports in the fabric.

If you select a product scope, violation counts display for the selected products and the ports that belong to the selected products.

If you select a port scope, violation counts display for the specified ports and the products to which the ports belong. If any of the selected ports are initiator or target ports, violation counts display for the attached switch port.

Select **All** to include all managed and monitored fabrics or groups in your AOR. The default is **All**. If the fabric or group you select is deleted from discovery, the widget refreshes and returns to the default (**All**).

Creating a customized network scope

You can create a network scope from any objects in your AOR. You can create network scopes based on Fabrics, Products, Product Groups, or Ports.

1. Click the **Network Scope** ellipsis button.

   The **Edit Scope** dialog box displays with a list of existing user-defined network scopes in the **Network Scopes** list.

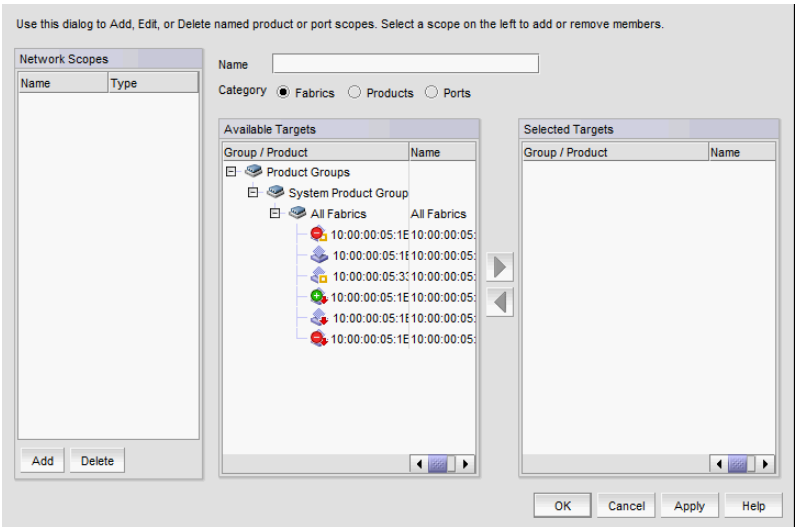


FIGURE 85 **Edit Scopes dialog box**

2. Click **Add**.

   A new network scope displays in the **Network Scopes** list.

3. Enter a name for the scope in the **Name** field.

4. Select one of the following options:

   - **Fabrics** — Select to create your network from one or more fabrics.
   - **Products** — Select to create your network from one or more products or product groups.
   - **Ports** — Select to create your network from one or more ports or port groups.

5. Select one or more the objects you want to include in the network from the **Available** list and click the right arrow button.

   The objects display in the **Selected** list. To remove an object from the **Selected** list, select it and click the left arrow button.

6. Click **OK** to save your changes and close the **Edit Scope** dialog box.

Editing a user-defined network scope

You can edit any user-defined network scope.

1. Click the **Network Scope** ellipsis button.

   The **Edit Scope** dialog box displays with a list of existing user-defined network scopes in the **Network Scopes** list.

2. Select the network scope you want to edit in the **Network Scopes** list.

   The network scope details display in the right side fields.

3. Change the name for the scope in the **Name** field, if needed.

4. To add objects, select one or more the objects you want to include in the network from the **Available Targets** list and click the right arrow button.

   The objects display in the **Selected Targets** list.

5. To remove an object from the **Selected Targets** list, select it and click the left arrow button.

6. Click **OK** to save your changes and close the **Edit Scope** dialog box.

Deleting a user-defined network scope

You can edit any user-defined network scope.

1. Click the **Network Scope** ellipsis button.

   The **Edit Scope** dialog box displays with a list of existing user-defined network scopes in the **Named Scopes** list.

2. Select the network you want to delete in the **Named Scopes** list.

3. Remove all objects from the **Selected Targets** list.

   To remove an object from the **Selected Targets** list, select it and click the left arrow button.

4. Click **Delete**.

5. Click **OK** to save your changes and close the **Edit Scope** dialog box.

Setting the data display time frame

Setting the time scope in the dashboard toolbar configures the data display time range for the status widgets and performance monitors that include a time range.

NOTE
Time scope does not affect the Events widget. For the Events widget, you set the time scope within the widget.

NOTE
sFlow monitors only display data for up to 1 day.

From the dashboard, select on of the following duration options for which you want to display data from the **Time Scope** list.

- **30 Minutes** — Displays data for the previous half hour.
- **1 Hour** — Displays data for the previous hour.
- **6 Hours** — Displays data for the previous 6 hours.
- **12 Hours** — Displays data for the previous 12 hours.
- **1 Day** — Displays data for the previous day.
- **3 Days** — Displays data for the previous 3 days.
- **1 Week** — Displays data for the previous week.
- **1 Month** — Displays data for the previous month.

The displayed data changes to the new time frame for any status widget or performance monitor affected by time.

Default dashboards

The Management application provides preconfigured dashboards which provide high-level overview of the network, the current states of managed devices, and performance of devices, ports, and traffic on the network.

Product Status and Traffic dashboard

The Product Status and Traffic dashboard provides the following preconfigured status widgets and performance monitors:

- IP Inventory widget
- Status widget
- Events widget
- Out of Range Violations widget
- Top Product Memory Utilization monitor
- Top Product CPU Utilization monitor
- Top Products with Unused Ports monitor
- Top Port Utilization Percentage monitor (includes details for all ports, Initiator ports, ISL ports, and Target ports)
- Bottom Port Utilization Percentage monitor (includes details for all ports, Initiator ports, ISL ports, and Target ports)

IP Port Health

The IP Ports Health dashboard provides the following preconfigured performance monitors:

- Top Port Errors monitor
- Top Port CRC Errors monitor
- Top Port Discards monitor
- Top Port Receive EOF monitor

- Top Port Underflow Errors monitor
- Top Port Overflow Errors monitor
- Top Port Runtime Errors monitor
- Top Port Too Long Errors monitor
- Top Port Alignment Errors monitor

Status widgets

The Management application provides the following preconfigured status widgets:

- Access Point Status widget — Pie chart view of access point devices categorized by operational and reachability status
- Events widget — Bar chart view of events grouped by severity and range
- Host Adapter Inventory widget — Stacked bar chart view of Host Adapters grouped by selected category
- IP Inventory widget — Stacked bar chart view of IP devices grouped by operational status and selected category
- IP Status widget — Pie chart view of IP devices categorized by operational and reachability status
- Out of Range Violations widget — Table view of all out of range threshold violations reported by Network OS devicesPort Health Violations widget — Table view of out of range port health violations. There are four versions of this monitor based on the type of port: All ports, initiator ports, ISL ports, and Target ports.
- Status widget — List view of various status attributes

Access Point Status widget

The **Access Point Status** widget displays the access point (AP) status as a pie chart.

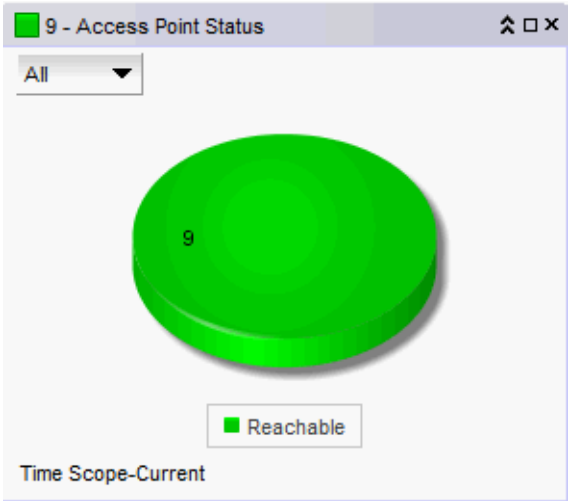


FIGURE 86 Access Point Status widget

The **Access Point Status** widget includes the following data:

- Severity icon/product count/widget title — The color of the worst status followed by the product count with that status displays before the widget title.
- **Show** list — A list of available managed AP products.
- Pie chart — The AP status as a percentage of the total number of devices.

  The pie chart displays the percentage in various colors on each slice. Tooltips showing the number of devices in that state are shown when you pause on the slice. When there is one status category with less than one percent of the total number of devices, the status widget displays the number of devices in each category on each slice.
- Color legend — Displays the color legend below the pie chart using the color codes in Table 21.

TABLE 21 AP status color codes

Color	Type
Green	Online — AP is managed by controller and online.
Red	Offline — AP is managed by controller, but is offline.
Gray	Pending Adoption — Controller found AP but not managed.

Customizing the Access Point Status widget

You can customize the **Access Point Status** widget to display status for a specific product.

Change the grouping by selecting one of the following from the **Show** list:

- **All —** Displays all the AP products.
- **AP7131** — Displays only AP 7131 products.
- **AP6511** — Displays only AP 6511 products.
- **AP650 —** Displays only AP 650 products.

Accessing additional data from the Access Point Status widget

Double-click a section in the **Access Point Status** widget to navigate to a filtered view of the **AP Products** report.

Events widget

The **Events** widget (Figure 87) displays the number of events by severity level for a specified time range as a stacked bar graph.

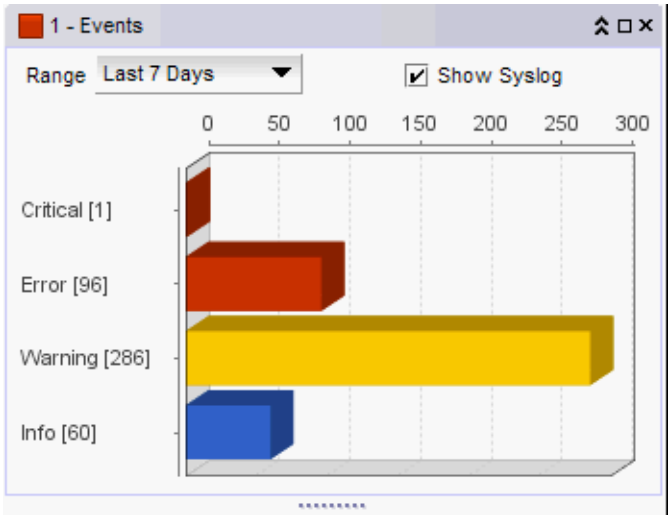


FIGURE 87 Events widget

The **Events** widget includes the following data:

- Severity icon/widget title/event count — The color of the worst severity followed by the event count with that severity displays before the widget title.
- **Range** list — Use to customize this widget to display a specific time range. Options include: This Hour, Last Hour, Today, Yesterday, Last 7 Days, and Last 30 Days.
- **Show Syslog** check box — Select to include Syslog information (default) on the Event Summary.
- Bar chart — The event severity using the color codes in Table 22.

TABLE 22 Event severity color codes

Color	Severity
Red ( )	Emergency
Brick Red( )	Alert
Brick Red ( )	Critical
Brick Red ( )	Error
Gold ( )	Warning
Grey ( )	Notice
Blue ( )	Info

- Network Scope — The network scope does not affect the **Events** widget. The **Events** widget always includes all objects in your AOR.
- Time Scope — The time scope.

The **Events** widget only includes events from products that are in your AOR.

The x-axis represents the number of occurrences of a particular event severity during the selected time period. If you pause on a bar, a tooltip shows the number of events with that severity level during the selected time period. Also, for each severity, the cumulative number of traps, application events, and security events is reported next to the horizontal bar. If Syslog messages are included, then they are included in the count. To conserve space, the number is shown as is or truncated to the nearest 1,000 ("K") or 1,000,000 ("M").

By default, Syslog events are included in the summary; however, because Syslog events occur at a much higher frequency than other events and therefore could skew the bars for the other events, you can exclude Syslog events. If they are excluded, they will not be displayed in the legend. Users' selections are persisted (per user per server).

Customizing the Events widget

You can customize the **Events** widget to display events for a specific duration and to display Syslog details.

- Display event information for a specific duration by selecting one of the following from the **Range** list:
  - **This Hour** — Displays event information for the current hour beginning when you launch the dashboard.
  - **Last Hour** — Displays event information for the previous hour to when you launch the dashboard.
  - **Today** — Displays event information for the current day beginning at 12:00 AM.
  - **Yesterday** — Displays event information for the previous day beginning at 12:00 AM of the previous day.
  - **Last 7 Days** — Displays event information for the last 7 days, including the current day.
  - **Last 30 Days** — Displays event information for the last 30 days, including the current day.
- Include Syslog information (default) on the **Event Summary** pane by selecting the **Show Syslog** check box.

  To exclude Syslog information, clear the **Show Syslog** check box.

Accessing additional data from the Events widget

Double-click a bar in the **Events** widget to navigate to an event custom report (HTML) that displays the events corresponding to the event type selected.

For information about report details, refer to "Fault Management" on page 1141.

Host Adapter Inventory widget

The **Host Adapter Inventory** widget (Figure 88) displays the host adapter products inventory as stacked bar graphs.

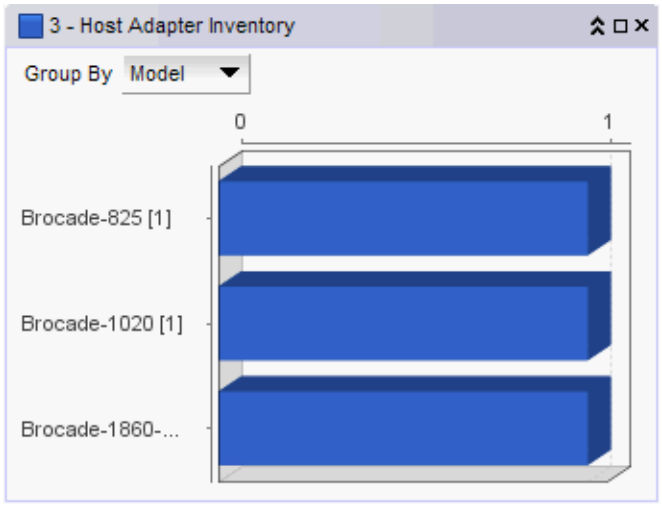


FIGURE 88 **Host Adapter Inventory widget**

The **Host Adapter Inventory** widget includes the following data:

- Severity icon/Host product count/widget title — The color of the worst severity and the Host product count with that severity displays before the widget title.
- **Group By** list — Use to customize this widget to display a specific grouping. Options include: **Model** (default), **Location**, **Driver**, **BIOS**, and **OS Type**.
- Bar chart — Displays each group as a separate bar on the graph. Displays the current state of all Host products discovered for a group in various colors on each bar. Tooltips showing the number of devices in that state are shown when you pause on the bar.
- Time Scope — The time scope.

Customizing the Host Adapter Inventory widget

You can customize the **Host Adapter Inventory** widget to display product inventory for a specific grouping. The group type and number of products in the group displays to the left of the associated bar; for example, 2.3.0.005 [3], where 2.3.0.005 is the driver number and [3] is the number of products running that driver level.

- Change the grouping by selecting one of the following from the **Group By** list:
  - **Model** — Displays the Host product inventory by model.
  - **Location** — Displays the Host product inventory by physical location.
  - **Driver** — Displays the Host product inventory by driver.
  - **BIOS** — Displays the Host product inventory by BIOS (boot code image version).
  - **OS Type** — Displays the Host product inventory by operating system.

- Zoom in on an area of the widget by dragging the mouse (upper left corner to lower right corner) to select one or more bars.

  NOTE
  If the ratio between the longest and shortest bar reaches 5000:1, you should maximize the widget prior to using zoom.

  To return the widget to its original state, reverse the selection (drag from lower right corner to upper left corner).

Accessing additional data from the Host Adapter Inventory widget

Double-click a bar in the **Host Adapter Inventory** widget to navigate to the **Host Adapter Inventory Report**.

IP Inventory widget

The **IP Inventory** widget (Figure 89) displays the IP products inventory as stacked bar graphs.

For a VCS fabric, each VCS fabric is counted as an individual product.

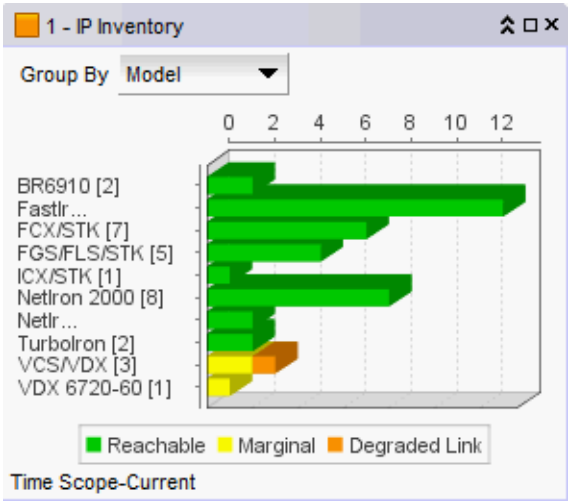


FIGURE 89 **IP Inventory widget**

The **IP Inventory** widget includes the following data:

- Severity icon/product count/widget title — The color of the worst severity followed by the IP product count with that severity displays before the widget title.
- **Group By** list — Use to customize this widget to display a specific group of products. Options include: **Firmware**, **Model**, **Product Type**, **Location**, and **Contact**.
- Bar chart — Displays each group as a separate bar on the graph. Displays the current state of all products discovered for a group in various colors on each bar. Displays the color legend below the x-axis. Tooltips showing the number of devices in that state are shown when you pause on the bar.

- Color legend — Displays the color legend below the bar chart.
  - Green — Reachable: IP product is online and accessible by IP (ICMP/TCP) and SNMP.
  - Orange — Degraded Link: IP product is accessible by IP (ICMP/TCP); however, it is not accessible by SNMP.
  - Maroon — Not Reachable: IP product is not online and not accessible by IP (ICMP/TCP).
- Time Scope — The time scope.

Customizing the IP Inventory widget

You can customize the **IP Inventory** widget to display product inventory for a specific grouping. The group type and number of products in the group displays to the left of the associated bar; for example, v04.1.00a [3], where v04.1.00a is the firmware number and [3] is the number of products running that firmware level.

- Change the grouping by selecting one of the following from the **Group By** list:
  - **Firmware** — Displays the product inventory by firmware release.
  - **Model** — Displays the product inventory by model.
  - **Product Type** — Displays the product inventory by product type.
  - **Location** — Displays the product inventory by physical location.
  - **Contact** — Displays the product inventory by contact name.
- Zoom in on an area of the widget by dragging the mouse (upper left corner to lower right corner) to select one or more bars.

  NOTE
  If the ratio between the longest and shortest bar reaches 5000:1, you should maximize the widget prior to using zoom.

  To return the widget to its original state, reverse the selection (drag from lower right corner to upper left corner).

Accessing additional data from the IP Inventory widget

Double-click a section of the bar in the **IP Inventory** widget to navigate to the **IP Products -** *Status* dialog box (where *Status* is the status of the section you selected). For more information, refer to "Viewing additional IP product data" on page 232

NOTE
It takes a few moments to populate newly discovered products in the **IP Products -** *Status* dialog box (where *Status* is the section of the widget you selected).

IP Status widget

The **IP Status** widget (Figure 90) displays the device status as a pie chart.

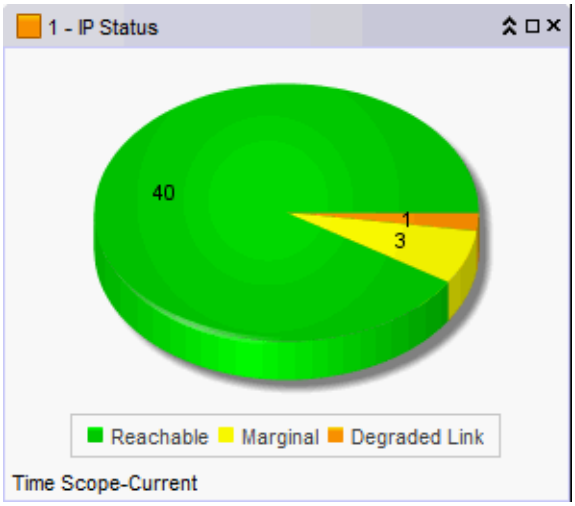


FIGURE 90 IP Status widget

The **IP Status** widget includes the following data:

- Severity icon/product count/widget title — The color of the worst status followed by the product count with that status displays before the widget title.
- Pie chart — The device status as a percentage of the total number of devices.

  The pie chart displays the percentage in various colors on each slice. Tooltips showing the number of devices in that state are shown when you pause on the bar. When there is one status category with less than one percent of the total number of devices, the status widget displays the number of devices in each category on each slice.

  For a VCS fabric, status is determined by the reachability of the individual members of the VCS fabric. The **IP Status** widget displays the most severe reachability of a member of the VCS fabric. For example, if one member of the VCS fabric has a reachability status of “degraded” and all other members are “reachable”, then the VCS fabric status displays as “degraded”.
- Color legend — Displays the color legend below the pie chart using the following color code:
  - Green — Reachable: IP product is online and accessible by IP (ICMP/TCP) and SNMP.
  - Yellow — Degraded Link: IP product is accessible by IP (ICMP/TCP); however, it is not accessible by SNMP.
  - Violet — Unhealthy: One or more units are not present, unit power is off, or the stacking connection is down.
  - Blue — Not Reachable: IP product is not online and not accessible by IP (ICMP/TCP).
- Time Scope — The time scope.

Accessing additional data from the IP Status widget

Double-click a section in the **IP Status** widget to navigate to the **IP Products -** *Status* dialog box (where *Status* is the status of the section you selected). For more information, refer to "Viewing additional IP product data" on page 232

NOTE
It takes a few moments to populate newly discovered products in the **IP Products -** *Status* dialog box (where *Status* is the section of the widget you selected).

Viewing additional IP product data

1. Double-click a section in the **IP Status** or **IP Inventory** widgets.

   The **IP Products -** *Status* dialog box (where *Status* is the section of the widget you selected) displays with the following fields and components:

   - **Product —** The product name.
   - **Fabric** — The fabric associated with the product.
   - **Product Type —** The type of product.
   - **State —** The state for the product and the port.
   - **Status —** The status for the product and the port.
   - **Tag —** The tag number of the product.
   - **Serial # —** The serial number of the product.
   - **Model** — The model number of the product.
   - **Port Count —** The number of ports on the product.
   - **Firmware —** The firmware version of the product.
   - **Location** — The physical location of the product. This field is editable at the fabric level.
   - **Contact —** The name of the person or group you should contact about the product. This field is editable at the fabric level.

2. Right-click any row in the table to access the corresponding shortcut menu for the device. For more information about shortcut menus, refer to "IP shortcut menus" on page 1268.
3. Click **Close**.

Status widget

The **Status** widget (Figure 91) displays the number of products managed and the number of events within the selected event time range, as well as various IP management processes and their current state.

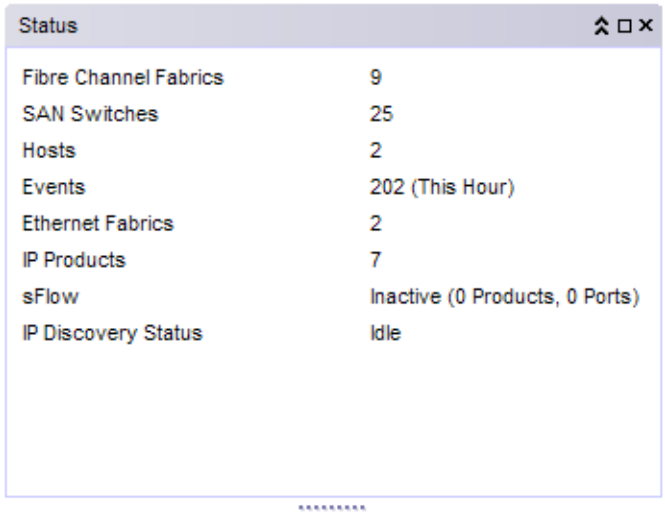


FIGURE 91 Status widget

The **Status** widget displays the following items for each product license:

- SAN Physical Switches — The number of discovered physical SAN switches.
- Hosts — The number of managed hosts.
- Events — The number of events within the last hour.
- Ethernet Fabrics — The number of managed Ethernet fabrics.
- IP Products — The number of managed IP products.
- sFlow — The current sFlow state.
- IP Discovery Status — The current IP discovery status.
- Time Scope — The time scope.

Fabric Watch widgets

The widget includes the Fabric Watch threshold violations for devices running Network OS 3.0.0 or later .

The Fabric Watch widgets display on the main **Dashboard** tab. The Management application provides the following preconfigured Fabric Watchwidgets:

- Out of Range Violations widget — Table view of all out of range threshold violations reported by your Network OS devices.
- Port Health Violations widget — Table view of out of range port health violations.

Out of Range Violations widget

The **Out of Range Violations** widget (Figure 92) displays the number of violations for each Fabric Watch category, and the number of network objects (such as ports, trunks, and switches) for Network OS devices with the Fabric Watch violation based on the selected fabric and a specified time range.

By default, this widget refreshes every minute. If any violations occur on fabrics in your area of responsibility (AOR) during the minute refresh time frame, the widget refreshes every 10 seconds. If you delete, discover, or unmonitor a device, the widget refreshes.

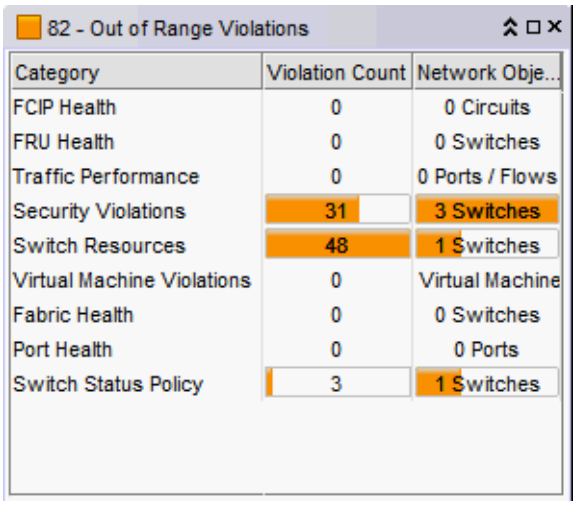


FIGURE 92 **Out of Range Violations widget**

The **Out of Range Violations** widget includes the following fields and components:

- Severity icon/product count/widget title — The color of the worst severity and the number of products with that severity displays before the widget title.
- **Category** — A list of the Fabric Watch dashboard categories. Always displays whether or not there is an associated violation. Categories include:
  - Fabric Health
  - FCIP Health
  - FRU Health
  - Port Health
  - Security Violations
  - Switch Resources
  - Switch Status Policy
  - Traffic Performance
  - Virtual Machine Violations

NOTE
Network OS Fabric Watch violations with appropriate counter values are displayed for Switch Status Policy, FRU Health, Security Violations, Switch Resources, and Port Health categories. Traffic Performance, FCIP Health, Fabric Health, and Virtual Machine Violations categories are not supported and display as blank.

- **Violation Count** — The total number of Fabric Watch rule violations for each category. Always displays whether or not there is a violation.
- **Network Object Count** — The number and network object type (such as switch, virtual machine, port, trunk, and so on) with a Fabric Watch violation for each category. Always displays whether or not there is a violation.
- **Refreshed** — The time of the last update for the widget.

Customizing the Out of Range Violations widget

You can customize the widget to display violations for a specific fabric or group and time frame.

- To display data for a specific fabric or group, refer to "Setting the network scope" on page 220.
- To display data for a specific duration, refer to "Setting the data display time frame" on page 222.
- Sort the contents by clicking the column header. Click the same column header again to reverse the sort order.

Port Health Violations widget

The **Port Health Violations** widget (Figure 93) displays the number of violations for each product based on the selected fabric and a specified time range. There are four port health violation widgets: All, ISL, Initiator, and Target.

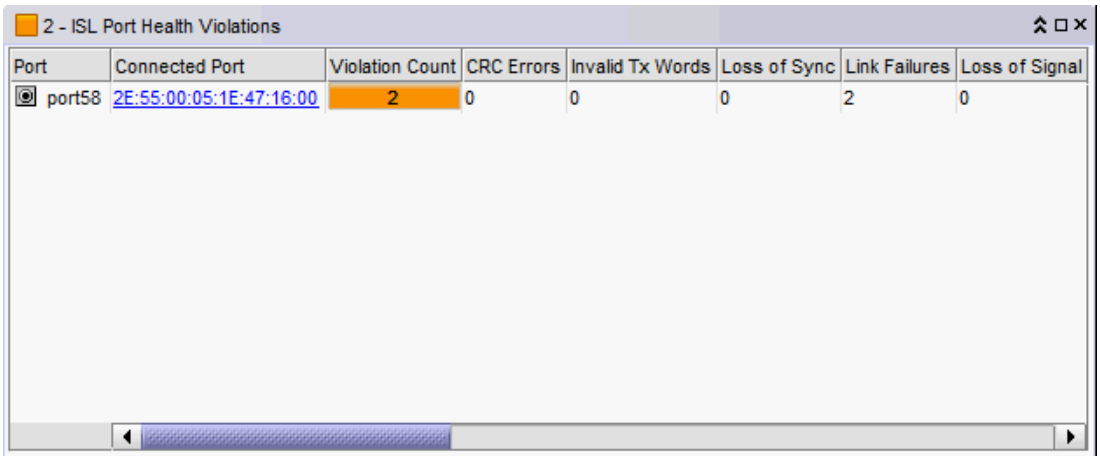


FIGURE 93 **Port Health Violations widget**

The **Port Health Violations** widget displays the following data for each product:

- Severity icon/port count/widget title — The color of the worst severity and the number of products with that severity displays before the widget title.
- **Product** — A product label such as product name, IP address, node WWN, domain ID, or zone alias.
- **Port** — A port identifier such as port name, number, address, WWN, user port number, or zone alias.

NOTE
All non-FC ports display either the MAC address or the port name instead of WWN.

- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.
- **Violation Count** — The number of Fabric Watch rule violations for the port.
- **CRC Errors** — The number of times an invalid cyclic redundancy check error occurs on a port or a frame that computes to an invalid CRC.
- **Invalid Tx Words** — The number of times an invalid transmission word error occurs on a port.
- **Loss of sync** — The number of times a synchronization error occurs on the port.
- **Link Failures** — The number of times a link failure occurs on a port or sends or receives NOS.
- **Loss of Signal** — The number of times that a signal loss occurs in a port.
- **Protocol Errors** — The number of times a protocol error occurs on a port.
- **Link Reset** — The ports on which the number of link resets exceed the specified threshold value.
- **C3TXTO** — The number of Class 3 discards frames because of timeouts.
- **State changes** — The state of the port has changed for one of the following reasons:
  - The port has gone offline.
  - The port has come online.
  - The port is faulty.
- **SFP Current** — The amount of supplied current to the SFP transceiver.
- **SFP Receive Power** — The amount of incoming laser, in µwatts, to help determine if the SFP transceiver is in good working condition.
- **SFP Transmit Power** — The amount of outgoing laser, in µwatts. Use this to determine the condition of the SFP transceiver.
- **SFP Voltage** — The amount of voltage supplied to the SFP transceiver.
- **SFP Temperature** — The physical temperature of the SFP transceiver, in degrees Celsius.
- **SFP Power On Hours** — The number of hours the 16 Gbps SFP transceiver is powered on.
- **Refreshed** — The time of the last update for the widget.

Network OS Fabric Watch violations with appropriate counter values are displayed for the following categories.

- **Abnormal Frame Terminations** — The number of frames abnormally terminated.
- **Symbol Errors** — The number of undefined or invalid symbols received.
- **IFG (InterFrame Gap) Errors** — The interframe gap between successive frames that is violated.

Customizing the Port Health Violations widget

You can customize the widget to display violations for a specific fabric and time frame.

- To display data for a specific fabric or group, refer to "Setting the network scope" on page 220.
- To display data for a specific duration, refer to "Setting the data display time frame" on page 222.
- Sort the contents by clicking the column header. Click the same column header again to reverse the sort order.

Accessing additional data from the widget

- Right-click a row in the widget to access the shortcut menu available for the associated device.Right-click any row and select **Locate** to locate the particular device to which the port belongs in the **Network Objects** products list.
- Double-click a row to navigate to the **Violations** dialog box.

Performance monitors

The **Performance Dashboard** provides a high-level overview of the performance on the network. This allows you to easily check the performance of devices, ports, and traffic on the network. The **Performance Dashboard** also provides several features to help you quickly access performance metrics and reports.

The dashboards update every ten minutes regardless of the currently selected tab (IP) or the LAN size.

You can change the default size of the status widgets and performance monitors by placing the cursor on the divider until a double arrow displays. Click and drag the adjoining divider to resize the window.

Reset the **Performance Dashboard** back to the default size by right-clicking in the white space and selected **Reset to Default**.

The Management application provides the following preconfigured performance monitors:

TABLE 23 Preconfigure performance monitors

Monitor title	Description	Data collectors
Top Port Alignment Errors	Table view of the alignment errors measure	All SAN TE port collector
Top Port C3 Discards	Table view of the C3 discards measure	All SAN FC port collector
Top Port C3 Discards RX TO	Table view of the C3 discards RX TO measure. There are four versions of this monitor based on the type of port: All ports, initiator ports, ISL ports, and Target ports.	All SAN FC port collector
Top Port CRC Errors	Table view of the CRC errors measure. There are four versions of this monitor based on the type of port: All ports, initiator ports, ISL ports, and Target ports.	All SAN FC port collector, All SAN TE port collector
Top Port Encode Error Out	Table view of the encode error out measure. There are four versions of this monitor based on the type of port: All ports, initiator ports, ISL ports, and Target ports.	All SAN FC port collector
Top Port Errors	Table view of the errors measure	Port error count collector
Top Port Overflow Errors	Table view of the overflow errors measure	All SAN TE port collector

TABLE 23 Preconfigure performance monitors

Monitor title	Description	Data collectors
Top Port Receive EOF	Table view of the received end-of-frames measure	All SAN TE port collector
Top Port Runtime Errors	Table view of the runtime errors measure	All SAN TE port collector
Top Port Sync Losses	Table view of the top port synchronization losses. There are four versions of this monitor based on the type of port: All ports, initiator ports, ISL ports, and Target ports.	All SAN FC port collector
Top Port Too Long Errors	Table view of the too long errors measure	All SAN TE port collector
Top Port Traffic	Table view of the traffic measure	All SAN FCIP tunnel collector, All SAN FC port collector, port throughput collector, All SAN TE port collector
Top Port Underflow Errors	Table view of the underflow errors measure	All SAN TE port collector
Top Port Utilization Percentage	Table view of the port utilization percentage measure. There are four versions of this monitor based on the type of port: All ports, initiator ports, ISL ports, and Target ports.	All SAN FCIP tunnel collector, All SAN FC port collector, port utilization collector, All SAN TE port collector
Bottom Port Utilization Percentage	Table view of the port utilization percentage measure. There are four versions of this monitor based on the type of port: All ports, initiator ports, ISL ports, and Target ports.	All SAN FCIP tunnel collector, All SAN FC port collector, port utilization collector, All SAN TE port collector
Top Product CPU Utilization	Table view of the CPU utilization percentage measure	Network OS CPU/memory utilization collector, NetIron/FastIron CPU/memory utilization collector, Wireless ports collector
Top Product Memory Utilization	Table view of the memory utilization percentage measure	Network OS CPU/memory utilization collector, NetIron/FastIron CPU/memory utilization collector, Wireless ports collector
Top Product Response Time	Table view of the response time measure	Ping Stats collector (IP)
Top Product Temperature	Table view of the temperature measure	Network OS temperature collector, System temperature collector
Top Products with Unused Ports	Table view of the products with unused ports measure	Ports Not in Use Collector

These preconfigured performance monitors can be turned off, hidden, and edited; however, you cannot delete the preconfigured monitors.

You can also create new performance monitors to display on the dashboard. For more information, refer to "User-defined performance monitors" on page 264.

Displaying monitors on the Performance Dashboard

1. From the **Dashboards** expand navigation bar, double-click **Performance Dashboard**.

   The **Performance Dashboard** displays.

2. Click the **Customize Dashboard** icon.

   The **Customize Dashboard** dialog box displays.

3. Select the check box in the **Display** column for each performance monitor you want to display on the **Performance Dashboard**.

4. Click **OK**.

Top Port Alignment Errors monitor

The **Top Port Alignment Errors** performance monitor displays the top ports with alignmenet errors in a table.

The Top Port Alignment Errors performance monitor includes the following data:

- Threshold icon/object count/monitor title — The color associated with the threshold and number of objects within that threshold displays next to the monitor title.
- **Port** — The port affected by this monitor.
- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.
- **Alignment Errors**— The number (error count) of alignment errors for the duration specified in the monitor.
- **Alignment Errors/sec** — The number (error rate) of alignment errors per second for the duration specified in the monitor.
- **Product** — The product affected by this monitor.
- **Type** — The type of port (for example, U-Port).
- **Identifier** — The port identifier.
- **Port Number** — The port number.
- **State** — The port state (for example, Enabled).
- **Status** — The port status (for example, Up).
- **Refreshed** — The time of the last update for the monitor.

To edit a port performance monitor, refer to "Editing a preconfigured performance monitor" on page 263.

Accessing additional data from top or bottom port monitors

- Double-click a row or right-click a row and select **Show Graph/Table** to navigate to the **Historical Graphs/Tables** dialog box for the selected measures. For more information, refer to "Performance Data" on page 969.

Top Port C3 Discards monitor

The **Top Port C3 Discards** monitor (Figure 94) displays the top ports with Class 3 frames discarded in a table. There are four port widgets: All, ISL, Initiator, and Target.

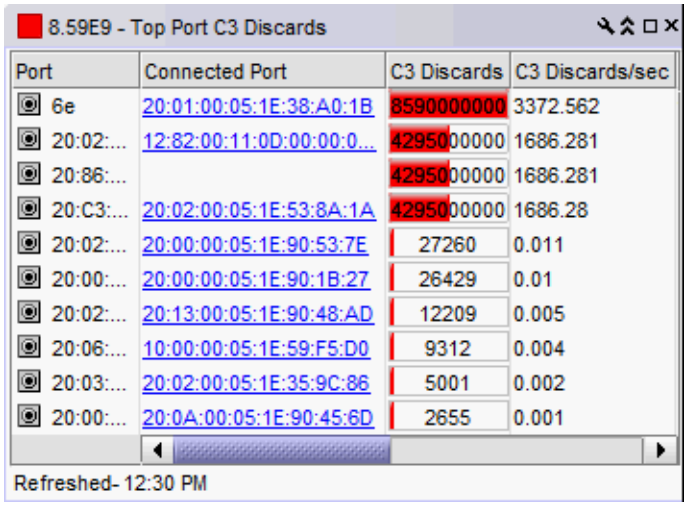


FIGURE 94 **Top Port C3 Discards monitor**

The **Top Port C3 Discards** monitor includes the following data:

- Severity icon/monitor title — The worst severity of the data based on the error count shown next to the monitor title.
- **Port** — The port affected by this monitor.
- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.
- **C3 Discards/sec** — The number (error rate) of Class 3 discard errors per second for the duration specified in the monitor.
- **C3 Discards** — The number (error count) of Class 3 discard errors for the duration specified in the monitor.
- **Product** — The product affected by this monitor.
- **Type** — The type of port (for example, U-Port).
- **Identifier** — The port identifier.
- **Port Number** — The port number.
- **State** — The port state (for example, Enabled).
- **Status** — The port status (for example, Up).
- **Refreshed** — The time of the last update for the monitor.

To customize the monitor to display data by a selected time frame as well as customize the display options, refer to "Editing a preconfigured performance monitor" on page 263.

Accessing additional data from the Top Port C3 Discards monitor

- Right-click a row in the monitor to access the shortcut menu available for the associated device.
- Double-click a row to navigate to the **Historical Graphs/Tables** dialog box. For more information, refer to "Performance Data" on page 969.

Top Port C3 Discards RX TO monitor

The **Top Port C3 Discards RX TO** monitor (Figure 95) displays the top ports with receive Class 3 frames received at this port and discarded at the transmission port due to timeout in a table.

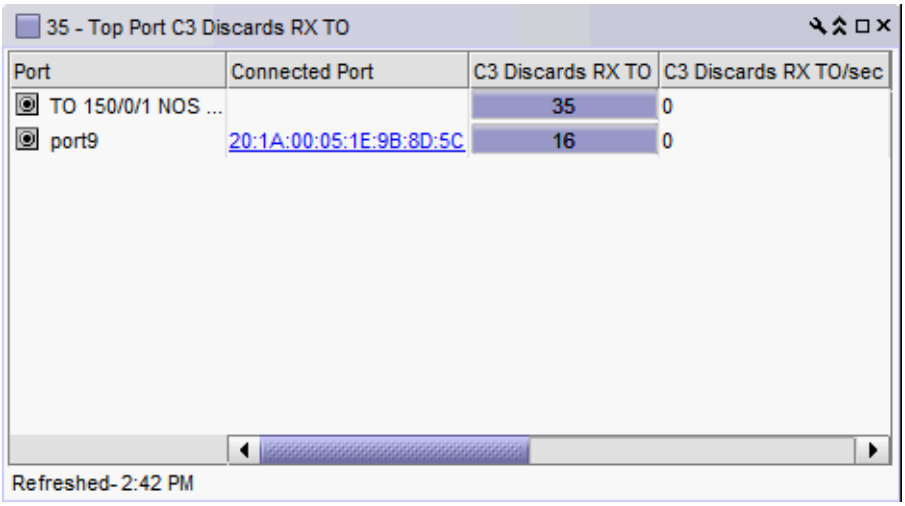


FIGURE 95 Top Port C3 Discards RX TO monitor

The **Top Port C3 Discards RX TO** monitor includes the following data:

- Severity icon/monitor title — The worst severity of the data based on the error count shown next to the monitor title.
- **Port** — The port affected by this monitor.
- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.
- **C3 Discards RX TO/sec** — The number (error rate) of Class 3 frames received at this port and discarded at the transmission port due to timeout errors per second for the duration specified in the monitor.

- **C3 Discards RX TO** — The number (error count) of Class 3 frames received at this port and discarded at the transmission port due to timeout errors for the duration specified in the monitor.
- **Product** — The product affected by this monitor.
- **Type** — The type of port (for example, U-Port).
- **Identifier** — The port identifier.
- **Port Number** — The port number.
- **State** — The port state (for example, Enabled).
- **Status** — The port status (for example, Up).
- **Refreshed** — The time of the last update for the monitor.

To customize the monitor to display data by a selected time frame as well as customize the display options, refer to "Editing a preconfigured performance monitor" on page 263.

Accessing additional data from the Top Port C3 Discards RX TO monitor

- Right-click a row in the monitor to access the shortcut menu available for the associated device.
- In a Top N or Bottom N C3 Discards TX TO and C3 Discards RX TO monitors, right-click an FC-port row and select **Discarded Frames** to navigate to the **Discarded Frames** dialog box. For more information, refer to "Viewing discarded frames from a port" on page 384.
- Double-click a row to navigate to the **Historical Graphs/Tables** dialog box. For more information, refer to "Performance Data" on page 969.

Top Port CRC Errors monitor

The **Top Port CRC Errors** monitor (Figure 96) displays the top ports with frames that contain cyclic redundancy check (CRC) errors in a table.

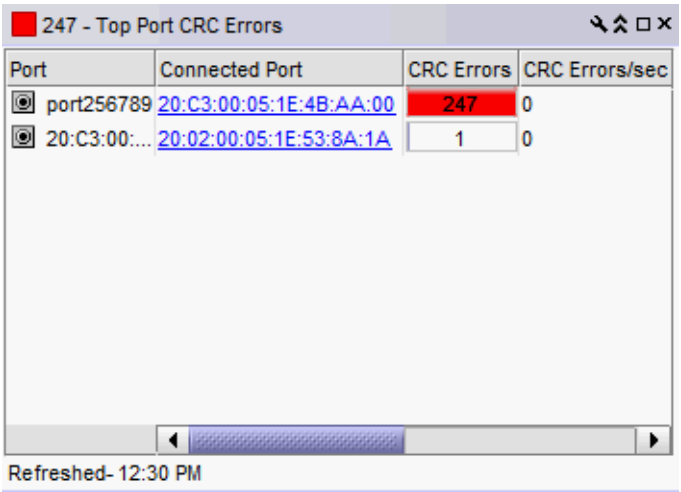


FIGURE 96 Top Port CRC Errors monitor

The **Top Port CRC Errors** monitor includes the following data:

- Severity icon/monitor title — The worst severity of the data based on the error count shown next to the monitor title.
- **Port** — The port affected by this monitor.
- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.
- **CRC Errors/sec** — The number (error rate) of cyclic redundancy check (CRC) errors per second for the duration specified in the monitor.
- **CRC Errors** — The number (error count) of cyclic redundancy check (CRC) errors for the duration specified in the monitor.
- **Product** — The product affected by this monitor.
- **Type** — The type of port (for example, U-Port).
- **Identifier** — The port identifier.
- **Port Number** — The port number.
- **State** — The port state (for example, Enabled).
- **Status** — The port status (for example, Up).
- **Refreshed** — The time of the last update for the monitor.

To customize the monitor to display data by a selected time frame as well as customize the display options, refer to "Editing a preconfigured performance monitor" on page 263.

Accessing additional data from the Top Port CRC Errors monitor

- Right-click a row in the monitor to access the shortcut menu available for the associated device. For more information about shortcut menus, refer to "Application menus" on page 1261.
- Double-click a row to navigate to the **Historical Graphs/Tables** dialog box. For more information, refer to "Performance Data" on page 969.

Top Port Discards monitor

The **Top Port Discards** monitor (Figure 97) displays the top ports with receive and transmit discards in a table.

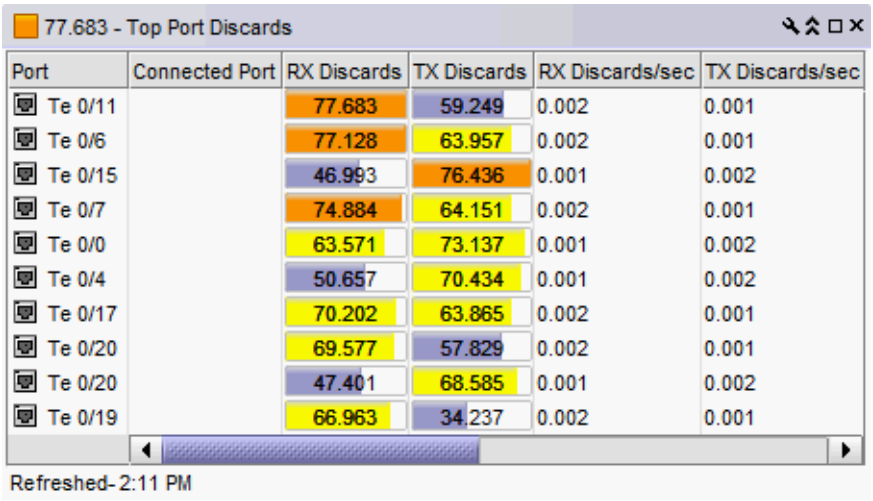


FIGURE 97 Top Port Discards monitor

The **Top Port Discards** monitor includes the following data:

- Severity icon/monitor title — The worst severity of the data based on the error count shown next to the monitor title.
- **Port** — The port affected by this monitor.
- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.
- **RX Discards/sec** — The number (error rate) of receive discard errors per second for the duration specified in the monitor.
- **RX Discards** — The number (error count) of receive discard errors.
- **TX Discards/sec** — The number (error rate) of transmit discard errors for the duration specified in the monitor.
- **TX Discards** — The number (error count) of transmit discard errors.
- **Product** — The product affected by this monitor.
- **Type** — The type of port (for example, U-Port).
- **Identifier** — The port identifier.
- **Port Number** — The port number.
- **State** — The port state (for example, Enabled).

- **Status** — The port status (for example, Up).
- **Refreshed** — The time of the last update for the monitor.

To customize the monitor to display data by a selected time frame as well as customize the display options, refer to "Editing a preconfigured performance monitor" on page 263.

Accessing additional data from the Top Port Discards monitor

- Right-click a row in the monitor to access the shortcut menu available for the associated device. For more information about shortcut menus, refer to "Application menus" on page 1261.
- Double-click a row to navigate to the **Historical Graphs/Tables** dialog box. For more information, refer to "Performance Data" on page 969.

Top Port Encode Error Out monitor

The **Top Port Encode Error Out** monitor (Figure 98) displays the top ports with encoding errors outside of frames in a table.

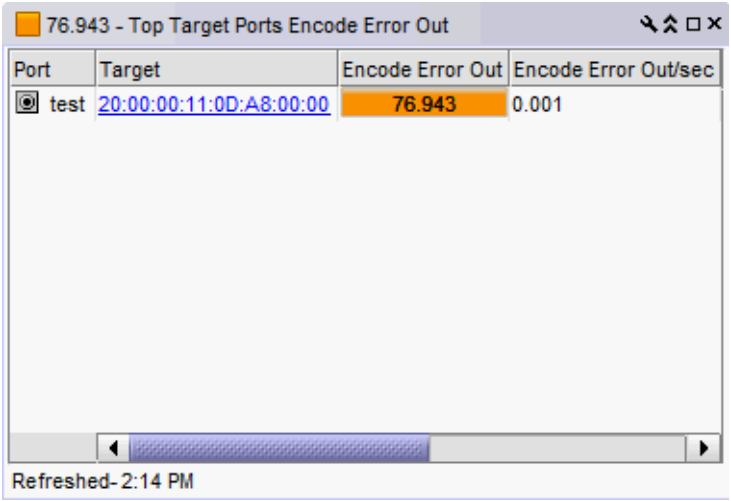


FIGURE 98 Top Port Encode Error Out monitor

The **Top Port Encode Error Out** monitor includes the following data:

- Severity icon/monitor title — The worst severity of the data based on the error count shown next to the monitor title.
- **Port** — The port affected by this monitor.
- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.

- **Encode Error Out/sec** — The number (error rate) of encoding errors outside of frames per second for the duration specified in the monitor.
- **Encode Error Out** — The number (error count) of encoding errors outside of frames for the duration specified in the monitor.
- **Product** — The product affected by this monitor.
- **Type** — The type of port (for example, U-Port).
- **Identifier** — The port identifier.
- **Port Number** — The port number.
- **State** — The port state (for example, Enabled).
- **Status** — The port status (for example, Up).
- **Refreshed** — The time of the last update for the monitor.

To customize the monitor to display data by a selected time frame as well as customize the display options, refer to "Editing a preconfigured performance monitor" on page 263.

Accessing additional data from the Top Port Encode Out Errors monitor

- Right-click a row in the monitor to access the shortcut menu available for the associated device. For more information about shortcut menus, refer to "Application menus" on page 1261.
- Double-click a row to navigate to the **Historical Graphs/Tables** dialog box. For more information, refer to "Performance Data" on page 969.

Top Port Errors monitor

The **Top Port Errors** monitor (Figure 99) displays the top ports with receive and transmit errors in a table.

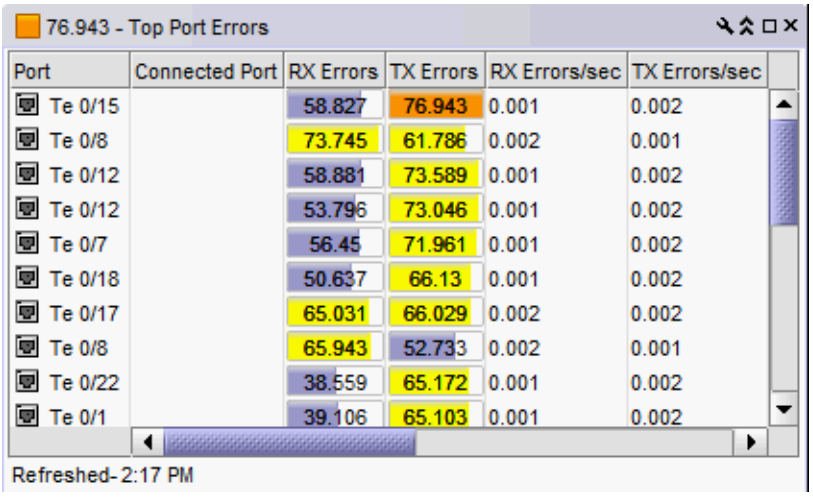


FIGURE 99 Top Port Errors monitor

The **Top Port Errors** monitor includes the following data:

- Severity icon/monitor title — The worst severity of the data based on the error count shown next to the monitor title.
- **Port** — The port affected by this monitor.
- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.
- **RX Errors/sec** — The number (error rate) of receive errors per second for the duration specified in the monitor.
- **RX Errors** — The number (error count) of receive errors.
- **TX Errors/sec** — The number (error rate) of transmit errors for the duration specified in the monitor.
- **TX Errors** — The number (error count) of transmit errors.
- **Product** — The product affected by this monitor per second.
- **Type** — The type of port (for example, U-Port).
- **Identifier** — The port identifier.
- **Port Number** — The port number.
- **State** — The port state (for example, Enabled).
- **Status** — The port status (for example, Up).
- **Refreshed** — The time of the last update for the monitor.

To customize the monitor to display data by a selected time frame as well as customize the display options, refer to "Editing a preconfigured performance monitor" on page 263.

Accessing additional data from the Top Port Errors monitor

- Right-click a row in the monitor to access the shortcut menu available for the associated device. For more information about shortcut menus, refer to "Application menus" on page 1261.
- Double-click a row to navigate to the **Historical Graphs/Tables** dialog box. For more information, refer to "Performance Data" on page 969.

Top Port Overflow Errors monitor

The **Top Port Overflow Errors** performance monitor (Figure 100) displays the top ports with overflow erros in a table.

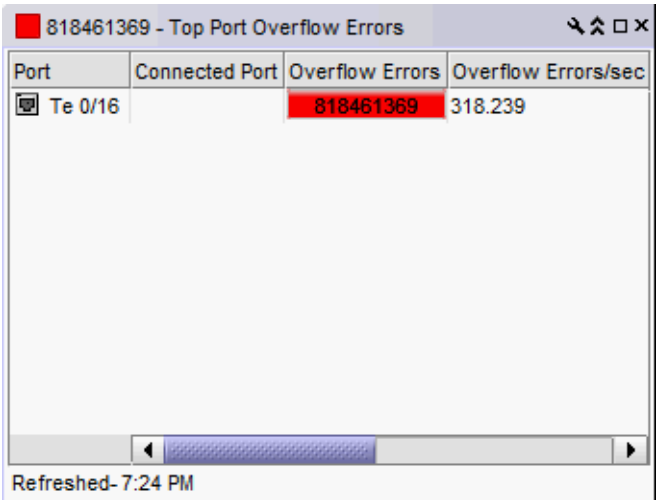


FIGURE 100 Top Port Overflow Errors performance monitor

The Top Port Overflow Errors performance monitor includes the following data:

- Threshold icon/object count/monitor title — The color associated with the threshold and number of objects within that threshold displays next to the monitor title.
- **Port** — The port affected by this monitor.
- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.
- **Overflow Errors**— The number (error count) of overflow errors for the duration specified in the monitor.
- **Overflow Errors/sec** — The number (error rate) of overflow errors per second for the duration specified in the monitor.
- **Product** — The product affected by this monitor.
- **Type** — The type of port (for example, U-Port).
- **Identifier** — The port identifier.
- **Port Number** — The port number.
- **State** — The port state (for example, Enabled).
- **Status** — The port status (for example, Up).
- **Refreshed** — The time of the last update for the monitor.

To edit a port performance monitor, refer to "Editing a preconfigured performance monitor" on page 263.

Top Port Receive EOF monitor

The **Top Port Receive EOF** performance monitor displays the top ports with received end-of-frames in a table.

The Top Port Receive EOF performance monitor includes the following data:

- Threshold icon/object count/monitor title — The color associated with the threshold and number of objects within that threshold displays next to the monitor title.
- **Port** — The port affected by this monitor.
- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.
- **Receive EOF** — The number (count) of end of frames received.
- **Receive EOF/sec** — The number (rate) of end of frames received per second for the duration specified in the monitor.
- **Product** — The product affected by this monitor.
- **Type** — The type of port (for example, U-Port).
- **Identifier** — The port identifier.
- **Port Number** — The port number.
- **State** — The port state (for example, Enabled).
- **Status** — The port status (for example, Up).
- **Refreshed** — The time of the last update for the monitor.

To edit a port performance monitor, refer to "Editing a preconfigured performance monitor" on page 263.

Top Port Runtime Errors monitor

The **Top Port Runtime Errors** performance monitor displays the top ports with runtime errors in a table.

The Top Port Runtime Errors performance monitor includes the following data:

- Threshold icon/object count/monitor title — The color associated with the threshold and number of objects within that threshold displays next to the monitor title.
- **Port** — The port affected by this monitor.

- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.
- **Runtime Errors**— The number (error count) of runtime errors for the duration specified in the monitor.
- **Runtime Errors/sec** — The number (error rate) of runtime errors per second for the duration specified in the monitor.
- **Product** — The product affected by this monitor.
- **Type** — The type of port (for example, U-Port).
- **Identifier** — The port identifier.
- **Port Number** — The port number.
- **State** — The port state (for example, Enabled).
- **Status** — The port status (for example, Up).
- **Refreshed** — The time of the last update for the monitor.

To edit a port performance monitor, refer to "Editing a preconfigured performance monitor" on page 263.

Top Port Sync Losses monitor

The **Top Port Sync Losses** monitor (Figure 101) displays the top ports with synchronization failures in a table.

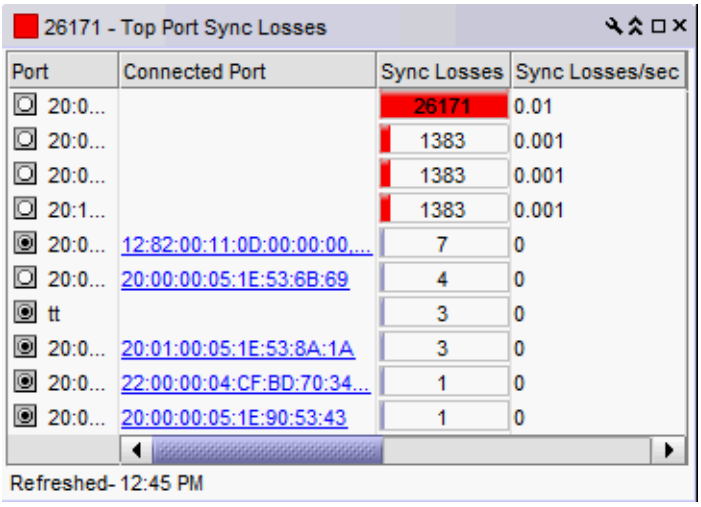


FIGURE 101 **Top Port Sync Losses monitor**

The **Top Port Sync Losses** monitor includes the following data:

- Severity icon/monitor title — The color of the worst severity of the data shown next to the monitor title.
- **Port** — The port affected by this monitor.
- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.
- **Sync Losses —** The number of synchronization failures for the port.
- **Sync Losses/sec —** The number of synchronization failures for the port per second.
- **Product** — The product affected by this monitor.
- **Type** — The type of port (for example, U-Port).
- **Identifier** — The port identifier.
- **Port Number** — The port number.
- **State** — The port state (for example, Online).
- **Status** — The port status (for example, In_Sync, No_Sync).
- **Refreshed** — The time of the last update for the monitor.

To customize the monitor to display data by a selected time frame as well as customize the display options, refer to "Editing a preconfigured performance monitor" on page 263.

Accessing additional data from the Top Port Link Resets monitor

- Right-click a row in the monitor to access the shortcut menu available for the associated device. For more information about shortcut menus, refer to "Application menus" on page 1261.
- Double-click a row to navigate to the **Custom: Historical Performance Graphs** dialog box. For more information, refer to "Performance Data" on page 969.

Top Port Too Long Errors monitor

The **Top Port Too Long Errors** performance monitor displays the top ports with frames longer than the maximum frame size allowed errors in a table.

The Top Port Too Long Errors performance monitor includes the following data:

- Threshold icon/object count/monitor title — The color associated with the threshold and number of objects within that threshold displays next to the monitor title.
- **Port** — The port affected by this monitor.

- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.
- **Too Long Errors**— The number (error count) of frames longer than the maximum frame size allowed errors for the duration specified in the monitor.
- **Too Long Errors/sec** — The number (error rate) of frames longer than the maximum frame size allowed errors per second for the duration specified in the monitor.
- **Product** — The product affected by this monitor.
- **Type** — The type of port (for example, U-Port).
- **Identifier** — The port identifier.
- **Port Number** — The port number.
- **State** — The port state (for example, Enabled).
- **Status** — The port status (for example, Up).
- **Refreshed** — The time of the last update for the monitor.

To edit a port performance monitor, refer to "Editing a preconfigured performance monitor" on page 263.

Top Port Traffic monitor

The **Top Port Traffic** monitor (Figure 102) displays the top ports with receive and transmit traffic in a table.

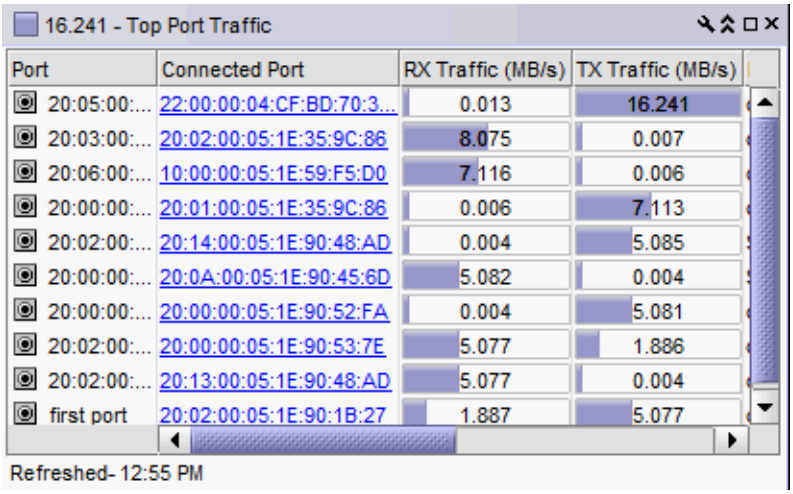


FIGURE 102 **Top Port Traffic monitor**

The **Top Port Traffic** monitor includes the following data:

- Severity icon/monitor title — Displays the worst severity of the data shown next to the monitor title.

NOTE
The **Top Port Traffic** widget displays the threshold colors based on the port speed. Click edit icon of the widget to customize the threshold values.

- **Port** — The port affected by this monitor.
- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.
- **RX Traffic (MB/s)** — The top receive traffic in megabits per second.
- **TX Traffic (MB/s)** — The top transmit traffic in megabits per second.
- **Product** — The product affected by this monitor.
- **Type** — The type of port (for example, U-Port).
- **Identifier** — The port identifier.
- **Port Number** — The port number.
- **State** — The port state (for example, Enabled).
- **Status** — The port status (for example, Up).
- **Refreshed** — The time of the last update for the monitor.

To customize the monitor to display data by a selected time frame as well as customize the display options, refer to "Editing a preconfigured performance monitor" on page 263.

Accessing additional data from the Top Port Traffic monitor

- Right-click a row in the monitor to access the shortcut menu available for the associated device. For more information about shortcut menus, refer to "Application menus" on page 1261.
- Double-click a row to navigate to the **Historical Graphs/Tables** dialog box. For more information, refer to "Performance Data" on page 969.

Top Port Underflow Errors monitor

The **Top Port Underflow Errors** performance monitor displays the top ports with underlow errors in a table.

The Top Port Underflow Errors performance monitor includes the following data:

- Threshold icon/object count/monitor title — The color associated with the threshold and number of objects within that threshold displays next to the monitor title.
- **Port** — The port affected by this monitor.

- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.
- **Underflow Errors**— The number (error count) of underflow errors for the duration specified in the monitor.
- **Underflow Errors/sec** — The number (error rate) of underflow errors per second for the duration specified in the monitor.
- **Product** — The product affected by this monitor.
- **Type** — The type of port (for example, U-Port).
- **Identifier** — The port identifier.
- **Port Number** — The port number.
- **State** — The port state (for example, Enabled).
- **Status** — The port status (for example, Up).
- **Refreshed** — The time of the last update for the monitor.

To edit a port performance monitor, refer to "Editing a preconfigured performance monitor" on page 263.

Top Port Utilization Percentage monitor

The **Top Port Utilization** monitor (Figure 103) displays the top port utilization percentages in a table.

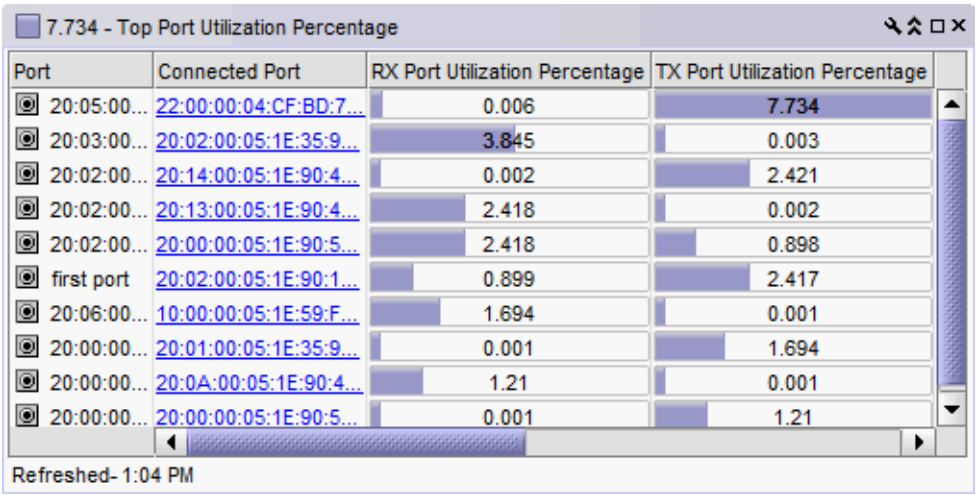


FIGURE 103 **Top Port Utilization monitor**

The **Top Port Utilization** monitor includes the following data:

- Severity icon/monitor title — The worst severity of the data shown next to the monitor title.
- **Port** — The port affected by this monitor.

- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.
- **RX Port Utilization Percentage** — The top receive port utilization percentages.
- **TX Port Utilization Percentage** — The top transmit port utilization percentages.
- **Product** — The product affected by this monitor.
- **Type** — The type of port (for example, U-Port).
- **Identifier** — The port identifier.
- **Port Number** — The port number.
- **State** — The port state (for example, Enabled).
- **Status** — The port status (for example, Up).
- **Refreshed** — The time of the last update for the monitor.

To customize the monitor to display data by a selected time frame as well as customize the display options, refer to "Editing a preconfigured performance monitor" on page 263.

Accessing additional data from the Top Port Utilization monitor

- Right-click a row in the monitor to access the shortcut menu available for the associated device. For more information about shortcut menus, refer to "Application menus" on page 1261.
- Double-click a row to navigate to the **Historical Graphs/Tables** dialog box. For more information, refer to "Performance Data" on page 969.

Bottom Port Utilization Percentage monitor

The **Bottom Port Utilization Percentage** monitor (Figure 104) displays the bottom port utilization percentages in a table.

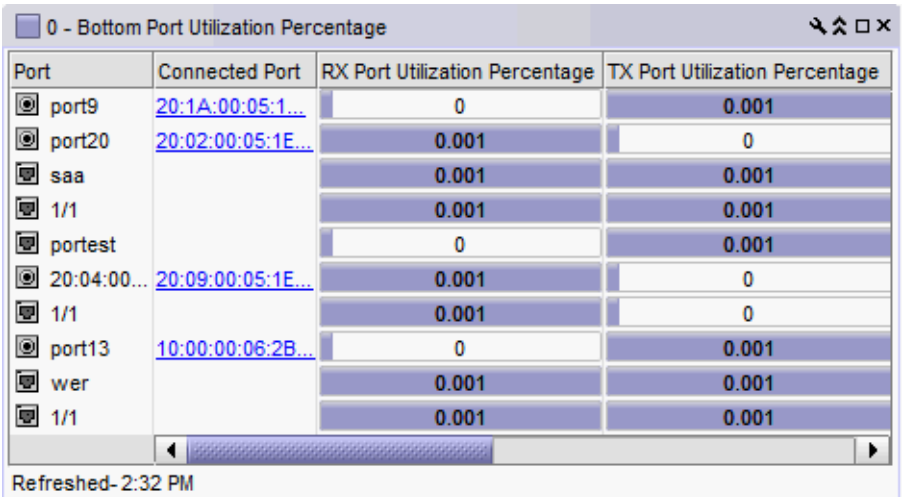


FIGURE 104 Bottom Port Utilization Percentage monitor

The **Top Port Utilization Percentage** monitor includes the following data:

- Severity icon/monitor title — The worst severity of the data shown next to the monitor title.
- **Port** — The port affected by this monitor.
- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.
- **RX Port Utilization Percentage** — The bottom receive port utilization percentages.
- **TX Port Utilization Percentage** — The bottom transmit port utilization percentages.
- **Product** — The product affected by this monitor.
- **Type** — The type of port (for example, U-Port).
- **Identifier** — The port identifier.
- **Port Number** — The port number.
- **State** — The port state (for example, Enabled).
- **Status** — The port status (for example, Up).
- **Refreshed** — The time of the last update for the monitor.

To customize the monitor to display data by a selected time frame as well as customize the display options, refer to "Editing a preconfigured performance monitor" on page 263.

Accessing additional data from the Top Port Utilization monitor

- Right-click a row in the monitor to access the shortcut menu available for the associated device. For more information about shortcut menus, refer to "Application menus" on page 1261.
- Double-click a row to navigate to the **Historical Graphs/Tables** dialog box. For more information, refer to "Performance Data" on page 969.

Top Product CPU Utilization monitor

The **Top Product CPU Utilization** monitor (Figure 105) displays the top product CPU utilization percentages in a table.

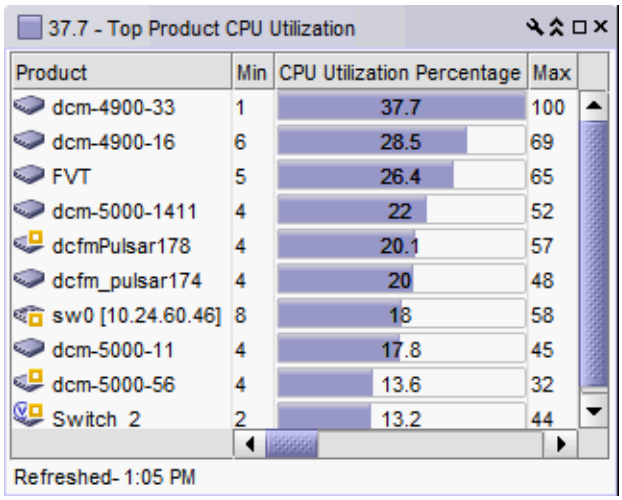


FIGURE 105 Top Product CPU Utilization monitor

The **Top Product CPU Utilization** monitor includes the following data:

- Severity icon/monitor title — The worst severity of the data shown next to the monitor title.
- **Product** — The product affected by this monitor.
- **Min** — The minimum value of the measure in the specified time range.
- **CPU Utilization Percentage** — The CPU utilization percentages.
- **Max** — The maximum value of the measure in the specified time range.
- **Fabric** — The fabric to which the device belongs.
- **Product Type** — The type of product (for example, switch).
- **State** — The product state (for example, Offline).
- **Status** — The product status (for example, Reachable).
- **Tag** — The product tag.
- **Serial #** — The serial number of the product.
- **Model** — The product model.
- **Port Count** — The number of ports on the product.
- **Firmware** — The firmware level running on the product.
- **Location** — The location of the product.

- **Contact —** A contact name for the product.
- **Refreshed** — The time of the last update for the monitor.

To customize the monitor to display data by a selected time frame as well as customize the display options, refer to "Editing a preconfigured performance monitor" on page 263.

Accessing additional data from the Top Product CPU Utilization monitor

- Right-click a row in the monitor to access the shortcut menu available for the associated device. For more information about shortcut menus, refer to "Application menus" on page 1261.
- Double-click a row to navigate to the **Historical Graphs/Tables** dialog box. For more information, refer to "Performance Data" on page 969.

Top Product Memory Utilization monitor

The **Top Product Memory Utilization** monitor (Figure 106) displays the top product memory utilization percentages in a table.

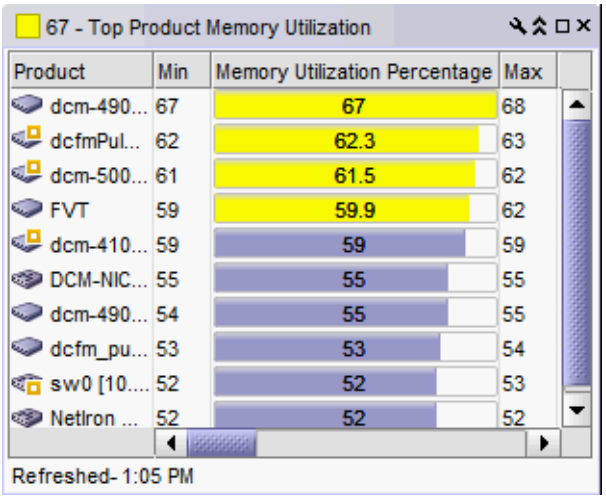


FIGURE 106 Top Product Memory Utilization monitor

The **Top Product Memory Utilization** monitor includes the following data:

- Severity icon/monitor title — The worst severity of the data shown next to the monitor title.
- **Product** — The product affected by this monitor.
- **Min** — The minimum value of the measure in the specified time range.
- **Memory Utilization Percentage** — The top memory utilization percentages.
- **Max** — The maximum value of the measure in the specified time range.
- **Fabric** — The fabric to which the device belongs.
- **Product Type** — The type of product (for example, switch).
- **State** — The product state (for example, Offline).
- **Status** — The product status (for example, Reachable).
- **Tag** — The product tag.

- **Serial # —** The serial number of the product.
- **Model** — The product model.
- **Port Count —** The number of ports on the product.
- **Firmware —** The firmware level running on the product.
- **Location —** The location of the product.
- **Contact —** A contact name for the product.
- **Refreshed** — The time of the last update for the monitor.

To customize the monitor to display data by a selected time frame as well as customize the display options, refer to "Editing a preconfigured performance monitor" on page 263.

Accessing additional data from the Top Product Memory Utilization monitor

- Right-click a row in the monitor to access the shortcut menu available for the associated device. For more information about shortcut menus, refer to "Application menus" on page 1261.
- Double-click a row to navigate to the **Historical Graphs/Tables** dialog box. For more information, refer to "Performance Data" on page 969.

Top Product Response Time monitor

The **Top Product Response Time** monitor (Figure 107) displays the top product response time in a table.

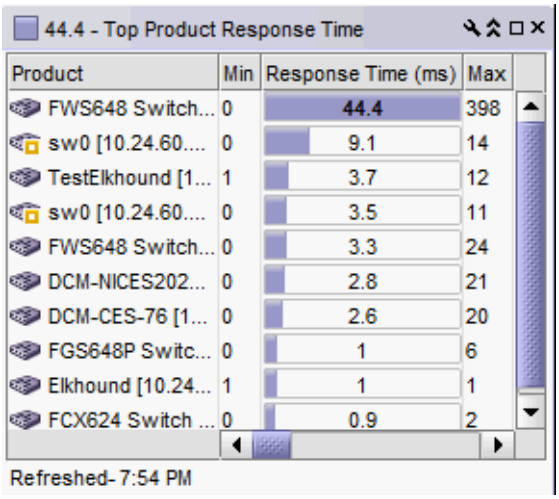


FIGURE 107 Top Product Response Time monitor

The **Top Product Response Time** monitor includes the following data:

- Severity icon/response time/monitor title — The worst severity of the data and the response time displays next to the monitor title.
- **Product** — The product affected by this monitor.
- **Min** — The minimum value of the measure in the specified time range.
- **Response Time (ms) —** The top response time in milliseconds.

- **Max** — The maximum value of the measure in the specified time range.
- **Fabric** — The fabric to which the device belongs.
- **Product Type** — The type of product (for example, switch).
- **State** — The product state (for example, Offline).
- **Status** — The product status (for example, Reachable).
- **Tag** — The product tag.
- **Serial #** — The serial number of the product.
- **Model** — The product model.
- **Port Count** — The number of ports on the product.
- **Firmware** — The firmware level running on the product.
- **Location** — The location of the product.
- **Contact** — A contact name for the product.
- **Refreshed** — The time of the last update for the monitor.

To customize the monitor to display data by a selected time frame as well as customize the display options, refer to "Editing a preconfigured performance monitor" on page 263.

Accessing additional data from the Top Product Response Time monitor

- Right-click a row in the monitor to access the shortcut menu available for the associated device. For more information about shortcut menus, refer to "Application menus" on page 1261.
- Double-click a row to navigate to the **Historical Graphs/Tables** dialog box. For more information, refer to "Performance Data" on page 969.

Top Product Temperature monitor

The **Top Product Temperature** monitor (Figure 108) displays the top product temperature in a table.

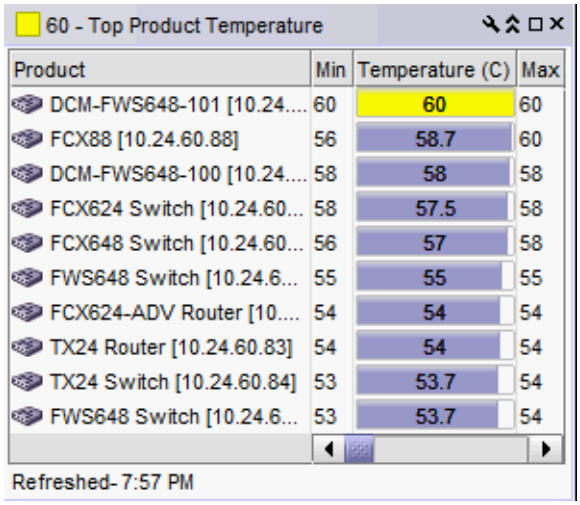


FIGURE 108 Top Product Temperature monitor

The **Top Product Temperature** monitor includes the following data:

- Severity icon/temperature/monitor title — The worst severity of the data and the temperature displays next to the monitor title.
- **Product** — The product affected by this monitor.
- **Min** — The minimum value of the measure in the specified time range.
- **Temperature** — The top temperatures.
- **Max** — The maximum value of the measure in the specified time range.
- **Fabric** — The fabric to which the device belongs.
- **Product Type** — The type of product (for example, switch).
- **State** — The product state (for example, Offline).
- **Status** — The product status (for example, Reachable).
- **Tag** — The product tag.
- **Serial #** — The serial number of the product.
- **Model** — The product model.
- **Port Count** — The number of ports on the product.
- **Firmware** — The firmware level running on the product.
- **Location** — The location of the product.
- **Contact** — A contact name for the product.
- **Refreshed** — The time of the last update for the monitor.

To customize the monitor to display data by a selected time frame as well as customize the display options, refer to "Editing a preconfigured performance monitor" on page 263.

Accessing additional data from the Top Product Temperature monitor

- Right-click a row in the monitor to access the shortcut menu available for the associated device. For more information about shortcut menus, refer to "Application menus" on page 1261.
- Double-click a row to navigate to the **Historical Graphs/Tables** dialog box. For more information, refer to "Performance Data" on page 969.

Top Products with Unused Ports monitor

The **Top Products with Unused Ports** monitor (Figure 105) displays the top products with ports not in use in a table.

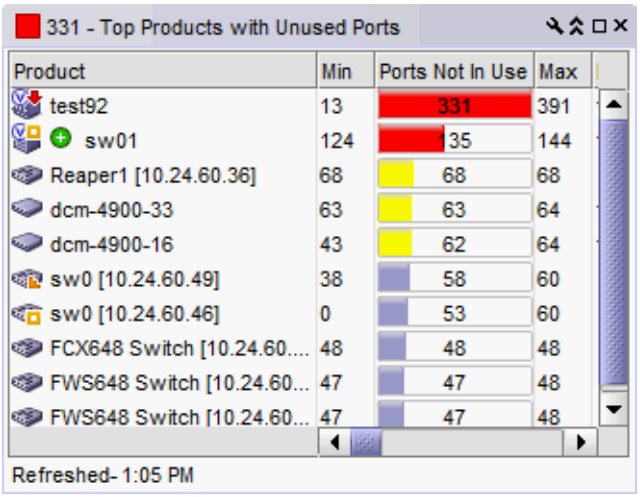


FIGURE 109 Top Product CPU Utilization monitor

The **Top Products with Unused Ports** monitor includes the following data:

- Severity icon/monitor title — The worst severity of the data shown next to the monitor title.
- **Product** — The product affected by this monitor.
- **Min** — The minimum value of the measure in the specified time range.
- **Ports Not In Use** — The number of ports not in use for the product.
- **Max** — The maximum value of the measure in the specified time range.
- **Fabric** — The fabric to which the device belongs.
- **Product Type** — The type of product (for example, switch).
- **State** — The product state (for example, Offline).
- **Status** — The product status (for example, Reachable).
- **Tag** — The product tag.
- **Serial #** — The serial number of the product.
- **Model** — The product model.
- **Port Count** — The number of ports on the product.
- **Firmware** — The firmware level running on the product.
- **Location** — The location of the product.
- **Contact** — A contact name for the product.
- **Refreshed** — The time of the last update for the monitor.

To customize the monitor to display data by a selected time frame as well as customize the display options, refer to "Editing a preconfigured performance monitor" on page 263.

Accessing additional data from the Top Product CPU Utilization monitor

- Right-click a row in the monitor to access the shortcut menu available for the associated device. For more information about shortcut menus, refer to "Application menus" on page 1261.
- Double-click a row to navigate to the **Historical Graphs/Tables** dialog box. For more information, refer to "Performance Data" on page 969.

Editing a preconfigured performance monitor

You can customize the monitor to display data by a selected time frame as well as customize the display options.

1. Click the edit icon ( ) on the monitor.

   From the **Performance** tab of the **Customize Dashboard** dialog box, select the monitor you want to edit and click **Edit**.

2. Select the number of products to include in a selected measure by entering a number in the **For Top N, Bottom N Monitors, N=** field.

   Valid values are from 1 through 25. The default is 10.

3. Configure the monitor to show only values greater than or less than a specified value by completing the following steps.

   a. Select the **Show values** check box.

   b. Select **greater than** or **less than** from the list.

   c. Enter a value in the field.

4. Configure threshold numbers and associated colors by completing the following steps.

   You can define three threshold numbers in decreasing order and four threshold colors. The default values are as follows: 90 and above displays red; 75 and above displays orange; 60 and above displays yellow; and all others display blue.

   a. Select the check box.

   b. Enter a number in the field.

   c. Click the color square to launch the **Color** dialog box.

      - To pick a color from a swatch, select the **Swatches** tab. Select a color from the display.
      - To specify a color based on hue, saturation, and brightness, click the **HSV** tab. Specify the hue (0 through 360 degrees), saturation (0 through 100%), value (0 through 100%), and transparency (0 through 100%).
      - To specify a color based on hue, saturation, and lightness, click the **HSL** tab. Specify the hue (0 through 360 degrees), saturation (0 through 100%), lightness (0 through 100%), and transparency (0 through 100%).
      - To specify a color based on values of red, green, and blue, click the **RGB** tab. Specify the values for red (0 through 255), green (0 through 255), blue (0 through 255), and alpha (0 through 255).
      - To specify a color based on values of cyan, magenta, yellow, and black, click the **CMYK** tab. Specify the values for cyan (0 through 255), magenta (0 through 255), yellow (0 through 255), black (0 through 255), and alpha (0 through 255).

- To reset to the default color, click **Reset**.

5. Click **OK** to save your changes.

User-defined performance monitors

The **Performance Dashboard** makes it easy for you to customize performance monitors specific to your needs. You can define up to 100 performance monitors; however, you can only display up to 30 performance monitors at a time.

Monitor types

You can create the following types of monitors:

- Top N (Products, Ports, and Traffic Flows monitors) — Displays the top number of products, ports, or traffic flows for the selected measure in a table.
- Bottom N (Products, Ports, and Traffic Flows monitors) Displays the bottom number of products, ports, or traffic flows for the selected measure in a table.
- Distribution (Products and Ports monitors) — Displays the number (distribution) of products or ports for each of the five percentage ranges defined for the selected measure in a bar graph
- Time Series (Products, Ports, and Traffic Flows monitors) — Displays the selected measures for products, ports, or traffic flows in a chart.
- Top N sFlows — Displays the top sFlow for MAC, IP, VM, or VLAN based on available flow data in a table.
- Performance graph — Displays the configured performance graph on the dashboard.

Measures

Depending on the object (products, ports, traffic) you want to monitor, you can choose from the following measures:

- Product
  - Memory Utilization Percentage — The memory utilization percentage for the product.
  - CPU Utilization Percentage — The CPU utilization percentage for the product.
  - Temperature — The temperature in Celsius for the product.
  - Fan Speed — The fan speed in RPM for the product.
  - Response Time — The response time in seconds for the product.
  - System Up Time — The system up time in days for the product.
  - Ports Not In Use — The number of ports not in use for the product.
  - Ping Packet Loss Percentage — The ping packet loss percentage for the product.
  - AP Client Count — The number of AP clients for the product.

- Port
  - Common
    - Port Utilization Percentage — The memory utilization percentage.
    - Traffic — The traffic in mbps.
    - CRC Errors — The number of CRC errors.
  - IP
    - Errors — The number of errors.
    - Discards — The number of discarded frames.
  - Wireless
    - Dropped Events — The number of dropped events.
    - MAC Errors — The number of MAC errors.
    - Back Packets Received — The number of bad packets received.
    - Tx Errors — The number of transmit errors.

Top or bottom product performance monitors

The top or bottom product performance monitors (Figure 110) display the top or bottom number of products (for example, top 10 products) for the selected measure in a table.

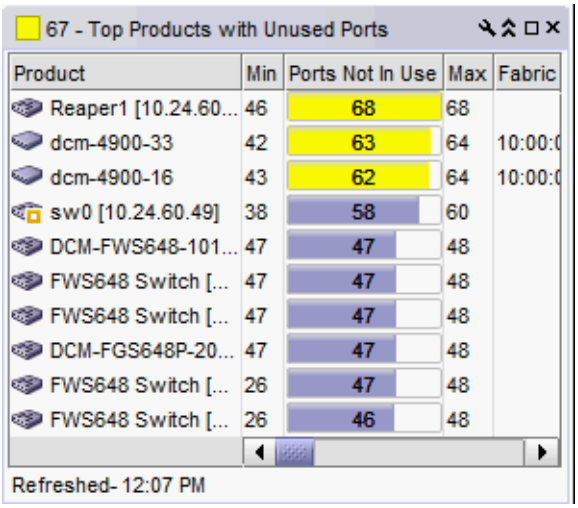


FIGURE 110 Top or bottom product performance monitor example

The top or bottom product performance monitor includes the following data:

- Threshold icon/object count/monitor title — The color associated with the threshold and number of objects within that threshold displays next to the monitor title.
- **Product** — The product affected by this monitor.
- **Min** — The minimum value of the measure in the specified time range.
- *Measure_Type* — The percentage bar of the selected measure.

  By default, products display sorted by the *Measure_Type* value (Top products sort from highest to lowest and bottom products sort lowest to highest). Click a column head to sort the columns by that value.

- **Max** — The maximum value of the measure in the specified time range.
- **Fabric** — The fabric to which the device belongs.
- **Product Type** — The type of product (for example, switch).
- **State** — The product state (for example, Offline).
- **Status** — The product status (for example, Reachable).
- **Tag** — The product tag.
- **Serial # —** The serial number of the product.
- **Model** — The product model.
- **Port Count —** The number of ports on the product.
- **Firmware —** The firmware level running on the product.
- **Location —** The location of the product.
- **Contact —** A contact name for the product.
- **Refreshed** — The time of the last update for the monitor.

To configure a product performance monitor, refer to "Configuring a user-defined product performance monitor" on page 270.

Accessing additional data from top or bottom product monitors

In a Top N or Bottom N monitor, double-click a row or right-click a row and select **Show Graph/Table** to navigate to the **Historical Graphs/Tables** dialog box for the selected measures. For more information, refer to "Performance Data" on page 969.

Top or bottom port performance monitors

The top or bottom port performance monitors (Figure 111) display the top or bottom number of ports (for example, bottom 10 ports) for the selected measure in a table.

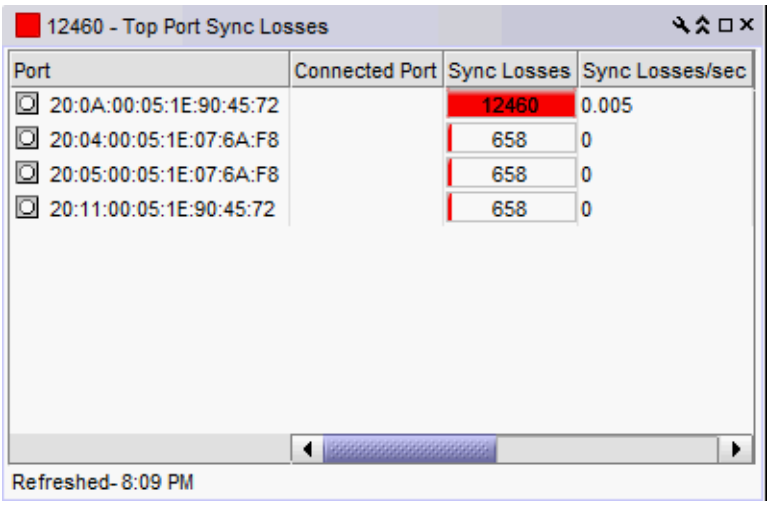


FIGURE 111 Top or bottom port performance monitor example

The top or bottom port performance monitor includes the following data:

- Threshold icon/object count/monitor title — The color associated with the threshold and number of objects within that threshold displays next to the monitor title.
- Severity icon/monitor title — The worst severity of the data based on the error count or error rate shown next to the monitor title.
- **Port** — The port affected by this monitor.
- *Connected_Port_Link* (where *Connected_Port_Link* is **Connected Port**, **Initiator**, or **Target**) — Displays one of the following:
  - **Connected Port** — The ISL or IFL port on the connected device. Click to launch the switch port properties dialog box.
  - **Initiator** — The initiator port on the connected device. Click to launch the device properties dialog box.
  - **Target** — The target port on the connected device. Click to launch the device properties dialog box.
- *Measure_Type* — The percentage bar of the selected measure. Depending on the selected measure, both the error rate (per second) and error count may display. For selected measures, more than one **Measure_Type** may display (for example RX and TX).

  By default, ports display sorted by the **Measure_Type** value (Top ports sort from highest to lowest and bottom ports sort lowest to highest). Click a column head to sort the columns by that value.
- **Product** — The product affected by this monitor.
- **Type** — The type of port (for example, U-Port).
- **Identifier** — The port identifier.
- **Port Number** — The port number.
- **State** — The port state (for example, Enabled).
- **Status** — The port status (for example, Up).
- **Refreshed** — The time of the last update for the monitor.

To configure a port performance monitor, refer to "Configuring a user-defined port performance monitor" on page 273.

Accessing additional data from top or bottom port monitors

- In a Top N or Bottom N monitor, double-click a row or right-click a row and select **Show Graph/Table** to navigate to the **Historical Graphs/Tables** dialog box for the selected measures. For more information, refer to "Performance Data" on page 969.

Distribution performance monitors

The distribution performance monitor (Figure 112) displays the distribution (number) of products or ports for each of the five percentage ranges defined for the selected measure in a bar graph.

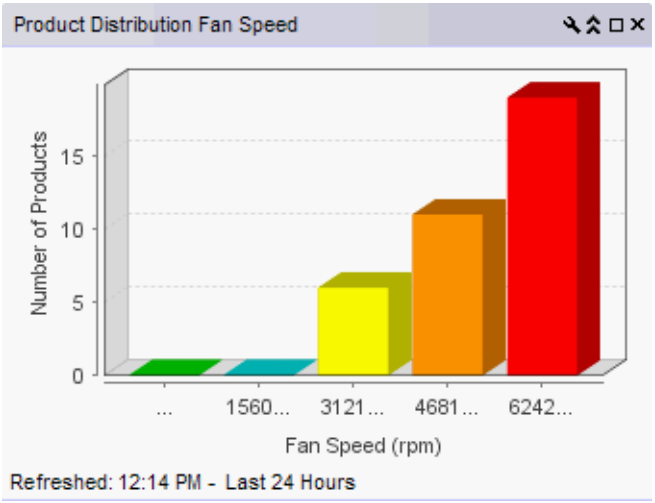


FIGURE 112 Distribution performance monitor example

The distribution performance monitor includes the following data:

- Monitor title — The user-defined monitor title.
- **Number of Products/Ports** (y-axis) — The y-axis always displays a numbered range (zero to the maximum number of objects) for the products or ports affected by the selected measure.
- *Measure_Type* (x-axis) — The x-axis display depends on the *Measure_Type* you selected for this monitor. Each bar on the graph maps directly to one of the five percentage ranges defined for the monitor. *Measure_Type* includes the following measures:

TABLE 24 Product measures types

- Memory Utilization Percentage
- CPU Utilization Percentage
- Temperature (C)
- Fan Speed (rpm)
- Response Time (s)
- System Up Time (days)
- Ports Not In Use
- Ping Packet Loss Percentage
- AP Client Count

TABLE 25 Port measures types

Common
- Port Utilization Percentage
- Traffic
- CRC Errors

IP
- Errors
- Discards

Wireless
- Dropped Events
- MAC Errors
- Back Packets Received
- Tx Errors

- **Refreshed** — The time of the last update for the monitor.

To configure a distribution performance monitor, refer to "Configuring a user-defined product performance monitor" on page 270 or "Configuring a user-defined port performance monitor" on page 273.

Accessing additional data from the Distribution monitors

- Place the cursor on a bar in the graph to display the number of products included in the count for the selected bar. For example, the tooltip "(Data Item 3, 22.6-33.8) = 6" means that there are six products within the third percentage range (displays the temperatures within the percentage range) for the selected measure (product temperature).
- Double-click a percentage range to navigate to the *Monitor_Title* **Distribution Data Details** dialog box. for more information, refer to "Viewing product distribution data details" on page 276 or "Viewing port distribution data details" on page 277.

Time series performance monitors

The time series performance monitors (Figure 113) display the selected measures in a chart.

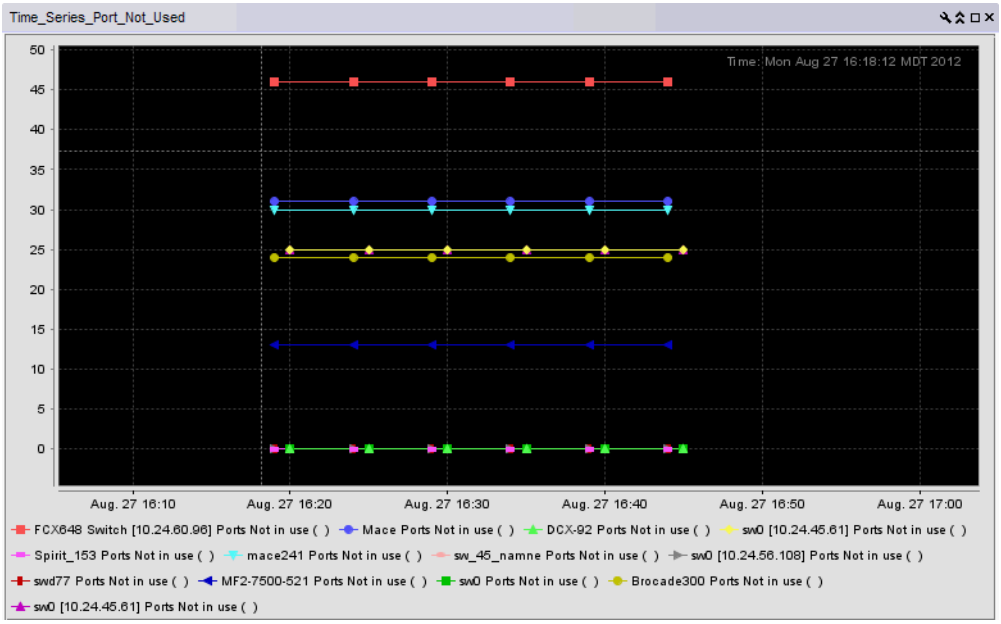


FIGURE 113 Time series performance monitor example

The time series performance monitor includes the following data:

- Monitor title — The user-defined monitor title.
- **Value** (y-axis) — The number of objects affected by this monitor.
- **Time** (x-axis) — The date and time the monitor collected the data.
- **Legend** (below the x-axis) — The line color and the associated data that each line represents.
- Network Scope — The network scope, such as Local or Published. Displays Local if you select the targets when creating the monitor. Displays Published if you select the **Use Network Scope** check box when creating the monitor.

Place the cursor on a data point in graph line to view details. Place the cursor on an Event icon to view the event details. Right-click the graph to access the graph shortcut menu (refer to "Configuring the performance graph" on page 989).

To configure a time series performance monitor, refer to "Configuring a user-defined product performance monitor" on page 270 or "Configuring a user-defined port performance monitor" on page 273.

Top sFlows performance monitors

The top sFlows performance monitors display the top sFlow measures based on available flow data in a table.

The top sFlow performance monitor includes the following data:

- MACs, IP Addresses, VMs, or VLANs — The number of products and associated ports affected by this monitor.
- **Port In —** The in port number.
- **Port Out —** The out port number.
- **MBytes —** The port speed.
- **Frames —** The number of frames.
- **Percentage —** The sFlow percentage for the product or port.

To configure an sFlow performance monitor, refer to "Configuring a user-defined sFlow performance monitor" on page 275.

Accessing additional data from the sFlow monitors

- Double-click a device row to navigate to the **sFlow Monitor Report** dialog box. For more information, refer to "Displaying sFlow monitoring reports" on page 1038.

Configuring a user-defined product performance monitor

1. From the **Dashboards** expand navigation bar, double-click **Performance Dashboard**.

   The **Performance Dashboard** displays.

2. Click the **Customize Dashboard** icon.

   The **Customize Dashboard** dialog box displays.

3. Click the **Performance** tab.

4. Click **Add**.

   The **Add Performance Dashboard Monitor** dialog box displays.

5. Enter a unique title for the monitor.

   The title can be up to 256 characters in length.

6. Select the type of monitor you are creating from the **Monitor Type - Products** area:

   - **Top N** — Select to monitor the top N (number) products affected by the selected measure.
   - **Bottom N** — Select to monitor the bottom N (number) products affected by the selected measure.
   - **Distribution** — Select to monitor the selected measure for five defined distribution percentages.

- **Time Series** — Select to monitor a selected measure for a range of time and specified target.

7. Select the product measure for the monitor in the **Measure** area:
   - **Memory Utilization Percentage**
   - **CPU Utilization Percentage**
   - **Temperature**
   - **Fan Speed**
   - **Response Time**
   - **System Up Time**
   - **Ports Not In Use**
   - **Ping Packet Loss Percentage**
   - **AP Client Count** (not available for Time Series monitors)
8. (Top N and Bottom N monitors only) Select the number products to include in a selected measure by entering a number in the **For Top N, Bottom N Monitors, N=** field.

   Valid values are from 1 through 25. The default is 10.
9. (Top N, Bottom N, and Distribution monitors only) Configure the monitor to show only values greater than or less than a specified value by completing the following steps.
   a. Select the **Show values** check box.
   b. Select **greater than** or **less than** from the list.
   c. Enter a value in the field.
10. (Top N, Bottom N, and Distribution monitors only) Configure threshold numbers and associated colors by completing the following steps.

    Depending on the monitor type you select, you can define up to four threshold numbers in increasing or decreasing order and up to five associated threshold colors.

    (Top N and Bottom N monitors only) The decreasing order defaults are as follows: 90 and above displays red, 75 and above displays orange, 60 and above displays yellow, and all others display blue. The maximum values allowed are -32,768 through 32,767 for SFP power and 0 through 32,767 for all other measures.

    (Distribution monitors only) The increasing order defaults are as follows: 0 through 20 displays green, 21 through 40 displays blue, 41 through 60 displays yellow, 61 through 80 displays orange, and 81 through 100 displays red.

    a. (Top N and Bottom N monitors only) Select the check box.
    b. Enter a number in the field.
    c. Click the color square to launch the **Color** dialog box.
       - To pick a color from a swatch, select the **Swatches** tab. Select a color from the display.
       - To specify a color based on hue, saturation, and brightness, click the **HSV** tab. Specify the hue (0 through 360 degrees), saturation (0 through 100%), value (0 through 100%), and transparency (0 through 100%).
       - To specify a color based on hue, saturation, and lightness, click the **HSL** tab. Specify the hue (0 through 360 degrees), saturation (0 through 100%), lightness (0 through 100%), and transparency (0 through 100%).

- To specify a color based on values of red, green, and blue, click the **RGB** tab. Specify the values for red (0 through 255), green (0 through 255), blue (0 through 255), and alpha (0 through 255).
- To specify a color based on values of cyan, magenta, yellow, and black, click the **CMYK** tab. Specify the values for cyan (0 through 255), magenta (0 through 255), yellow (0 through 255), black (0 through 255), and alpha (0 through 255).
- To reset to the default color, click **Reset**.

11. (Time series monitors only) Add targets for the monitor by clicking **Add** and completing steps in "Adding targets to a user-defined performance monitor" on page 272.

    Remove targets from the monitor by selecting one or more targets in the **Targets** list and clicking **Remove**.

12. Click **OK** on the **Add Performance Dashboard Monitor** dialog box.

    The **Customize Dashboard** dialog box displays with the new monitor in the **Performance Monitors** list.

13. Click **OK** on the **Customize Dashboard** dialog box.

    The **Performance Dashboard** dialog box displays with the new monitors at the bottom of the dashboard.

Accessing additional data from user-defined product performance monitors

- In a Distribution monitor, double-click a percentage range to navigate to the *Measure_Type* **Distribution Data Details** dialog box. For more information, refer to "Viewing product distribution data details" on page 276 or "Viewing port distribution data details" on page 277.
- In a Top N or Bottom N product monitor, double-click a row or right-click a row and select **Show Graph/Table** to navigate to the **Historical Graphs/Tables** dialog box for the selected measures. For more information, refer to "Performance Data" on page 969.
- In a Top N sFlow monitor, double-click a device row to navigate to the **sFlow Monitor Report** dialog box. For more information, refer to "Interpreting an sFlow traffic report" on page 1041.

Adding targets to a user-defined performance monitor

You can only add targets for Time Series monitors.

1. From the **Dashboards** expand navigation bar, double-click **Performance Dashboard**.

   The **Performance Dashboard** displays.

2. Click the **Customize Dashboard** icon.

   The **Customize Dashboard** dialog box displays.

3. Click the **Performance** tab.
4. Click **Add**.

   The **Add Performance Dashboard Monitor** dialog box displays.

5. Select **Time Series** from the **Monitor Type - Product** or **Port** area.
6. Select the port measure for the monitor in the **Measure** area
7. Display data for a specific duration from the **Duration** options.

8. Click **Add** beneath the **Targets** table.

   The **Performance Dashboard Monitor Targets** dialog box displays.

   Depending on the type of measure you select, you can add IP products/ports to the list of targets.

   If you selected a product measure, continue with step 9.

   If you selected an IP port measure, continue with step 9.

9. Click the **IP** tab.
10. Select IP targets from the **Available IP Sources** list.
11. Click the right arrow button to move the targets to the **Selected Sources** list.
12. Click **OK** on the **Performance Dashboard Monitor Targets** dialog box.

    The targets display in the **Targets** list of the **Add Performance Dashboard Monitor** dialog box.

13. Click **OK** on the **Add Performance Dashboard Monitor** dialog box.

    The **Customize Dashboard** dialog box displays with the new monitor in the **Performance Monitors** list.

14. Click **OK** on the **Customize Dashboard** dialog box.

    The **Performance Dashboard** dialog box displays with the new monitors at the bottom of the dashboard.

Configuring a user-defined port performance monitor

1. From the **Dashboards** expand navigation bar, double-click **Performance Dashboard**.

   The **Performance Dashboard** displays.

2. Click the **Customize Dashboard** icon.

   The **Customize Dashboard** dialog box displays.

3. Click the **Performance** tab.
4. Click **Add**.

   The **Add Performance Dashboard Monitor** dialog box displays.

5. Select the type of monitor you are creating from the **Monitor Type - Port** area:
   - **Top N** — Select to monitor the top N (number) ports affected by the selected measure.
   - **Bottom N** — Select to monitor the bottom N (number) ports affected by the selected measure.
   - **Distribution** — Select to monitor the selected measure for five defined distribution percentages.
   - **Time Series** — Select to monitor a selected measure for a range of time and specified targets.
6. Select the port measure for the monitor in the **Measure** area:

Common
- Port Utilization Percentage
- Traffic
- CRC Errors

IP
- Errors
- Discards

Wireless
- Dropped Events
- MAC Errors
- Back Packets Received
- Tx Errors

7. (Top N and Bottom N monitors only) Select the number of ports to include in a selected measure by entering a number in the **For Top N, Bottom N Monitors, N=** text box.

   Valid values are from 1 through 25. The default is 10.

8. (Top N, Bottom N, and Distribution monitors only) Configure the monitor to show only values greater than or less than a specified value by completing the following steps.

   a. Select the **Show values** check box.

   b. Select **greater than** or **less than** from the list.

   c. Enter a value in the field.

9. (Top N, Bottom N, and Distribution monitors only) Configure threshold numbers and associated colors by completing the following steps.

   Depending on the monitor type you select, you can define up to four threshold numbers in increasing or decreasing order and up to five associated threshold colors.

   (Top N and Bottom N monitors only) The decreasing order defaults are as follows: 90 and above displays red, 75 and above displays orange, 60 and above displays yellow, and all others display blue. The maximum values allowed are -32,768 through 32,767 for SFP power and 0 through 32,767 for all other measures.

   (Distribution monitors only) The increasing order defaults are as follows: 0 through 20 displays green, 21 through 40 displays blue, 41 through 60 displays yellow, 61 through 80 displays orange, and 81 through 100 displays red.

   a. (Top N and Bottom N monitors only) Select the check box.

   b. Enter a number in the field.

   c. Click the color square to launch the **Color** dialog box.

      - To pick a color from a swatch, select the **Swatches** tab. Select a color from the display.
      - To specify a color based on hue, saturation, and brightness, click the **HSV** tab. Specify the hue (0 through 360 degrees), saturation (0 through 100%), value (0 through 100%), and transparency (0 through 100%).
      - To specify a color based on hue, saturation, and lightness, click the **HSL** tab. Specify the hue (0 through 360 degrees), saturation (0 through 100%), lightness (0 through 100%), and transparency (0 through 100%).
      - To specify a color based on values of red, green, and blue, click the **RGB** tab. Specify the values for red (0 through 255), green (0 through 255), blue (0 through 255), and alpha (0 through 255).

- To specify a color based on values of cyan, magenta, yellow, and black, click the **CMYK** tab. Specify the values for cyan (0 through 255), magenta (0 through 255), yellow (0 through 255), black (0 through 255), and alpha (0 through 255).
- To reset to the default color, click **Reset**.

10. (Time series monitors only) Add targets for the monitor by clicking **Add** and completing the steps in "Adding targets to a user-defined performance monitor" on page 272.

    Remove targets from the monitor by selecting one or more targets in the **Targets** list and clicking **Remove**.

11. Click **OK** on the **Add Performance Dashboard Monitor** dialog box.

    The **Customize Dashboard** dialog box displays with the new monitor in the **Performance Monitors** list.

12. Click **OK** on the **Customize Dashboard** dialog box.

    The **Performance Dashboard** dialog box displays with the new monitors at the bottom of the dashboard.

Accessing additional data from user-defined port performance monitors

- In a Distribution monitor, double-click a percentage range to navigate to the *Measure_Type* **Distribution Data Details** dialog box. For more information, refer to "Viewing product distribution data details" on page 276 or "Viewing port distribution data details" on page 277.
- In a Top N or Bottom N monitor, double-click a row or right-click a row and select **Show Graph/Table** to navigate to the **Historical Graphs/Tables** dialog box for the selected measures. For more information, refer to "Performance Data" on page 969.
- In a Top N sFlow monitor, double-click a device row to navigate to the **sFlow Monitor Report** dialog box. For more information, refer to "Interpreting an sFlow traffic report" on page 1041.

Configuring a user-defined sFlow performance monitor

1. From the **Dashboards** expand navigation bar, double-click **Performance Dashboard**.

   The **Performance Dashboard** displays.

2. Click the **Customize Dashboard** icon.

   The **Customize Dashboard** dialog box displays.

3. Click the **Performance** tab.

4. Click **Add**.

   The **Add Performance Dashboard Monitor** dialog box displays.

5. Select the type of monitor you are creating from the **Monitor Type - Top N sFlows** area:

   - **MAC**
   - **IP**
   - **VM**
   - **VLAN**

6. Select the number of products to include in a selected measure by entering a number in the **For Top N, Bottom N Monitors, N=** text box.

Valid values are from 1 through 25. The default is 10.

7. Configure the monitor to show only values greater than or less than a specified value by completing the following steps.
   a. Select the **Show values** check box.
   b. Select **greater than** or **less than** from the list.
   c. Enter a value in the field.
8. Add targets for the monitor by clicking **Add** and completing the steps in "Adding targets to a user-defined performance monitor" on page 272.
9. Remove targets from the monitor by selecting one or more targets in the **Targets** list and clicking **Remove**.
10. Click **OK** on the **Add Performance Dashboard Monitor** dialog box.

    The **Customize Dashboard** dialog box displays with the new monitor in the **Performance Monitors** list.
11. Click **OK** on the **Customize Dashboard** dialog box.

    The **Performance Dashboard** dialog box displays with the new monitors at the bottom of the dashboard.

Accessing additional data from user-defined sFlow performance monitors

- In a Top N sFlow monitor, double-click a device row to navigate to the **sFlow Monitor Report** dialog box. For more information, refer to "Interpreting an sFlow traffic report" on page 1041.

Viewing product distribution data details

Each bar on the product distribution graph maps directly to one of the five percentage ranges defined for the distribution performance monitor (refer to "Distribution performance monitors" on page 267).

1. Double-click a bar in the graph.

   The *Monitor_Title* **Data Details** dialog box displays.
2. Review the data.

   The product distribution data details include the following fields and components:

   - **Product** — The name of the product affected by the selected measure.
   - *Measure_Type* — This column depends on which measure you select for the monitor.
     - Memory Utilization Percentage — The memory utilization percentage for the product.
     - CPU Utilization Percentage — The CPU utilization percentage for the product.
     - Temperature — The temperature in Celsius for the product.
     - Fan Speed — The fan speed in RPM for the product.
     - Response Time — The response time in seconds for the product.
     - System Up Time — The system up time in days for the product.
     - Ports Not In Use — The number of ports not in use for the product.
     - Ping Packet Loss Percentage — The ping packet loss percentage for the product.
     - AP Client Count — The number of AP clients for the product.

- **Fabric** — The fabric to which the device belongs.
- **Product Type** — The type of product (for example, switch).
- **State** — The product state (for example, Offline).
- **Status** — The product status (for example, Reachable).
- **Tag** — The product tag.
- **Serial #** — The serial number of the product.
- **Model** — The product model.
- **Port Count** — The number of ports on the product.
- **Firmware** — The firmware level running on the product.
- **Location** — The location of the product.
- **Contact** — A contact name for the product.

3. Click **Close**.

Viewing port distribution data details

Each bar on the port distribution graph maps directly to one of the five percentage ranges defined for the distribution monitor (refer to "Distribution performance monitors" on page 267).

1. Double-click a bar in the graph.

   The *Monitor_Title* **Data Details** dialog box displays.

2. Review the data.

   The port distribution data details include the following fields and components:

   - **Port** — The port affected by the selected measure.
   - **TX/RX** — Whether the port is transmitting (TX) or receiving (RX) data. This column is not available for all measures.
   - *Measure_Type* — This column depends on which measure you select for the monitor.
     - Common
       - Port Utilization Percentage — The memory utilization percentage.
       - Traffic — The traffic in mbps.
       - CRC Errors — The number of CRC errors.
     - IP
       - Errors — The number of errors.
       - Discards — The number of discarded frames.
     - Wireless
       - Dropped Events — The number of dropped events.
       - MAC Errors — The number of MAC errors.
       - Back Packets Received — The number of bad packets received.
       - Tx Errors — The number of transmit errors.
   - **Product** — The product affected by this monitor.
   - **Type** — The type of port (for example, U-Port).
   - **Identifier** — The port identifier.

- **Port Number** — The port number.
- **State** — The port state (for example, Enabled).
- **Status** — The port status (for example, Up).

3. Click **Close**.

Configuring a monitor from a performance graph

1. Configure the performance graph.

   To configure a real-time performance graph, refer to "Monitoring real-time performance" on page 983. To configure a historical performance graph, refer to "Performance Data" on page 969.

2. Click **Save As Widget** to create a monitor of the graph data for the dashboard.

   The **Performance Dashboard Monitor Title** dialog box displays. The Management application generates a default name for the monitor using the following naming convention: *Chart_Type - MM DD, YYYY HH:MM* AM/PM. For example, Realtime Chart Monitor - Nov 2, 2012 11:02 AM. For more information, refer to "Viewing Historical Graphs/Tables" on page 1009.

3. Enter a unique name for the monitor and click **OK**.
4. Click **OK** on the confirmation message.

Chapter

8

View Management

In this chapter

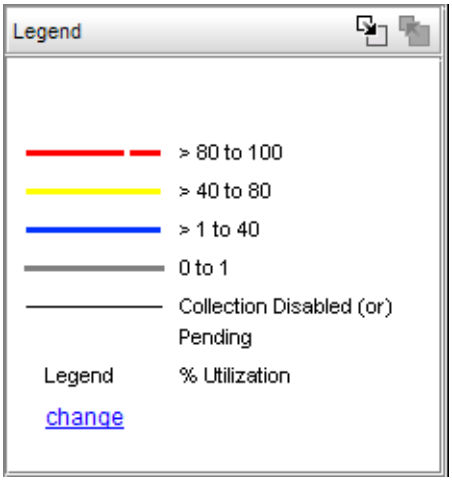


FIGURE 114 Utilization Legend

IP tab overview

The **IP** tab displays the Product List, Topology Map, Master Log, and Minimap.

You can change the default size of the display by placing the cursor on the divider until a double arrow displays. Click and drag the adjoining divider to resize the window. You can also show or hide an area by clicking the left or right arrow on the divider.

The following graphic illustrates the various areas, and descriptions of them are listed below.

NOTE
Some areas may be hidden by default. To view areas of the **IP** tab, select **View > Show Panels > All Panels**, or press **F12**.

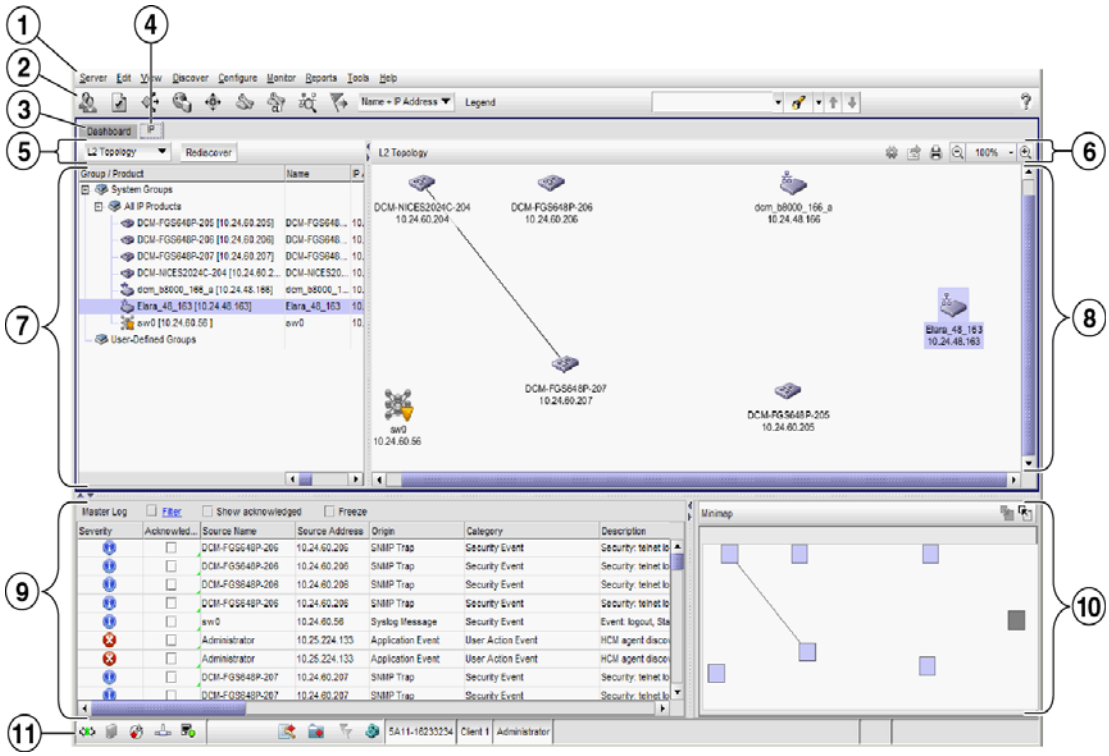


FIGURE 115 Main Window - IP tab

1. **Menu bar —** Lists commands you can perform on the **IP** tab. Some menu items display as disabled unless you select the correct object from the product list or topology map. For a list of the many functions available on each menu, refer to "IP main menus" on page 1262.
2. **IP main toolbar —** Provides buttons that enable quick access to dialog boxes and functions. For more information, refer to "IP main toolbar" on page 281.
3. **Dashboard tab —** Provides a high-level overview of the network managed by Management application server. For more information, refer to the "Dashboard Management" on page 211.
4. **IP tab —** Displays the Master Log, Minimap, Connectivity Map (topology), and Product List.
5. **Product List toolbar —** Enables you to select the type of topology map you want to display in the main window. Does not display until you discover a product or network. For more information, refer to "Network Objects view" on page 307.

6. **Topology Map toolbar —** Provides tools for viewing the Topology Map as well as exporting the Topology Map as an image. Does not display until you discover a device or network. For more information, refer to "Topology Map toolbar" on page 283.
7. **Product List —** Lists the products discovered in the Management application. For more information, refer to "IP Product List" on page 284.
8. **Topology Map —** Displays the topology, including discovered and monitored devices and connections. For more information, refer to "Topology Map" on page 285.
9. **Master Log —** Displays all events that have occurred on the Management application. For more information, refer to "Master Log" on page 287.
10. **Minimap —** Displays a "bird's-eye" view of the entire topology. Does not display until you discover a fabric. For more information, refer to "Minimap" on page 288.
11. **Status bar —** Displays data regarding the connection, port, product, special event, call home, and backup status, as well as Server and User data. For more information, refer to "Status bar" on page 289.

IP main toolbar

The toolbar is located beneath the Menu bar and provides icons to perform various functions.

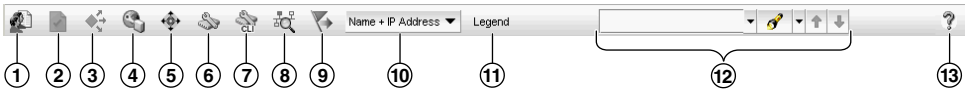


FIGURE 116 Main toolbar

The icons on your toolbar vary based on the licensed features on your system.

1. **Users —** Displays the **Users** dialog box. Use to configure users, roles, and areas of responsibility.
2. **Properties —** Displays the **Properties** dialog box of the selected device. Use to view or edit device properties.
3. **Launch Element Manager —** Launches the Element Manager of the selected device. Use to configure a device through its Element Manager.
4. **IP Product Discovery —** Displays the **Discover Setup - IP** dialog box. Use to configure discovery.
5. **Zoning —** Displays the **Zoning** dialog box. Use to configure zoning.
6. **Configuration Wizard** — Displays the **Configuration Wizard**. Use to create and deploy product configurations as well as configure payloads.
7. **CLI Configuration —** Displays the **CLI Configuration** dialog box. Use to create, verify, and deploy global and product monitoring configurations.
8. **Configuration Repository** — Displays the **Configuration Repository** dialog box. Use to set up, track, and back up product configurations.
9. **Event Actions** — Displays the **Event Actions** dialog box. Use to manage event actions for SAN and IP configurations.
10. **Product Label** — Use to set the device labels to display as Name and IP Address, Name, or IP Address.

11. **Legend —** Use to view the topology legend. For more information, refer to "Topology map elements" on page 315.
12. **Product List Search —** Use to search for a device in the product list.
13. **Help —** Displays the Online Help.

Product List toolbar

This toolbar is located at the top of the product list and provides lists, links, and buttons to perform various functions. The items on this toolbar vary based on what you select from the **Type** list.

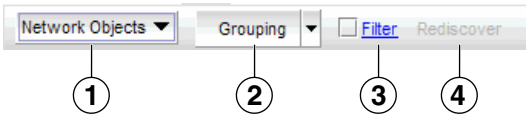


FIGURE 117 Product list toolbar

1. View list — Use to select the one of the following view types: Network Objects, IP Topology, L2 Topology, and VLAN Topology.

   The areas of the main display vary depending on the display type you select.

   - **Network Objects** — Displays the Product List toolbar, Product List, and Master Log.
   - **L2 Topology** — Displays the Product List toolbar, Product List, Topology Map toolbar, Topology Map, Master Log, and Minimap.
   - **Ethernet Topology** — Displays the Product List toolbar, Product List, Topology Map toolbar, Topology Map, Master Log, and Minimap.
   - **IP Topology** — Displays the Product List toolbar, Product List, Topology Map toolbar, Topology Map, Master Log, and Minimap.
   - **VLAN Topology** — Displays the Product List toolbar, Product List, Topology Map toolbar, Topology Map, Master Log, and Minimap.
   - **Host Topology** — Displays the Host Product List toolbar, Product List, Topology Map toolbar, Topology Map, Master Log, and Minimap.
2. **Grouping** type list — Use to create product and port groups, as well as edit, duplicate, and delete groups. Only displays when you select **Network Objects** from the **Type** list.
3. **Filter** check box and link — Use to create a product filter based on reachability status. Only displays when you select **Network Objects** from the **Type** list.
4. **Rediscover** button — Use to restart the discovery process.

Host Product List toolbar

The **Port Display** buttons are located at the top right of the Product List and enable you to configure how ports display. You have the option of viewing connected (or occupied) product ports, unoccupied product ports, or attached ports. Not enabled until you discover a fabric or host.

NOTE
Occupied/connected ports are those that originate from a device, such as a switch. Attached ports are ports of the target devices that are connected to the originating device.

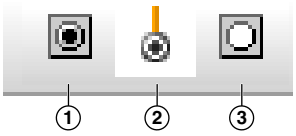


FIGURE 118 Port Display buttons

1. **Show/Hide Occupied Port** — Displays or hides the ports of the devices in the fabrics (present in the topology map) that are connected to other devices.
2. **Show/Hide Attached Port** — Displays or hides the attached ports of the target devices.
3. **Show/Hide Unoccupied Port** — Displays or hides the ports of the devices (shown in the topology map) that are not connected to any other device.

Topology Map toolbar

This toolbar is located at the top of the Topology Map and provides icons and buttons to perform various functions.

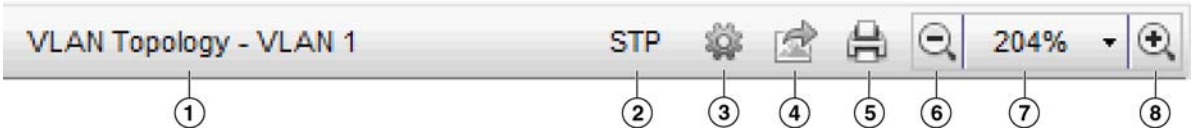


FIGURE 119 Topology Map toolbar

The items on the Topology Map toolbar vary based on what you select from the **Type** list on the Product List toolbar.

1. View Name — Name of the selected topology.
2. **STP** button — Only displays when you select **VLAN Topology** from the View list. Use to enable or disable STP. Rest cursor on button to display tooltip.
3. **Topology Display** button — Use select the layout, add an map image, or change the background color for the topology map.
4. **Export** icon — Use to export the topology to a PNG file.
5. **Print** icon — Use to print the current Topology Map image.
6. **Zoom Out** icon — Use to zoom out on the Topology Map.

7. Reset zoom list — Use to reset the zoom (Actual Size, Fit Content, 25%, 50%, 75%, 100%, 125%, 150%, 200%, or 500%) of the Topology Map.
8. **Zoom In** icon — Use to zoom in on the Topology Map.

Host topology map toolbar

The Host Topology map toolbar is located at the top right side of the **View** window and provides tools to export the topology, to zoom in and out of the Topology Map, collapse and expand groups, and fit the topology to the window. Not enabled until you discover a host.

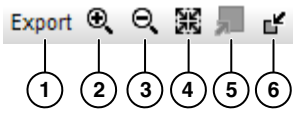


FIGURE 120 Host Topology Map toolbar

1. **Export** — Use to export the topology to a PNG file.
2. **Zoom In** — Use to zoom in on the Connectivity Map.
3. **Zoom Out** — Use to zoom out on the Connectivity Map.
4. **Fit in View** — Use to scale the map to fit within the Connectivity Map area.
5. **Expand** — Use to expand the map to show all ports in use on a device.
6. **Collapse** — Use to collapse the map to show only devices (hides ports).

IP Product List

Lists the devices discovered in the Management application.

The Product List, located on the **IP** tab, displays an inventory of all discovered devices and ports. The Product List is a quick way to look up product and port information, including serial numbers and IP addresses.

To display the Product List, select **View > Show Panels > Product List** or press **F9**.

You can edit information in the Product List by double-clicking in a field marked with a green triangle. You can sort the Product List by clicking a column heading.

The following columns (presented here in default order) are included in the Product List.

- **Group/Product** — The icon and name of the product or product group. Also, the status of the product or product group.

  For VDX/VCS products, the status is computed from the operational status and reachability status.
- **Name** — Displays the name of the product.
- **IP Address** — Displays the IP address (IPv4 or IPv6 format) of the product.
- **Product Type** — Displays the type of product, such as Router or L2 Switch.
- **Serial #** — Displays the serial number of the product.

- **Status —** Displays the status for the produc, such as Reachable, Marginal, Degraded Link, or Not Reachable.
- **State** (Ethernet Fabrics only) — Displays the Ethernet Fabric state, such as online or offline.
- **Vendor —** Displays the name of the product's vendor.
- **Model —** Displays the model number of the product.
- **Port Count —** Displays the number of ports on the product.
- **Firmware —** Displays the firmware version of the product.
- **Build Label** (not available for Ethernet Fabrics or Network Objects) **—** Displays the firmware build number.
- **Location —** Displays the physical location of the product.
- **Contact —** Displays the name of the person or group you should contact about the product.
- **Description —** Displays the description of the product.
- User-defined property labels — Displays the user-defined property labels. You can create up to three user-defined property labels.

Product List functions

- Customize — Customize the Product list. For more information, refer to "Product List customization" on page 297.
- Sort — Click a column head to sort the list. Click a column head again to reverse the sort order
- Two-way selection — Select a device in the Product List and that device is highlighted on the Topology Map and vice versa.
- Table shortcut menus — Right-click a column header in the Product List to view the menu. For a list of right-click menus, refer to "Customizing application tables" on page 294.
- Device shortcut menus — Right-click a device in the Product List to view the menu. For a list of right-click menus, refer to "IP shortcut menus" on page 1268.

Topology Map

The Topology map displays the topology, including discovered and monitored devices and connections. For more information about topology maps, refer to "IP topology view manager" on page 306.

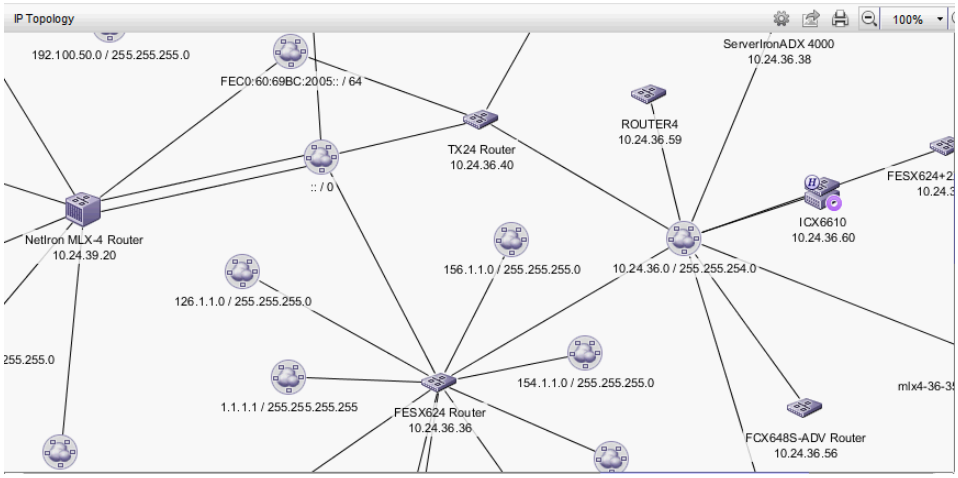


FIGURE 121 Topology Map

Topology Map functions

- Two-way selection — Select an icon on the topology map and that device is highlighted in the Product List and vice versa. For more information about icons, refer to "Icon legend" on page 290.
- Node/Device double-click — Double-click a node (subnet) to display the devices beneath it. Double-click a device to display the **Properties** dialog box for the selected device. For more information about device properties, refer to "IP device properties" on page 1314.
- User-defined properties — User-defined properties display in the Product List. For more information, refer to "Properties customization" on page 1329.
- Zoom In/Zoom Out — Click the appropriate button to zoom in or out on the topology map.

  On the L2, Ethernet Fabrics, IP, and VLAN topologies, click anywhere on the topology map and use the mouse wheel to zoom in and out.
- ToolTips — Pause on a node, device, or connection to view information. For more information about tooltip flyovers, refer to "Flyover settings" on page 140.
- Shortcut menus — Right-click a device in the Product List to view the menu. For a list of shortcut menus, refer to "IP shortcut menus" on page 1268.

Topology map keyboard shortcuts

For the L2, Ethernet Fabrics, IP, and VLAN topologies, you can use the keystrokes shown in the table below to perform common topology map functions.

TABLE 26 Topology keyboard shortcuts

Keyboard Shortcut	Description
Number Pad +	Zoom in on the topology.
Number Pad -	Zoom out on the topology.
Control + 0	Set the zoom level to 100%.
Control + P	Launch the **Print** dialog box.
Control + E	Launch the **Export** dialog box.

TABLE 26 Topology keyboard shortcuts

Keyboard Shortcut	Description
Control + ,	Launch the **Topology Display** dialog box.
Right Arrow	Move the selection to the node on the right (if available).
Left Arrow	Move the selection to the node on the left (if available).
Up Arrow	Move the selection to the node above the current selection (if available).
Down Arrow	Move the selection to the node that is below the current selection (if available).

Master Log

The Master Log, which displays in the lower area of the main window, lists the events and alerts that have occurred on the Network. If you do not see the Master Log, select **View > Show Panels > All Panels** or press **F5**.

The default order of the Master Log columns is 'Severity', 'Acknowledged', 'Last Event Server Time', and 'Description'. Which columns are displayed and in what order can be controlled through the "Customize Columns" dialog, as described in "Displaying columns" and in "Changing the order of columns". You can sort the Master Log by clicking a column heading. By default, the Master Log is sorted by the **Last Event Server Time** column. To filter information in the Master Log, refer to "Filtering events in the Master Log" on page 1210. To view event properties, refer to "Displaying event properties from the Master Log" on page 1207.

The following fields and columns are included in the Master Log:

- **Severity —** The severity of the event. When the same event (Warning or Error) occurs repeatedly, the Management application automatically eliminates the additional occurrences. For more information about events, refer to "Fault Management" on page 1141. For a list of the event icons, refer to "Event icons" on page 292.
- **Acknowledged —** Whether the event is acknowledged or not. Select the check box to acknowledge the event.
- **Source Name —** The product on which the event occurred.
- **Source Address —** The IP address (IPv4 or IPv6 format) of the product on which the event occurred.
- **Origin —** The event source type (for example trap, pseudo event, application, or syslog).
- **Category —** The type of event that occurred (for example, client/server communication events).
- **Description —** A description of the event.
- **Last Event Server Time —** The time and date the event last occurred on the server.
- **Count —** The number of times the event occurred.
- **Module Name —** The name of the module on which the event occurred.
- **Message ID —** The message ID of the event.
- **Product Address —** The IP address of the product on which the event originated.
- **Contributor —** The name of the contributor on which the event occurred.
- **Node WWN —** The world wide name of the node on which the event occurred.
- **Fabric Name —** The name of the fabric on which the event occurred.
- **Operational Status —** The operational status (such as, unknown, healthy, marginal, or down) of the product on which the event occurred.

- **First Event Product Time —** The time and date the event first occurred on the product.
- **Last Event Product Time —** The time and date the event last occurred on the product.
- **First Event Server Time —** The time and date the event first occurred on the server.
- **Audit —** The audit of the event.
- **Virtual Fabric ID —** The VFID of the product on which the event occurred.
- **Zone Alias** — Displays the zone alias of the product or port.

Minimap

The **Minimap**, which displays in the lower right corner of the main window, is useful for getting a bird's-eye view of the topology, or to quickly jump to a specific place on the topology. To jump to a specific location on the topology, click that area on the Minimap. A close-up view of the selected location displays on the topology.

Use the Minimap to view the entire topology and to navigate more detailed map views. This feature is especially useful if you have a large topology. Does not display until you discover a device.

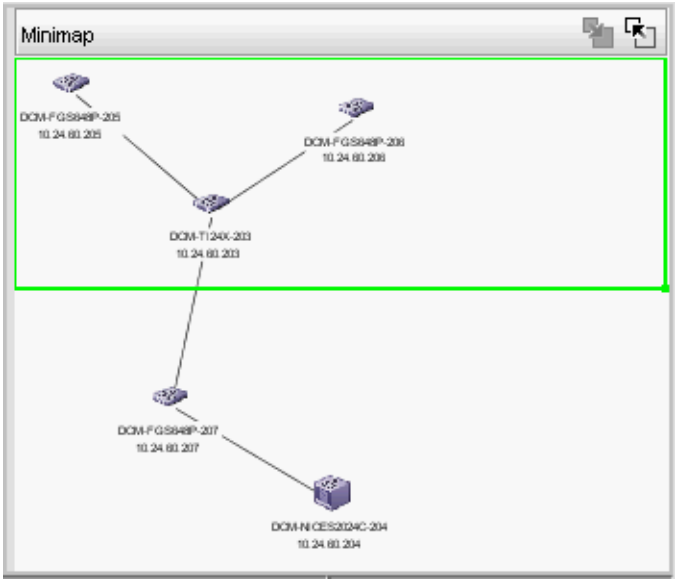


FIGURE 122 IP Minimap

Anchoring or floating the Minimap

You can anchor or float the Minimap to customize your main window.

- To float the Minimap and view it in a separate window, click the **Detach** icon ( ) in the upper right corner of the Minimap.
- To anchor the Minimap and return the Minimap to its original location on the main window, do one of the following steps:
  - Click the **Attach** icon ( ) in the upper right corner of the Minimap.
  - Click the **Close** icon ( ) in the upper right corner of the Minimap.
  - Double-click the logo in the upper left corner of the Minimap.
  - Click the logo in the upper left corner of the Minimap and select **Close** (**ALT** + **F4**).

Resizing the Minimap

On an anchored Minimap, place the cursor on the left border of the Minimap until a double-pointed arrow displays. Click and drag the adjoining divider.

On a floating Minimap, place the cursor on a border of the Minimap until a double-pointed arrow displays. Click and drag to change the window size.

Status bar

The status bar displays at the bottom of the main window. The status bar provides a variety of information about the SAN and the application. The icons on the status bar change to reflect different information, such as the current status of products, fabrics, and backup.

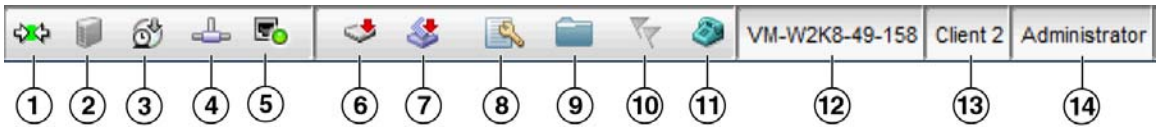


FIGURE 123 Status Bar

The icons on your status bar will vary based on the licensed features on your system.

1. **Connection Status —** Displays the Server-Client connection status. Also displays whether the client topology is in sync with the server. Resynchronize with the server by restarting the client.
2. **Server Status** — Displays the status of the server disk space (for example, low or sufficient).
3. **Server Backup Status —** Displays a backup status icon, which allows you to determine the current backup status. Right-click and select **Backup now** to begin back up immediately. Right-click and select **Configure backup** to launch the **Options** dialog box - **Server Backup** pane and configure backup. Let the pointer pause on the backup status icon to display the following information in a tooltip.
   - **Backup in Progress icon —** Backup started at hh:mm:ss, in progress... *XX* files in *Directory_Name* are backed up.
   - **Countdown to Next Scheduled Backup icon —** Waiting for next backup to start.
   - **Backup Disabled icon —** Backup is disabled.
   - **Backup Failed icon —** Backup failed at hh:mm:ss mm/dd/yyyy.
4. **Network Size Status —** Displays a memory allocation status icon, which allows you to determine the current network size status. Double-click the icon to launch the **Memory Allocation** pane of the **Options** dialog box. Let the pointer pause on the backup status icon to display the following information in a tooltip.
   - **Network size within limits icon —** Network size is within the recommended count.
   - **Ne work size exceeds limits icon —** Network size exceeds the recommended count.
5. **Server Port Status —** Displays port status for the following ports: CIM Indication for Event Handling, CIM Indication for HCM Proxy, FTP,SCP/SFTP, SNMP Trap, Syslog, , Web Server (HTTP), and Web Server (HTTPS). Click to launch the **Port Status** dialog box. For more information about port status, refer to "Viewing port status" on page 10.
6. **Product Status —** Displays the status of the most degraded device in the SAN. For example, if all devices are operational except one (which is degraded), the Product Status displays as degraded. Click this icon to open the **Product Status Log**.

7. **Fabric Status —** Displays the state of the fabric that is least operational, based on ISL status. The possible states are: operational, unknown, degraded or failed. Select a product or fabric from the Connectivity Map or Product List and click this icon to open the related **Fabric Log** (only available for persisted fabrics).
8. **Configuration Deviation Status** (IronWare and Network OS products only) — Displays whether or not product's have deviated from their baseline configuration. Click this icon to open the **Change Tracking** tab of the **Configuration Repository** dialog box.
9. **Policy Monitor Status —** Displays whether or not a policy monitor has failed or partially failed. Click to launch the **Policy Monitor** dialog box. For more information about policy monitors, refer to "Viewing policy monitor status" on page 1106.
10. **Special Events** — Displays whether or not a special event has been triggered. Click to launch the **Special Events** dialog box. For more information about special events, refer to "Creating an event action definition" on page 1166.
11. **Call-Home Status —** (Trial and Licensed version only) Displays a call home status icon when one or more product are discovered, which allows you to determine the current call home status. Click to launch the **Call Home Notification** dialog box. For more information about Call Home status and icons, refer to "Viewing Call Home status" on page 358.
12. **Server Name —** Displays the name of the Server to which you are connected. Click to launch the **Server Properties** dialog box. For more information, refer to "Viewing server properties" on page 9.
13. **Total Users —** Displays the number of clients logged into the server. Click to launch the **Active Sessions** dialog box. For more information, refer to "Viewing active sessions" on page 8.
14. **User's ID —** Displays the user ID of the logged in user. Click to launch the **User Profile** dialog box. For more information, refer to "User profiles" on page 205.
15. **Trial license** (Not shown) — Displays the trial expiration information to the right of the User's ID.

Icon legend

Various icons are used to illustrate devices and connections in a network. The following tables list icons that display on the Connectivity Map and Product List.

IP product icons

The following table lists the manageable IronWare and Network OS product icons that display on the topology. Manageable devices display with blue icons. Unmanageable devices display with gray icons. Some of the icons shown only display when certain features are licensed.

TABLE 27

Icon	Description	Icon	Description
	IP Fixed Configuration Switch		IP Stackable Switch
	IP Chassis		HyperEdge Stackable Switch

TABLE 27

Icon	Description	Icon	Description
	VLAN		Wireless Access Point
	Wireless Controller		VDX Switch (L2)
	VCS fabric		Unlicensed VCS fabric
	VDX Router (L3-enabled)		IP Subnet
	Layer 2 Cloud		Unmanaged Product
			Third-Party Product

Host product icons

The following table lists the manageable Host product icons that display on the topology. Fabric OS manageable devices display with blue icons. Unmanageable devices display with gray icons. Some of the icons shown only display when certain features are licensed.

TABLE 28

Icon	Description	Icon	Description
	HBA		HBA Mezzanine Card
	CNA		CNA Mezzanine Card
	Unmanaged HBA		Any IO
	Host		Unmanaged Host
	VM Host		Virtual HBA
	Ethernet Cloud		Layer 2 Cloud

IP group icons

The following table lists the manageable IP product group icons that display on the topology.

TABLE 29

Icon	Description	Icon	Description
	Switch Group, Product Group		

IP port icons

The following table lists the port icons that display in the Product List.

TABLE 30

Icon	Description
	IP Port
	Virtual IP Port
	IP Port Group

IP product status icons

The following table lists the product status icons that display on the topology.

TABLE 31

Icon	Status
No icon	Reachable
	Degraded/Marginal
	Down/Failed
	Degraded Link
	Not Reachable
	Unknown/Link Down
	Unhealthy

Event icons

The following table lists the event icons that display on the topology and Master Log. For more information about events, refer to .

TABLE 32

Event Icon	Description
	Emergency
	Alert
	Critical
	Error
	Warning
	Notice
	Informational
	Debug

Customizing the main window

You can customize the main window to display only the data you need by displaying different levels of detail on the Connectivity Map (topology) or Product List.

Zooming in and out of the Connectivity Map

You can zoom in or out of the Connectivity Map to see products and ports.

Zooming in

To zoom in on the Connectivity Map, use one of the following methods:

- Click the zoom-in icon ( ) on the Connectivity Map toolbar.
- Press CTRL and the plus sign on the number pad on the keyboard.

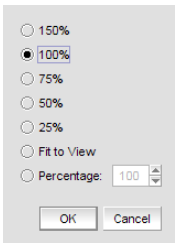


FIGURE 124 Zoom dialog box

Zooming out

To zoom out of the Connectivity Map, use one of the following methods:

- Click the zoom-out icon ( ) on the Connectivity Map toolbar.
- Press CTRL and the minus sign on the number pad on the keyboard.

Exporting the topology

You can save the topology to an image (PNG format).

1. Click **Export** in the toolbar.

   The **Export Topology To PNG File** dialog box displays.

2. Browse to the directory where you want to export the image.
3. Edit the name in the **File Name** field, if necessary.
4. Click **Save**.

   If the file name is a duplicate, a message displays. Click **Yes** to replace the image or click **No** to go back to the **Export Topology To PNG File** dialog box and change the file name.

   The **File Download** dialog box displays.

5. Click **Open** to view the image or click **Cancel** to close the dialog box.

Customizing application tables

You can customize any table in the Management application main interface (for example, the Master Log or the Product List) or in individual dialog boxes in the following ways:

- Display only specific columns
- Display columns in a specific order
- Resize the columns to fit the contents
- Sort the table by a specific column or multiple columns
- Copy information from the table to another application
- Export information from the table
- Search for information
- Expand the table to view all information
- Collapse the table

Displaying columns

To only display specific columns, complete the following steps.

1. Right-click anywhere in the table and select **Customize** or **Table > Customize**.

   The **Customize Columns** dialog box displays.

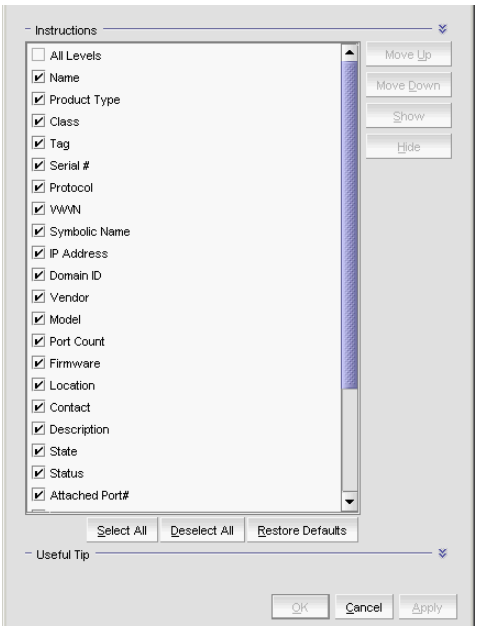


FIGURE 125 Customize Columns dialog box

2. Choose from the following options:
   - Select the check box to display a column.
     OR
     Select the column name and click **Show**.
   - Clear the check box to hide a column.
     OR
     Select the column name and click **Hide**.
   - Click **Select All** to select all check boxes.
   - Click **Deselect All** to clear all check boxes.
   - Click **Restore Defaults** to restore the table to the original settings.
3. Click **OK**.

Changing the order of columns

To change the order in which columns display, choose from one of the following options.

Rearrange columns in a table by dragging and dropping the column to a new location.

OR

1. Right-click anywhere in the table and select **Customize** or **Table > Customize**.

   The **Customize Columns** dialog box displays.
2. Select the name of the column you want to move and use the **Move Up** button and **Move Down** button to move it to a new location.
3. Click **OK**.

Resizing the columns

You can resize a single column or all columns in the table.

To resize a single column, right-click the column header and select **Size Column to Fit** or **Table > Size Column to Fit**.

To resize all columns in the table, right-click anywhere in the table and select **Size All Columns to Fit** or **Table > Size All Columns to Fit**.

Sorting table information

To sort the table by a single column, click the column header.

To reverse the sort order, click the column header again.

To sort the table by multiple columns, complete the following steps.

1. Click the primary column header.
2. Press CTRL and click a secondary column header.

Copying table information

You can copy the entire table or a specific row to another application (such as Notepad, Excel, Word, and so on).

1. Choose from one of the following options:
   - Right-click anywhere in the table and select **Table > Copy Table**.
   - Select the table row that you want to export and select **Table > Copy Row.**
2. Open the application to which you want to copy the Product List information.
3. Select **Edit > Paste** (or press CTRL + V).
4. Save the file.

Exporting table information

You can export the entire table or a specific row to a text file.

1. Choose from one of the following options:
   - Right-click anywhere in the table and select **Table > Export Table**.
   - Select the table row that you want to export and select **Table > Export Row.**

   The **Save table to a tab delimited file** dialog box displays.
2. Browse to the location where you want to save the file.
3. Enter the file name in the **File Name** field.
4. Click **Save**.

Searching for information in a table

You can search for information in the table by any of the values found in the table.

1. Right-click anywhere in the table and select **Table > Search**.

   The focus moves to the Search field.

FIGURE 126 Search field

2. Enter all or part of the search text in the Search field and press **Enter**.

   The first instance is highlighted in the table.

3. Press **Enter** to go to the next instance of the search text.

Expanding and collapsing tables

You can expand a table to display all information or collapse it to show only the top level.

To expand the entire table, right-click anywhere in the table and select **Expand All** or **Table > Expand All**.

To collapse the entire table, right-click anywhere in the table and select **Collapse All** or **Table > Collapse All**.

Product List customization

NOTE
Properties customization requires read and write permissions to the Properties - Add / Delete Columns privilege.

You can customize the Product List by creating user-defined product and port property labels. You can also edit or delete user-defined property labels, as needed.

You can create up to three user-defined property labels from the Product List for each of the following object types: product and port properties. Product property labels created from the Product List display in the Product List and the **Properties** dialog box. You can create port property labels from the Product List; however, you can only view them on the **Ports** tab of the **Properties** dialog box. User-defined properties must be unique across all **Properties** dialog boxes and the Product List.

You cannot edit the user-defined property field contents from the Product List; however, you can edit the field in the **Properties** dialog box.

Property fields containing a green triangle ( ) in the lower right corner are editable. To edit a field with a green triangle ( ), click in the field and make your changes.

Adding a property label

You can create up to three user-defined product and port property labels from the Product List. To add a new property label (column heading), complete the following steps.

1. Right-click any column heading on the Product List and select **Add Column**.

   The **Add Property** dialog box displays.

2. Enter a label and description for the property.

   The label must be unique and can be up to 30 characters.

   The description can be up to 126 characters.

3. Select the property type from the **Type** list.

   Options include: Product or Port.

4. Click **OK**.

   The new property displays in the last column of the Product List as well as the associated Properties dialog box based on the selected type.

   You cannot edit the user-defined property field contents from the Product List; however, you can edit the field in the **Properties** dialog box.

   Property fields containing a green triangle ( ) in the lower right corner are editable. To edit a field with a green triangle ( ), click in the field and make your changes.

Editing a property label

You can only edit labels that you create on the Product List.

To edit a user-defined property label (column heading), complete the following steps.

1. Right-click the column heading on the Product List for the property you want to edit and select **Edit Column**.

   The **Edit Property** dialog box displays.

2. Change the label and description for the property, as needed.

   The label must be unique and can be up to 30 characters.

   The description can be up to 126 characters.

   You cannot change the property type.

3. Click **OK**.

   The property details are updated in the Product List as well as the Properties dialog box.

   You cannot edit the user-defined property field contents from the Product List; however, you can edit the field in the **Properties** dialog box.

   Property fields containing a green triangle ( ) in the lower right corner are editable. To edit a field with a green triangle ( ), click in the field and make your changes.

Deleting a property label

You can only delete labels that you created on the Product List. To delete a label, complete the following steps.

1. Right-click the user-defined column heading on the Product List you want to delete and select **Delete Column**.

2. Click **Yes** on the confirmation message.

The column you selected is deleted from the Product List as well as the Properties dialog box.

Search

You can search for a objects by text or regular expression.

- **Text** — Enter a text string in the search text box. This search is case sensitive.

  For example, if you are searching for a device in the Product List, you can enter the first five characters in a device name. All products in the Product List that contain the search text display highlighted.

- **Regular Expression** — Enter a Unicode regular expression in the search text box. (For hints, refer to "Regular Expressions" on page 1333.) All products in the Product List that contain the search text display highlighted. This search is case insensitive.

  For example, you might need to search ports. To search for a port using a Unicode regular expressions, enter "2/1|2/2|2/3". This search will find Ports 2/1, 2/2, and 2/3 on all devices.

The Search features contains a number of components. The following graphic illustrates the various areas, and descriptions of them are listed below.

1. Text field — Enter the text or unicode regular expression for which you want to search.
2. Search list — Select one of the following options:
   - **Text** option — Select this option if you entered a text string in the text field.
   - **Regular Expression** option — Select this option if you entered a unicode regular expression in the text field.
   - **Clear Search** command — Select this option to clear the search text field
   - **Help** command — Select this option to view help for this feature.
3. Search up button — Click to search upward in the list.
4. Search down button — Click to search downward in the list.

Searching for a device

You can search for a device by name, WWN, or device type. When searching in the Connectivity Map, make sure you search the right view (**View > Manage View > Display View >** *View_Name*) with the appropriate options of port display (**View > Port Display >** *Display_Option*) and connected end devices (**View > Port Display > Show All**) enabled.

To search for a device, complete the following steps.

1. Enter your search criteria in the search field.

NOTE
To search for a device, the device must be discovered and display in the topology.

2. Choose one of the following options:
   - Select **Text** from the search list and enter a text string in the search text box.

     This search is case sensitive.
   - Select **Regular Expression** from the search list and enter a Unicode regular expression in the search text box.

     This search is case insensitive
3. Press **Enter** or click the search icon.

   The search results display highlighted.

   If the search finds more than one match, a message displays, advising you to restrict the search by restricting the search by node (refer to "Restricting a search by node" on page 300) or by looking for exact matches (refer to "Searching for an exact match" on page 301).

Restricting a search by node

When a device is assigned to a product group, it may be listed in the Product node, as well as Product Groups node. Therefore the search results include the device under both the Product node and the Product Group node.

NOTE
To search for a device, the device must be discovered and display in the topology.

To restrict the search only to specific nodes, complete the following steps.

1. Select the Product node or Product Group node that you want to search.
2. Choose one of the following options:
   - Select **Text** from the search list.
   - Select **Regular Expression** from the search list.
3. Enter your search criteria in the search field.
   - **Text** — Enter a text string in the search text box. This search is case sensitive.

     For example, you can enter the first five characters in a device name. All products in the Product List that contain the search text display highlighted.
   - **Regular Expression** — Enter a Unicode regular expression in the search text box. (For hints, refer to "Regular Expressions" on page 1333.) All products in the Product List that contain the search text display highlighted. This search is case insensitive.
4. Press **Enter** or click the search icon.

   The search results display highlighted.

Searching for an exact match

To search for an exact match, complete the following steps.

1. Choose one of the following options:
   - Select **Text** from the search list.
   - Select **Regular Expression** from the search list.
2. Enter your search criteria in the search field.
   - **Text** — Enter a text string in the search text box. This search is case sensitive.

     For example, you can enter the first five characters in a device name. All products in the Product List that contain the search text display highlighted.
   - **Regular Expression** — Enter a Unicode regular expression in the search text box. (For hints, refer to "Regular Expressions" on page 1333.) All products in the Product List that contain the search text display highlighted. This search is case insensitive.
3. Press **Ctrl** and click the search icon.

   The search results display highlighted.

   Example

   If you search for IP address "192.1.1.101" and then press CTRL and click the search icon, the application only highlights "192.1.1.101". This search does not highlight "SI-101 [192.1.1.101]".

   If you search for port "1/2" and then press CTRL and click the search icon, the application only highlights port "1/2". This search does not highlight ports "1/2", "1/20", "1/21", "1/22", and so forth.

Clearing search results

To clear search results, select **Clear Search** from the search list.

Address Finder

NOTE
Address Finder is not supported on Fabric OS products.

NOTE
Address Finder is only supported on Network OS products running 3.0 or later.

Address Finder locates where hosts are connected to your network from traffic on the network. The list of interfaces provides information on the location of the source of the address, relative to each network device, although the source may be directly or indirectly connected to the listed interfaces.

Address Finder uses the network topology information recorded during the discovery process based on information from devices running Foundry Discovery Protocol (FDP) and Link Layer Discovery Protocol (LLDP) and from the topology_data.txt file.

If a workstation is connected to a third-party device, and that device is connected to a IronWare or Network OS device, then Address Finder should be able to report the downstream port from which that traffic is coming (that is, the port to which the third-party device is connected), as long as the workstation is sending traffic that passes through the IronWare or Network OS device.

This directional information indicates which device interface can be used to reach the target MAC address. By combining this information with the knowledge of the network topology, you can trace a path from a device to the wireless client in question.

Address Finder finds MAC addresses that are in the forwarding tables at the moment when the search is performed.

You can use Address Finder if you have the Address Finder privilege in your user account or role. For more information about privileges, refer to "User Privileges" on page 1283.

Finding IP addresses

NOTE
Address Finder is only supported on Network OS products running 3.0 or later.

When searching for an IP address, Address Finder sends a couple of packets to the target IP address to prime Address Resolution Protocol (ARP) caches. It then looks in the Management application database to find all the Layer 3 devices on the target subnet, and then queries the ARP table of each one to find the target IP address. The result of the query provides the corresponding MAC address. Once the MAC address is known, then the MAC address is searched for in the learned MAC address tables of each device that is in the database that has an IP address on the same subnet as the target IP address. To find a MAC address, refer to "Finding MAC addresses" on page 304.

To find an IP address, complete the following steps.

1. Click the **IP** tab.
2. Select **Tools > Address Finder**.

   The **Address Finder** dialog box displays.

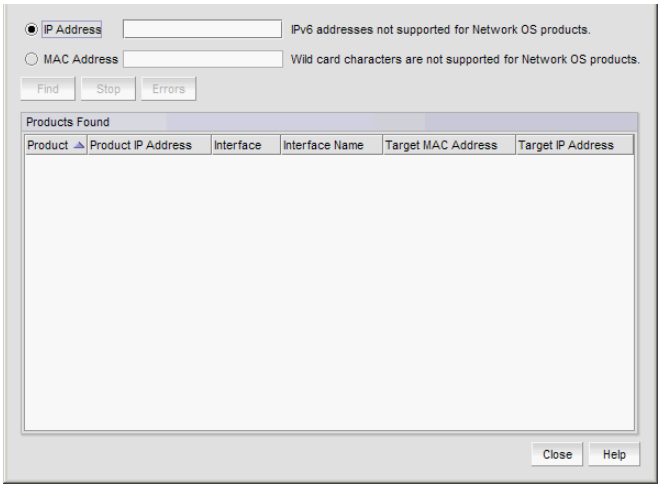


FIGURE 127 Address Finder dialog box

3. Select the **IP Address** option and enter the IP address (IPv4 or IPv6 format) that you want to find.

NOTE
IPv6 address search is only supported on Ethernet router products running IronWare OS 5.4 or later.

NOTE
IPv6 address search is not supported on Network OS products.

4. Select the **Find only in the selected products** check box to limit the search to selected products.

   When you access Address Finder from the Element Manager interface (refer to "Element Manager interface overview" on page 725), the **Find only in the selected products** check box is selected by default to limit the search to the selected Ethernet router device.

5. Select the product you want to include in the search in the **Available Products** list.
6. Click the right arrow button to move the selected products to the **Selected Products** list.
7. Click **Find** to begin the search.

   If the search is successful, the products display in the **Products Found** table as they are found. Note that products may not display immediately.

   Click **Stop** to stop the search.

   The table shows the following information:

   - **Product** — The product icon and host name of the device that has seen or learned the IP addresses for which you searched, or the host name of the device where the IP address belongs to the network device.
   - **Product IP Address** — The IP address of the device that has seen or learned the target IP address.
   - **Interface** — The interface that has seen or learned the MAC address.
   - **Interface Name** — The administratively configured name of the interface.
   - **VLAN Name** — The VLAN ID of the interface.
   - **Target MAC Address** — The MAC address you wanted to find.
   - **Target IP Address** — The IP address you wanted to find.

   Sort the search results by clicking the column header. Click the same column header again to reverse the sort order.

NOTE
Address Finder cannot detect IP addresses assigned to POS or ATM ports. However, Address Finder will find IP addresses across a POS or ATM port.

   You can sort the search results by a specific column by clicking the column header. Click the same column header again to reverse the sort order.

   If errors occur during the search, the **Errors** button becomes enabled. Click **Errors** to display the error messages. Error messages are grouped by the error description (Reason). You may need to scroll down to read the entire error message. Click **OK** when you have finished reading the message. Make any necessary corrections in the network before repeating the search.

8. Click **Port Properties** to launch the **Port Properties** dialog box for the device.

9. Click **Attached Port Properties** to launch the **Port Properties** dialog box for the device.

NOTE
The **Attached Port Properties** button is only supported for Network OS devices.

The **Ports** tab of the **VCS Properties** dialog box displays with the attached ports highlighted.

10. Click **Close** to close the **Address Finder** dialog box.

Finding MAC addresses

NOTE
MAC address search is supported on Network OS products running 2.1.0 or later.

To find a MAC address, Address Finder searches the learned MAC address tables of each device that is in the database. To find a IP address, refer to "Finding IP addresses" on page 302.

To find a MAC address, complete the following steps.

1. Click the **IP** tab.
2. Select **Tools > Address Finder**.

   The **Address Finder** dialog box displays.

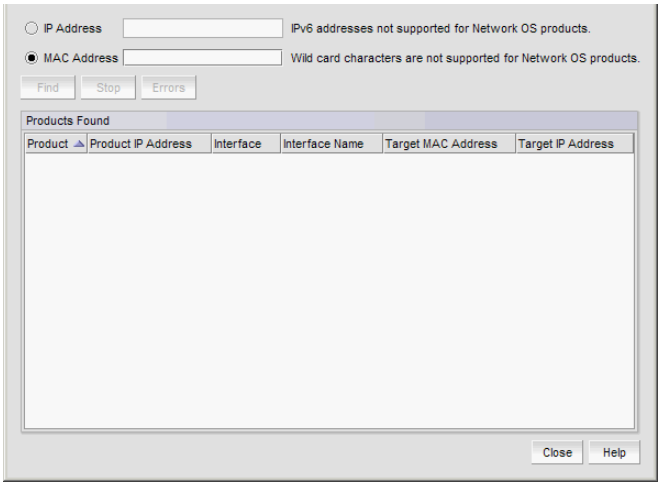


FIGURE 128 Address Finder dialog box

3. Select the **MAC Address** option and enter the address in hexadecimal characters in the field.

   You can use any of the following methods to separate the characters in the address:

   - Hyphens (for example: aa-bb-cc-dd-ee-ff)
   - Periods (for example: aa.bb.cc.dd.ee.ff)
   - Colons (for example: aa:bb:cc:dd:ee:ff)
   - Spaces (for example: aa bb cc dd ee ff)
   - No spaces (for example: aabbccddeeff)

   To find more than one address, use question marks as wildcard characters (for example: aa-bb-cc-dd-??-??).

NOTE
Wildcard character search is not supported on Network OS products.

4. Select the **Find only in the selected products** check box to limit the search to selected products.

   When you access Address Finder from the Element Manager interface (refer to "Element Manager interface overview" on page 725), the **Find only in the selected products** check box is selected by default to limit the search to the selected Ethernet router device.

5. Select the product you want to include in the search in the **Available Products** list.
6. Click the right arrow button to move the selected products to the **Selected Products** list.
7. Click **Find** to begin the search.

   If the search is successful, the products display in the **Products Found** table as they are found. Note that products may not display immediately.

NOTE
When Address Finder searches for the Target MAC address and no topology information exists (for example, FDP & LLDP is disabled on the router and switch), two entries display – one from the router and one from the switch.

NOTE
When you find targets using the MAC address wildcard, the **Products Found** table shows the IP addresses of hosts connected to the routers. IP addresses of hosts connected to L2 switches are blank because Layer 2 switches typically do not learn the IP addresses of end nodes attached to the Layer 2 switch as it is not in the ARP table of the switch.

NOTE
You cannot use special addresses (such as a broadcast MAC address (FFFF.FFFF.FFFF) or any MAC in multicast range (0100.5E00.0000 – 0100.5E7F.FFFF) to find products.

Click **Stop** to stop the search.

The table shows the following information:

- **Product** — The product icon and host name of the device that has seen or learned the MAC addresses for which you searched, or the host name of the device where the MAC address belongs to the network device.
- **Product IP Address** — The IP address of the device that has seen or learned the target IP address.
- **Interface** — The interface that has seen or learned the MAC address.
- **Interface Name** — The administratively configured name of the interface.
- **VLAN** — The VLAN ID of the interface.
- **Target MAC Address** — The MAC address you wanted to find. This field standardizes the MAC address format as follows: aa.bb.cc.dd.ee.ff.
- **Target IP Address** — The IP address you wanted to find.

You can sort the search results by a specific column by clicking the column header. Click the same column header again to reverse the sort order.

If errors occur during the search, the **Errors** button becomes enabled. Click **Errors** to display the error messages. Error messages are grouped by the error description (Reason). You may need to scroll down to read the entire error message. Click **OK** when you have finished reading the message. Make any necessary corrections in the network before repeating the search.

8. Click **Port Properties** to launch the **Port Properties** dialog box for the device.
9. Click **Attached Port Properties** to launch the **Port Properties** dialog box for the device.

NOTE
The **Attached Port Properties** button is only supported for Network OS devices.

The **Ports** tab of the **VCS Properties** dialog box displays with the attached ports highlighted.

10. Click **Close** to close the **Address Finder** dialog box.

IP topology view manager

The topology view manager enables you to choose how to view devices in your network. Topology views only contain devices included in your area of responsibility (AOR).

To display topology views in the Management application, make sure you meet the following requirements.

- Make sure that all IronWare OS or Network OS devices on the network have the Foundry Discovery Protocol (FDP) or Link Layer Discovery Protocol (LLDP) enabled so that connections between devices display. To enable FDP or LLDP using the Configuration Wizard, refer to "IP Configuration Wizard" on page 765.

NOTE
FDP is not supported in an IPv6 network; therefore, you must enable LLDP on the devices to displays link in a L2 topology.

- Make sure that all non-IronWare OS or Network OS devices have LLDP or the Cisco Discovery Protocol (CDP) enabled so that connections between devices display.
- Make sure all devices display under the Network Object tree. If they do not display, you should run discovery or add the devices manually in the **Discover Setup IP** dialog box.
- Make sure you have the appropriate privilege (IP - Main Display - Ethernet Fabric, IP - Main Display - IP, IP - Main Display - L2, IP - Main Display - MRP, or IP - Main Display - VLAN) for the topology map you want to view. For more information about privileges, refer to "User Privileges" on page 1283.

Displaying topology views

To display a topology view, select the one of the following view types from the view list on the Product List toolbar:

- Network Objects — For more information, refer to "Network Objects view" on page 307.
- IP Topology — For more information, refer to "IP Topology view" on page 309.
- L2 Topology — For more information, refer to "L2 Topology view" on page 309.
- Ethernet Fabrics — For more information, refer to "Ethernet Fabrics view" on page 310.

- VLAN Topology — For more information, refer to "VLAN Topology view" on page 310.
- Host Topology — For more information, refer to "Host Topology view" on page 313.

Network Objects view

The Network Objects view displays a list of discovered products in a table (Product List). This view allows you to manage user authentications and permissions on discovered devices. In addition, you can place devices into management groups, which are used for configuration, deployment, accounting, monitoring, and reporting processes.

The following columns (presented here in alphabetical order) are included in the Product List:

- **Build Label.** Select to display the firmware build number.
- **Contact.** Select to display the name of the person or group you should contact about the product. This field is editable at the fabric level.
- **Description.** Select to display the description of the product. This field is editable at the fabric level.
- **Product Type.** Select to display the type of product.
- **Firmware.** Select to display the firmware version of the product.
- **Group/Product.** Select to display discovered products, product groups, and port groups.
- **IP Address.** Select to display the IP address (IPv4 or IPv6 format) of the product.
- **Location.** Select to display the physical location of the product. This field is editable at the fabric level.
- **Model.** Select to display the model number of the product.
- **Name.** Select to display the name of the product. This field is editable at the fabric, device, and port levels.
- **Port Count.** Select to display the number of ports on the product.
- **Serial #.** Select to display the serial number of the product.
- **Status.** Select to display the status for the product and the port.
- **Vendor.** Select to display the name of the product's vendor.
- User-defined property labels — Displays the user-defined property labels. You can create up to three user-defined property labels.

Network Object view functions

- Sort — Click a column head to sort the list. Click a column head again to reverse the sort orders.
- Node/Device double-click — Double-click a node (subnet) to display the devices beneath it. Double-click a device to display the **Properties** dialog box for the selected device. For more information, refer to "IP device properties" on page 1314.
- User-defined properties — User-defined properties display in the Product List. For more information, refer to "Properties customization" on page 1329.
- Shortcut menus — Right-click a device in the Product List to view the menu. For a list of shortcut menus, refer to "IP shortcut menus" on page 1268.

Filtering devices in the Network Objects Product List

To filter specific devices from the Network Objects Product List, complete the following steps.

1. Select **Network Objects** from the view list on the Product List toolbar.
2. Click **Filter**.

   The **Product Filter** dialog box displays. Only the categories or objects listed under the **Selected Categories** list display on the Network Objects Product List. Available categories include:

   - **Contact** — Lists the contact name for the discovered products.
   - **Firmware** — Lists the firmware on the discovered products.
   - **Location** — Lists the location of the discovered products.
   - **Model** — Lists the models of the discovered products.
   - **Product Type** — Lists the types of discovered products.
3. Select the **Enable filter** check box.
4. Filter the Product List by product status by selecting one or more of the following check boxes:

   - Reachable
   - Degraded Link
   - Not Reachable
   - Unhealthy
   - Healthy
   - Marginal
   - Down

   By default, all product status types are included. Clear the check mark from each status type you do not want to include in the filter.
5. Add a category or object within the category to the filter by selecting the category or object in the **Available Categories** list and clicking the right arrow button.
6. Remove a category or object from the filter by selecting the category or object in the **Selected Categories** list and clicking the left arrow button.
7. Click **OK**.

   The updated Product List contains only the selected categories and objects. The **Filter** check box displays with a check mark.

Clearing the Network Objects Product List filter

To clear the filter and display all discovered devices in the Network Objects Product List, clear the **Filter** check box.

The updated Product List contains only all discovered devices as well as all product groups and port groups.

IP Topology view

The IP Topology view displays a map of the devices on your network. To display the topology map for IP, you must have the IP - Main Display - IP privilege. For more information about privileges, refer to "User Privileges" on page 1283.

For more information about the components and customization of the topology map, refer to the following sections:

- "IP topology map components" on page 315.
- "Topology map elements" on page 315.
- "Topology map layout" on page 317.

For more information about functions you can perform on the topology map, refer to "Topology Map functions" on page 286.

L2 Topology view

The L2 Topology view displays a map of the Layer 2 traffic for devices on your network. The links on the map show physical links between physical ports of devices. If devices have more than one physical link between them, all physical links display on the topology map. To display the topology map for Layer 2, you must have the IP - Main Display - L2 privilege. For more information about privileges, refer to "User Privileges" on page 1283.

The L2 Topology view Product List has two categories, System Groups and User-defined Groups. System Groups has only All IP Products as a category, which contains all IP products in the system. User-defined Groups contain all user-defined product groups with **Topology Display** enabled. Each user-defined product group shows the products contained within that product group.

For more information about the components and customization of the topology map, refer to the following sections:

- "IP topology map components" on page 315.
- "Topology map elements" on page 315.
- "Topology map layout" on page 317.

For more information about functions you can perform on the topology map, refer to "Topology Map functions" on page 286.

Ethernet Fabrics view

The Ethernet Fabrics view displays a map of the traffic for VCS devices on your network. To view the fabric members and TRILL (Transparent Interconnection of Lots of Links) connections for a fabric, double-click the fabric in the Product List. To display the topology map for Ethernet Fabrics, you must have the Main Display - Ethernet Fabric privilege. For more information about privileges, refer to "User Privileges" on page 1283.

The Ethernet Fabrics view Product List contains all the VCS fabrics known to the system. Within each VCS fabric, nodes that are part of that VCS fabric display. You can only view one VCS fabric at a time.

For more information about the components and customization of the topology map, refer to the following sections:

- "IP topology map components" on page 315.
- "Topology map elements" on page 315.
- "Topology map layout" on page 317.

For more information about general functions you can perform on the topology map, refer to "Topology Map functions" on page 286.

VLAN Topology view

The VLAN Topology view displays a map of the VLAN traffic for devices on your network. You can also view primary, isolated, and community PVLAN in the VLAN Topology and Product List. You can access the STP or RSTP Topology from this view. To display topologies for VLANs, you must have the Main Display - VLAN privilege in your user role. For more information about privileges, refer to "User Privileges" on page 1283.

The VLAN Product List contains all the port VLANs and PVLANs known to the system. Within each VLAN, products that are a part of that VLAN display. You can select which VLAN topology you wish to view. The default VLAN ID is the first entry in the VLAN Product List.

For more information about the components and customization of the topology map, refer to the following sections:

- "IP topology map components" on page 315.
- "Topology map elements" on page 315.
- "Viewing STP/RSTP topology" on page 311.
- "Topology map layout" on page 317.

For more information about functions you can perform on the topology map, refer to "Topology Map functions" on page 286.

STP/RSTP topology

You can display topology maps for STP or RSTP configurations from the VLAN Topology view. Before you display the STP or RSTP topology, make sure you meet the following requirements:

- The devices are running FDP or LLDP.

  If you do not enable FDP or LLDP on a product, the product displays without any links.

- The snIfStpTable MIB table (OID.1.3.6.1.4.1.1991.1.1.3.5.2) is enabled on the device and has either STP or RSTP configured. This MIB is not supported on third-party products.

Viewing STP/RSTP topology

To view this topology map, complete the following steps.

1. Select **VLAN Topology** from the view list on the Product List toolbar.

   Pause on the **STP** button. A tool tip appears, indicating whether STP is on or off.

2. If STP is off, click **STP** to turn it on.

3. Select a VLAN or PVLAN from the **VLAN Product List**.

   All devices with STP mode on the selected VLAN display on the map, regardless of their connectivity. STP-enabled devices display with a Bridge ID.

   The STP Topology view supports both STP and RSTP; however, the map does not differentiate between the two protocols. You can use the STP/RSTP report to determine which protocol is enabled on a device. MSTP protocol is not supported.

   When STP mode is active, dynamic updates is not active. Instead, a **Refresh** button displays on the Topology Map toolbar, next to the **STP** button, to enable you to manually trigger an update.

   Table 33 displays the elements of the STP Topology map.

TABLE 33 STP/RSTP Topology map elements

Element	Description
Device name IP address Bridge ID	Each device on the map displays its device name, IP address and bridge ID.
[Root]	The root bridge.
 solid line	The bridges on the topology in normal operating state.
 link with arrow head	The port is in a forwarding state and has the root port role.
 link with block	The port is in a blocking state or discarding.
 link with diamond	The port is in a disabled state.

TABLE 33 STP/RSTP Topology map elements

Element	Description
# (U) # (T) # (D)	The port or interface number used to create the link and one of the following: • (U) — Untagged port • (T) — Tagged port • (D) — Dual-mode port
tool tips	Link tool tips — identifies the devices at each end of the link to help you locate the devices on the map. Node tool tips — identifies the device name, IP address, and bridge ID of the node. If the node is a root bridge, [Root] appears in the tool tip.

Generating an STP/RSTP Report

If STP is enabled on the VLAN Topology, you can generate an STP/RSTP report for a device.

To generate an STP/RSTP report, complete the following steps.

1. Select **VLAN Topology** from the view list on the Product List toolbar.

   Mouse over the STP button. A tool tip appears, indicating whether STP is on or off.

2. If STP is off, click **STP** to turn it on.
3. Select a VLAN or PVLAN from the VLAN Product List.
4. Right-click a device on the topology map and select STP Report from the list.

   The STP/RSTP Report displays. The report is divided into two areas. The top area shows STP information that applies globally to the device. It indicates the STP Mode (802.1x for STP or 802.1w for RSTP) and the values of the global parameters. The second area displays STP or RSTP configuration for each device port.

Exporting an STP/RSTP Report

To export an STP/RSTP report, complete the following steps.

1. Select **VLAN Topology** from the view list on the Product List toolbar.

   Mouse over the STP button. A tool tip appears, indicating whether STP is on or off.

2. If STP is off, click **STP** to turn it on.
3. Select a VLAN or PVLAN from the VLAN Product List.
4. Right-click a device on the topology map and select STP Report from the list.

   The STP/RSTP Report displays.

5. Click **Export**.

   The **File Download** dialog box displays.

6. Click **Save.**

   The **Save As** dialog box displays.

7. Browse to the location where you want to save the report.
8. Enter a name for the report in the **File Name** field.

9. Click **Save**.

E-mailing an STP/RSTP Report

To export an STP/RSTP report, complete the following steps.

1. Select **VLAN Topology** from the view list on the Product List toolbar.

   Mouse over the STP button. A tool tip appears, indicating whether STP is on or off.
2. If STP is off, click **STP** to turn it on.
3. Select a VLAN or PVLAN from the VLAN Product List.
4. Right-click a device on the topology map and select STP Report from the list.

   The STP/RSTP Report displays.
5. Click **E-mail**.
6. Enter one or more e-mail addresses in the **E-mail Recipients** or **Other Recipients** fields.
7. Edit the Subject field, if necessary.
8. Enter a message in the Body text box.
9. Click **Send**.

Host Topology view

The Host Topology view displays a list of discovered hosts in a table (Product List). This view allows you to manage user authentications and permissions on discovered devices.

The following columns (presented here in alphabetical order) are included in the Product List:

- **Additional Port Info.** Displays additional port information.
- **All Levels.** Displays all discovered fabrics, groups, devices, and ports as both text and icons. Also, displays the status of the fabrics, groups, devices, and ports. For a list of icons that display in the **All Levels** column, refer to the following tables:
  - "Host product icons" on page 291
  - "IP product icons" on page 290
  - "IP port icons" on page 292
- **Additional Port Info.** Displays additional information about the port.
- **Attached Port #.** Displays the number of the attached port.
- **BB Credit.** Displays the BB Credit of the port.
- **Class.** Displays the class value of the FICON device port.
- **Contact.** Displays the name of the person or group you should contact about the product. This field is editable at the fabric level.
- **Description.** Displays the description of the product. This field is editable at the fabric level.
- **Domain ID.** Displays the Domain ID for the product in the format xx(yy), where xx is the normalized value and yy is the actual value on the wire.
- **FC Address.** Displays the Fibre Channel address of the port.
- **Firmware.** Displays the firmware version of the product.

- **IP Address.** Displays the IP address (IPv4 or IPv6 format) of the product.
- **Location.** Displays the physical location of the product. This field is editable at the fabric level.
- **Model.** Displays the model number of the product.
- **Name.** Displays the name of the product. This field is editable at the fabric, device, and port level.
- **Port #.** Displays the number of the port.
- **Port Count.** Displays the number of ports on the product.
- **Port Type.** Displays the type of port (for example, expansion port, node port, or NL_port).
- **Product Type.** Displays the type of product.
- **Protocol.** Displays the protocol for the port.
- **Serial #.** Displays the serial number of the product.
- **Speed Configured (Gbps).** Displays the actual speed of the port in Gigabits per second.
- **State.** Displays the state for the product and the port.
- **Status.** Displays the status for the product and the port.
- **Symbolic Name.** Displays the symbolic name for the port.
- **TAG.** Displays the tag number of the product.
- **Vendor.** Displays the name of the product's vendor.
- **WWN.** Displays the world wide name of the product or port.
- **Zone Alias**. Displays the zone alias of the product or port.
- User-defined property labels — Displays the user-defined property labels. You can create up to three user-defined property labels.

For more information about the components and customization of the topology map, refer to the following sections:

- "IP topology map components" on page 315.
- "Topology map elements" on page 315.
- "Topology map layout" on page 317.

For more information about functions you can perform on the topology map, refer to "Topology Map functions" on page 286.

IP topology map components

Topology maps are divided into three sections:

- Product List — The top left pane displays a list of all devices (topology tree) in your AOR. Devices display in topology groups. The Management application has a Search tool that you can use to find a device quickly. (Refer to "Using the Search tool" on page 53 for more information.)

  For more information about the Product List and functions you can perform on the Product List, refer to "IP Product List" on page 284.

- Topology Map — The top right pane displays the devices using graphic elements (icons). Automatically displays links between devices running FDP or LLDP on the topology maps.

  For more information about the Topology Map and functions you can perform on the Topology Map, refer to "Topology Map" on page 285.

- Minimap — The bottom right pane displays an overall view of the Topology Map. To jump to a specific location on the Topology Map, click that area on the Minimap, and a close-up view of the selected location displays on the Topology Map. For more information about the Minimap and using the Minimap, refer to "Minimap" on page 288.

Topology map elements

Topology maps are comprised of nodes and connections. To display the topology legend, click the **Legend** button on the main toolbar.

The **Legend** dialog box displays.

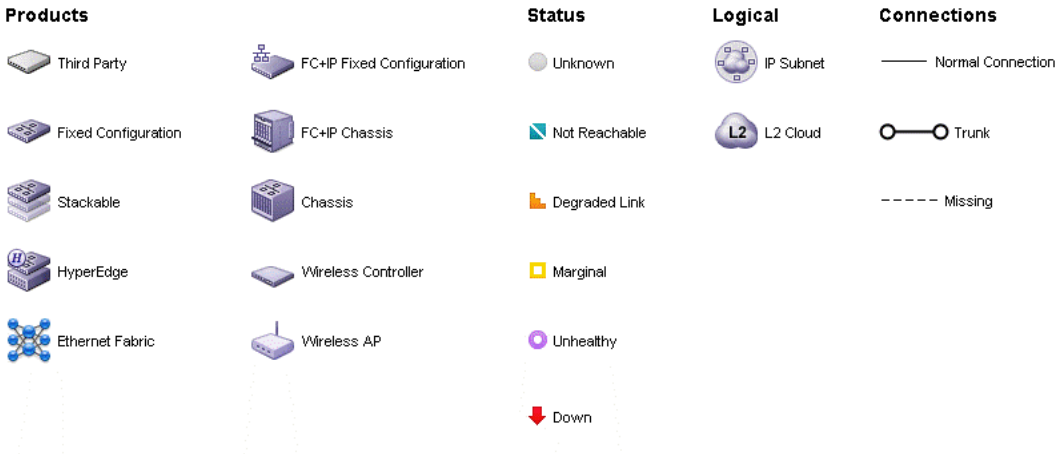


FIGURE 129 Legend dialog box

Table 34 displays the elements included in the topology.

TABLE 34 Legend components

Icon	Description	Icon	Description
Products			
	Third-Party		FC+IP Fixed Configuration
	Fixed Configuration		FC+IP Chassis
	Stackable		Wireless Controller
	Chassis		Wireless AP
	Ethernet Fabric		HyperEdge
Status			
	Unknown		Not Reachable
	Degraded Link		Marginal
	Down		Unhealthy
Logical			
	IP Subnet		Layer 2 Clouds
Connections			
	Normal Connection		Trunk
	Missing		

The following list describes the basic elements included in a topology map.

- IP devices — This node displays as a blue box. To view all IP product icons, refer to "IP product icons" on page 290. Double-click a product icon to display the **Properties** dialog box. For more information, refer to "IP device properties" on page 1314.
- Third-party devices — This node displays as a gray box.
- Subnets — This node displays as a blue circle. Double-click a subnet to display the devices within the subnet.

- Layer 2 Clouds — This node displays as a blue cloud. When two or more devices with FDP or LLDP enabled connect to a device or network without FDP or LLDP capability, the L2 cloud icon is displayed to represent the connection between the device types. This icon means that IronWare OS or Network OS devices are not directly connected to each other and each IronWare OS or Network OS device does not have Layer 2 information from other devices.
- Interface connections — The connections between nodes (devices, IP Subnets, or Layer 2 clouds) display as a gray line. The numbers on the line show the ports or virtual routing interfaces that form the connection.
- Missing interface connections — A dashed line indicates a missing connection.
- Trunks — Each trunk (MCT or ICL) displays as a straight line with circles at each end.

Viewing flyovers on the topology map

The Management application allows you to enable flyover display on Topology Maps. To enable flyover display, refer to "Turning flyovers on or off" on page 142.

- Device node — Mouse over to view the display name, IP address, and status of the device.
- Connections — Flyover display varies depending on the type of connection.
  - Interface connection — Mouse over to display IP address and port number for each end of the connection.
  - Trunk connection — Mouse over to display the truck group identifier and the IP address, port number, and type of trunk (MCT or ICL) for each end of the connection.
  - Layer 2 Cloud connections — Mouse over to display IP address for each end of the connection.

Topology map layout

The Management application provides several layouts for the IP Topology, Ethernet Fabrics, L2 Topology, and VLAN Topology views, so that you can determine which one provides the best display of your network topology. When selecting a layout, keep the following in mind:

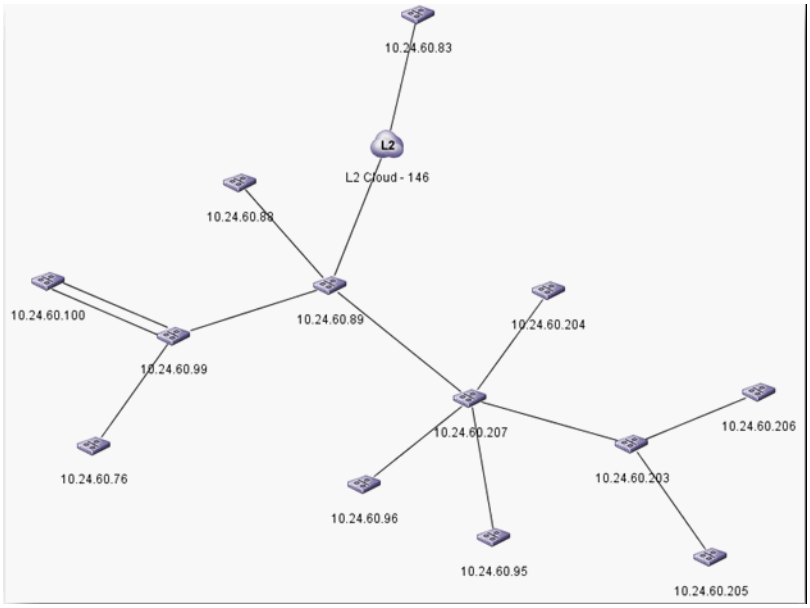
- When you first open a Topology view, the Topology Map uses the layout option specified in the **Topology Display** dialog box. In a typical topology, the default layout for all topology views is Organic. For IP Topology, the default layout is Circular. For VLAN topologies, the default layout is Orthogonal (Merge Lines).
- The position of nodes on the next layout type depends on their position in the previously displayed layout. You may see a better display if you choose the Circular layout first, then choose the next layout you want to try.
- As you move from one layout to another the Management application animates the process of redrawing the map.

  When a topology map update is in progress, you can interact with client. The layout management is a background thread. The amount of computing resource required to draw a new layout depends on the number of nodes and connections on the network. If the layout execution duration exceeds a minimum threshold, a progress bar displays. The minimum threshold duration is 1 second.
- During a session, as you enter and exit any of the topology views, the last layout used is the one displayed when you return to that topology view. However, the layouts are reset to the default layouts when you logout of the Management application.

The following examples show the differences between the layouts. They may or may not match the map drawn for your network. Also, some of the examples may look alike; however, the layouts may look different on networks with more devices.

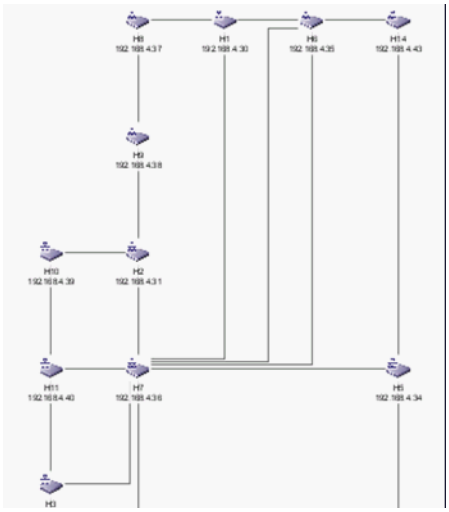
Organic

The Organic layout distributes the nodes evenly, makes connection lengths uniform, minimizes crisscrossing of connections, and tries to prevent nodes from touching each other. This layout is best for the visualization of highly connected backbone regions with attached peripheral ring or star structures.



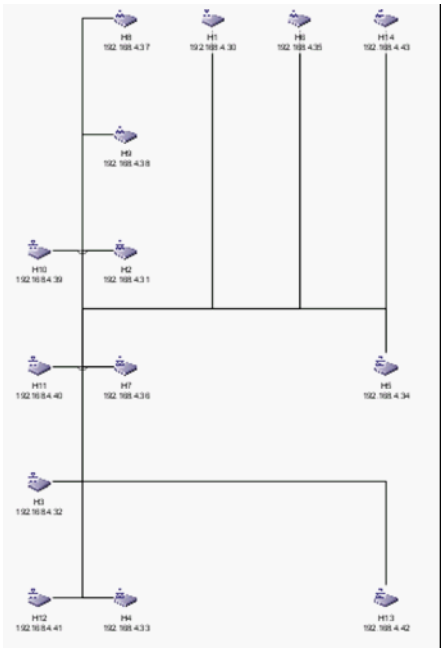
Orthogonal

The Orthogonal layout displays the nodes compactly with no overlaps, minimizes crisscrossing of connections, and tries to prevent nodes from touching each other. This layout is best for medium-sized sparse graphs since it produces clear representations of complex networks.



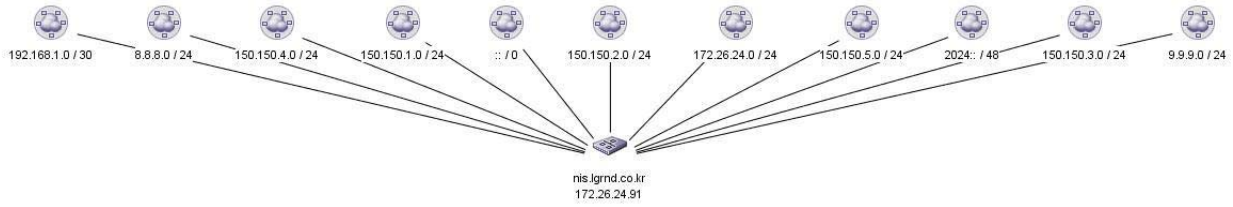
Orthogonal (Merge Lines)

The Orthogonal (Merge Lines) layout displays the nodes in a concise tree-like structure using vertical and horizontal line segments.



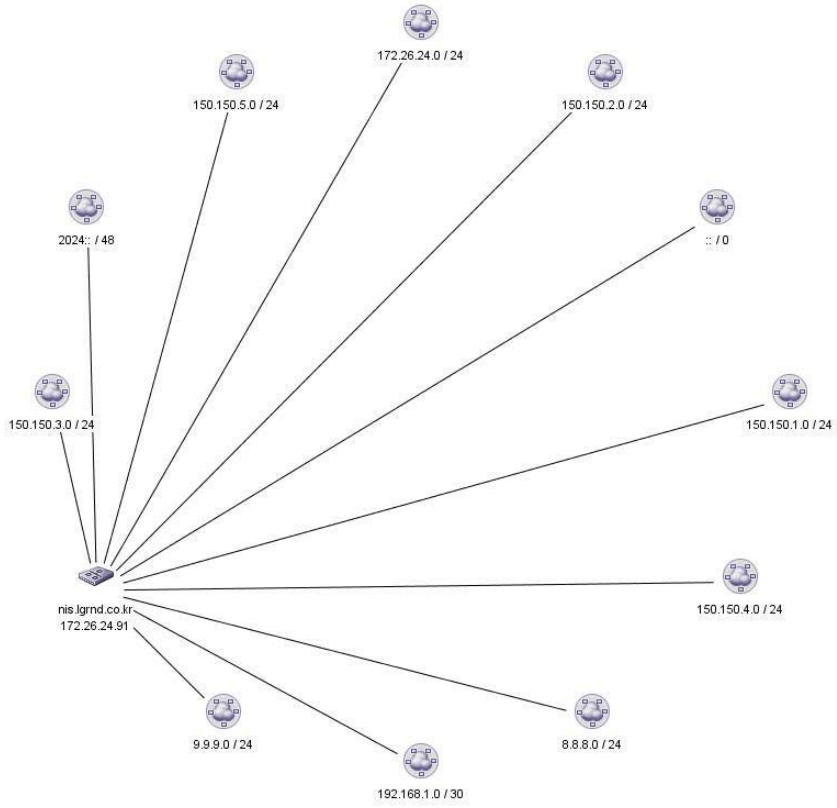
Hierarchical

The Hierarchical layout is best for a complex map. This layout might have a start point and end point, with some overall flow between those points.



Circular

The Circular layout distributes all nodes in a circle, with equal spacing between each neighbor node.



Free Form

This layout is the one you customize by repositioning the nodes on the map.

Selecting a topology map layout

To change the topology layout, complete the following steps.

1. Select one of the following view types from the view list on the Product List toolbar.
   - L2 Topology
   - Ethernet Fabrics
   - IP Topology
   - VLAN Topology
2. Click the **Topology Display** icon on the Topology Map toolbar.

   The **Topology Display** dialog box displays.

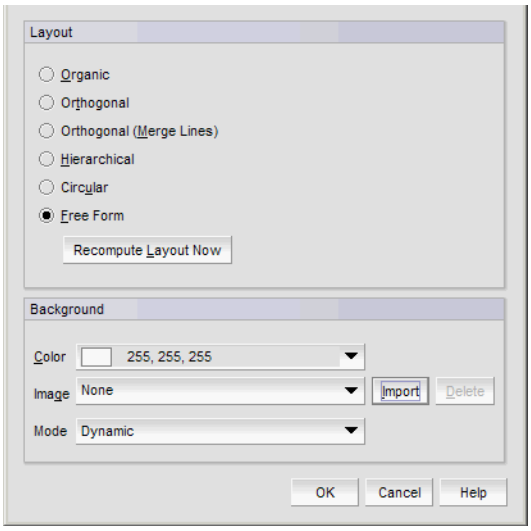


FIGURE 130 Topology Display dialog box

3. Select one of the following topology layouts in the **Layout** area.
   - **Organic**
   - **Orthogonal**
   - **Orthogonal (Merge Lines)**
   - **Hierarchical**
   - **Circular**
   - **Free Form**
4. Click **Recompute Layout Now**.

   The Management application redraws the Topology Map.
5. Click **OK** on the **Topology Display** dialog box.

Creating a customized layout

You can create one customized layout for each group node in each topology view.

To customize the layout for a topology map, complete the following steps.

1. Select the view you want to customize from the view list on the Product List toolbar.
   - IP Topology
   - L2 Topology
   - Ethernet Fabrics
   - VLAN Topology
2. Click a node and drag it to a new position on the map.

   The application automatically changes the layout to Free Form. To move one or more nodes at the same time, complete the following steps:

a. Use Ctrl + click to select one or more nodes or click in an empty part of the topology and drag a box around the nodes you want to move.

b. Select one of the highlighted nodes and drag the selected nodes to a new position on the map.

3. Repeat step 2 until you have repositioned all nodes.

   Navigation to another view topology or tab or exiting the application automatically saves your changes. If you change the topology map layout (refer to "Selecting a topology map layout" on page 320) and want to return to this customized layout, complete the following steps.

   a. Click the **Topology Display** icon on the Topology Map toolbar.

      The **Topology Display** dialog box displays.

   b. Select **Free Form** in the **Layout** area.

   c. Click **OK** on the **Topology Display** dialog box.

Creating customized topology links

The Management application enable you to create network topology links manually using the topology_data.txt file located in the *Install_Home*\conf\discovery\ip directory. You only need to add the link in one direction between two devices. Once you add the link, L2 neighbor collection uses the topology_data.txt file, in addition to links detected using FDP and LLDP, to construct links for each device. You add multiple entries for a single device as needed.

Changes to the topology_data.txt file do not require a management server restart, the changes display during the next L2 neighbor collection for the devices.

The data file uses the following format:

- The hash character (#) at the beginning of a line indicates a comment and is not parsed during L2 neighbor collection.
- Specify each link on a separate line.
- Each link consists of two columns separated by white space.
- Each column consists of an IP address, then a vertical bar (|), then the interface name.
- The interface name must use the exact format returned by the ifName MIB variable for that device.The interface name can be found in the Interface Name column of the Detailed Product Report, Physical Ports section.
- If the ifName value contains a space in the name, then the interface name should be within double quotes.

  Examples

  ```
  143.140.1.222|ethernet8/12 192.1.7.182|ethernet49
  10.24.84.1|"ExT 0/15" 10.24.84.4|"ExT 0/16"
  143.140.1.222|"ethernet 8/12" 192.1.7.182|"ethernet 49"
  143.140.1.222|"ethernet 8/12" 192.1.7.182|ethernet49
  ```

To create a customized topology link, complete the following steps.

1. Open the topology_data.txt (located in *Install_Home*\conf\discovery\ip) file in a text editor.
2. Add the link using the following format:

Device_One_IP_Address|*Interface_Name Device_Two_IP_Address*|*Interface_Name* where *Device_One_IP_Address* is the IP address for the device at one end of the link, *Interface_Name* the is the exact format returned by the ifName MIB variable for the device, and *Device_Two_IP_Address* is the IP address for the device at the other end of the link.

3. Save and close the topology_data.txt file.

   The customized topology links display during the next L2 neighbor collection for the devices.

Customizing the Topology Map

To customize the Topology Map, complete the following steps.

1. Click the **Topology Display** icon on the Topology Map toolbar.

   The **Topology Display** dialog box displays.

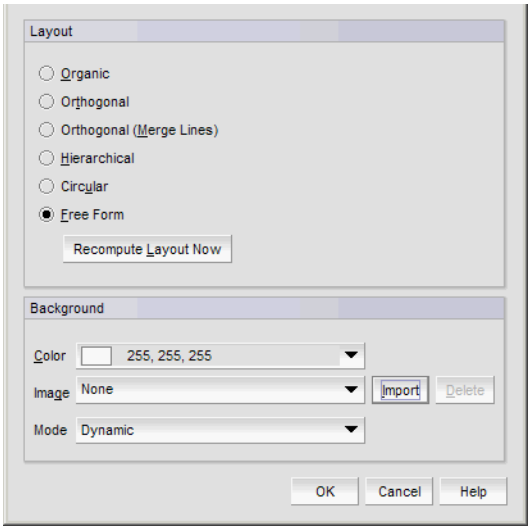


FIGURE 131 Topology Display dialog box

2. Change the background color by selecting a color from the **Color** list.

   a. To select a color not included in the **Color** list, select **More Colors** from the **Color** list.

      The **Choose a Color** dialog box displays.

   b. Choose one of the following options to select the color you want:

      - To pick a color from a swatch, select the **Swatches** tab. Select a color from the display.
      - To specify a color based on hue, saturation, and value, click the **HSV** tab. Specify the hue (0 to 359 degrees), saturation (0 to 100%), value (0 to 100%), and transparency (0 to 100%).
      - To specify a color based on hue, saturation, and lightness, click the **HSL** tab. Specify the hue (0 to 360 degrees), saturation (0 to 100%), lightness (0 to 100%), and transparency (0 to 100%).
      - To specify a color based on values of red, green, and blue, click the **RGB** tab. Specify the values for red, green, blue, and alpha (0 to 255) or enter a color code in the **Color Code** field.

- To specify a color based on values of cyan, magenta, yellow, and black, click the **CMYK** tab. Specify the values for cyan, magenta, yellow, black, and alpha (0 to 255).

c. Click **OK** on the **Choose a Color** dialog box.

3. Add an image to the background by selecting an image from the **Image** list.

   To import an image, refer to "Adding a background image to a map" on page 324.

4. Set the background image mode by selecting one of the following from the **Mode** list:

   - **Dynamic** — Select when the background image is considered to be part of the displayed contents and not a decoration. In this mode, an object on a specific point of the image, stays on that specific point during zooming or scrolling on the topology. In this mode, the application uses the background color to draw visible regions outside the bounds of the background image.
   - **Fullscreen** — Select to display the upper left corner of the background image in the upper left corner of the topology and scale the background image to the size of the topology. In this mode, the background is static (zooming or scrolling have no effect). If you resize the topology, the background image scales accordingly.
   - **Tiled** — Select to display the background image as tiles on the topology. In this mode, the background is static (zooming or scrolling have no effect).
   - **Bricked** — Select to display the background image as bricks on the topology. In this mode, the background is static (zooming or scrolling have no effect).
   - **Centered** — Select to display the background image centered in the topology. In this mode, the application uses the background color to draw visible regions outside the bounds of the background image. In this mode, the background is static (zooming or scrolling have no effect).
   - **Plain** — Select to display the background image at a specific origin on the topology. In this mode, the application uses the background color to draw visible regions outside the bounds of the background image. In this mode, the background is static (zooming or scrolling have no effect).

5. Click **OK** on the **Topology Display** dialog box.

Adding a background image to a map

Make sure you have the background image on your hard drive. You can use any image type (supported by Java), including GIF, JPG, JPEG, or PNG file format.

NOTE
The image file name cannot be longer than 64 characters.

You can add a background image to each topology sub type. For example VLAN 5 and VLAN 14 can have different background images.

To add a background image to a Topology Map, complete the following steps.

1. Click the **Topology Display** icon on the Topology Map toolbar.

   The **Topology Display** dialog box displays with the name of the current background image in the **Image** list. The **Image** lists includes all imported background images.

2. Click **Import**.

   The **Open** dialog box displays.

3. Browse to the map image.
4. Click **Open**.

   The imported image displays in the **Image** list.
5. Set the background image mode by selecting one of the following from the **Mode** list:
   - **Dynamic** — Select when the background image is considered to be part of the displayed contents and not a decoration. In this mode, an object on a specific point of the image, stays on that specific point during zooming or scrolling on the topology. In this mode, the application uses the background color to draw visible regions outside the bounds of the background image.
   - **Fullscreen** — Select to display the upper left corner of the background image in the upper left corner of the topology and scale the background image to the size of the topology. In this mode, the background is static (zooming or scrolling have no effect). If you resize the topology, the background image scales accordingly.
   - **Tiled** — Select to display the background image as tiles on the topology. In this mode, the background is static (zooming or scrolling have no effect).
   - **Bricked** — Select to display the background image as bricks on the topology. In this mode, the background is static (zooming or scrolling have no effect).
   - **Centered** — Select to display the background image centered in the topology. In this mode, the application uses the background color to draw visible regions outside the bounds of the background image. In this mode, the background is static (zooming or scrolling have no effect).
   - **Plain** — Select to display the background image at a specific origin on the topology. In this mode, the application uses the background color to draw visible regions outside the bounds of the background image. In this mode, the background is static (zooming or scrolling have no effect).
6. Click **OK** on the **Topology Display** dialog box.

   The image displays in the background of the Topology Map.

Deleting a background image from the library

You can only delete images not in use in any topology or by any user. To delete a background image to a Topology Map, complete the following steps.

1. Click **Map** on the Topology Map tool bar.

   The **Topology Background Map** dialog box displays.
2. Select the image you want to delete in the **Image Library** list and click **Delete**.
3. Click **OK** on the **Topology Background Map** dialog box.
4. Click **Yes** on the confirmation message.

Exporting the topology

To export a Topology Map as an image file, complete the following steps.

1. Click the **Export** icon on the Topology Map tool bar.

   The **Export** dialog box displays.

2. Browse to the location where you want to save the map image.
3. Enter a name for the map in the **File Name** field.
4. Select the export file type in the **File of Type** list.

   Options include: PNG, GIF, JPG, BMP, PDF, and EMF.
5. Click **Save**.

Printing a map

To print a Topology Map, complete the following steps.

1. Click the **Print** icon on the Topology Map tool bar.

   The **Print** dialog box displays.
2. To configure the page setup, click **Page** on the **Print** dialog box.

   The **Page Setup** dialog box displays.
   a. Select the page size from the **Size** list.
   b. Select the source from the **Source** list.
   c. Select **Portrait** or **Landscape** from the **Orientation** area.
   d. Enter the top, bottom, left and right margins in the **Margins** area.
   e. Click **OK** on the **Page Setup** dialog box.
3. To zoom in and out, click **Zoom In** or **Zoom Out**.
4. To set a specific zoom, select an option from the list.

   Options include: Fit, Fit Width, 10%, 25%, 50%, 60%, 70%, 80%, 90%, 100%, 200%, 300%, or 400%.
5. To set additional options (such as poster print, headers, and footers), click **Options**.

   The **Print Options** dialog box displays.
   a. Click the **General** tab.
   b. Enter the number of rows in the **Poster Rows** field.
   c. Enter the number of columns in the **Poster Columns** field.
   d. Enter the number of columns in the **Poster Columns** field.
   e. To add poster coordinates, select the **Add Poster Coords** check box.
   f. Click the **Title** tab.
   g. Enter a title in the **Text** field.
   h. Select a color for the title bar from the **Titlebar Color** list.
   i. Select a color for the title from the **Text Color** list.
   j. Enter a title in the **Text** area.
   k. Enter the font size in the **Font size** field.
   l. Click the **Footer** tab.

m. Enter a footer in the **Text** field.

n. Select a color for the footer from the **Footer Color** list.

o. Select a color for the title from the **Text Color** list.

p. Enter a title in the **Text** area.

q. Enter the font size in the **Font size** field.

r. Click **OK** on the **Print Options** dialog box.

6. Click **Print**.

   The **Print** dialog box displays.

7. Select a printer from the **Name** list.

8. Click **OK** on the **Print** dialog box.

9. Click the close (X) button on the **Print** dialog box.

Port actions

The Management application allows to you enable and disable port actions, display the port properties of the Network OS device to which the FCoE WWN is attached, as well as access performance monitoring from the **Port** tab of the **Properties** dialog box.

Enabling port actions

To enable port actions, complete the following steps.

1. Select one of the following view types from the view list on the Product List toolbar.
   - Network Object
   - IP Topology
   - L2 Topology
   - Ethernet Fabrics
   - VLAN Topology
2. Right-click the device in the Product List and select **Properties**.

   The *Device_Name* **Properties** dialog box displays.

3. Click the **Port** tab.
4. Select **Enable** from the **Port Actions** list.

   NOTE
   If the VDX FC Port is enabled through the **Properties** dialog box, the **Port Status** displays as "No_Light". To obtain the updated value, re-open the **Properties** dialog box after the next collection cycle.

5. Click **OK** to close the dialog box.

Disabling port actions

To disable port actions, complete the following steps.

1. Select one of the following view types from the view list on the Product List toolbar.
    - Network Object
    - IP Topology
    - L2 Topology
    - Ethernet Fabrics
    - VLAN Topology
2. Right-click the device in the Product List and select **Properties**.

    The *Device_Name* **Properties** dialog box displays.
3. Click the **Port** tab.
4. Select **Disable** from the **Port Actions** list.
5. Click **OK** to close the dialog box.

Displaying port properties for an attached device

The **Display Attached Port Properties** option is only applicable for routed-in devices. The device must be managed by the Management application and part of your AOR.

To display the port properties of the Network OS device to which the FCoE WWN is attached, complete the following steps.

1. Select one of the following view types from the view list on the Product List toolbar.
    - Network Object
    - IP Topology
    - L2 Topology
    - Ethernet Fabrics
    - VLAN Topology
2. Right-click the device in the Product List and select **Properties**.

    The *Device_Name* **Properties** dialog box displays.
3. Click the **Port** tab.
4. Select a port with one or more world wide names (WWN) displaying in the **Connected Devices** field.
5. Select **Display Attached Port Properties** from the **Port Actions** list.
6. Click **OK** to close the dialog box.

    The *VCS_Name* **Properties** dialog box displays with the attached ports highlighted in the **Ports** tab.

Accessing performance monitoring

To access performance monitoring dialog boxes, complete the following steps.

1. Select one of the following view types from the view list on the Product List toolbar.
   - Network Object
   - IP Topology
   - L2 Topology
   - Ethernet Fabrics
   - VLAN Topology
2. Right-click the device in the Product List and select **Properties**.

   The *Device_Name* **Properties** dialog box displays.
3. Click the **Port** tab.
4. Select one of the following from the **Performance** list.
   - Real Time Graph/Table
   - Historical Graph/Table

     The **Real Time Graph/Table** or **Historical Graph/Table** dialog box displays.

     To configure and generate real time performance, refer to "IP real-time performance monitoring" on page 983.

     To configure and generate historical performance, refer to "IP historical performance monitoring" on page 995.
5. Click **OK** to close the *Device_Name* **Properties** dialog box.

Chapter

9

MRP Topology

In this chapter

MRP Topology overview

The Metro Ring Protocol (MRP) is a IronWare proprietary protocol used to prevent Layer 2 loops and to provide fast reconvergence in a Layer 2 ring topology. The MRP Topology view displays a map of the MRP rings on your network. To display the topology map for MRP, you must have the IP - Main Display – MRP privilege in your user role and the MRP device must be in your area of responsibility (AOR).

Before you display the MRP topology, make sure you meet the following requirements on your devices:

- The device is MRP-enabled.
- The devices are running FDP or LLDP.

  If you do not enable FDP or LLDP on a product, the product displays without any links.
- The snMetroRingTable MIB table (OID.1.3.6.1.4.1.1991.1.1.3.29.2.1) is enabled on the device and has MRP configured. This MIB is not supported on third-party products.

MRP Topology view is available for the following devices:

- FastIron Edge Switch running FES software release 04.0.00 and later.
- FastIron X Series devices running FSX software release 04.0.00 and later.
- FastIron CX switches running FCX software release 04.0.00 and later.
- FastIron GS, FastIron LS, and FastIron WS running FGS software release 04.0.00 and later.

You can use the CLI Configuration Manager to deploy MRP configurations to devices. You can also configure MRP using the device CLI. You can use the Element Manager to access the device or go directly to the device CLI. You must enable the MRP trap on the devices so that the Management application can monitor MRP ring status. For more information about MRP rings and configuration instructions, refer to your hardware's configuration guide.

Viewing a MRP Topology map

The MRP Topology view does not support dynamic updates. You must manually refresh the view For more information, refer to "Refreshing MRP Topology data" on page 340.

To view a MRP Topology map, select **Monitor > MRP Topology**.

The **MRP Topology** dialog box displays.

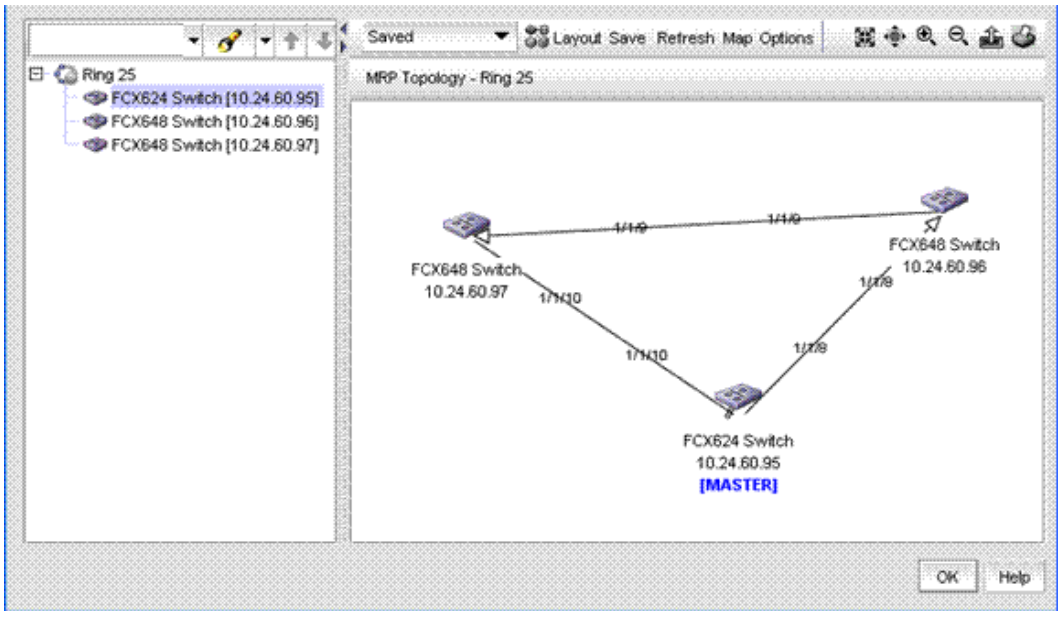


FIGURE 132 MRP Topology dialog box

The MRP Topology map is divided into two sections:

- Product List — The top left pane displays a list of all MRP rings (topology tree) discovered in the network that are in your AOR. Each ring is identified by its ring number. Double-click a ringin the Product List to display the devices in the MRP ring. The Management application has a Search tool that you can use to find a device quickly. (Refer to "Using the Search tool" on page 53 for more information.)

  When you select a ring in the Product List, the application displays the ring in the Topology Map. When you select a device in the Product List, the application highlights the device on the Topology Map as well.

- Topology Map — The right pane displays the devices in a MRP ring using graphic elements (icons). Links between devices running FDP or LLDP display automatically on the topology maps.

When you select a device on the Topology Map, the application highlights the device in the Product List.

Viewing a MRP ring

To view a MRP ring, click a ring in the Product List.

The selected ring displays in the Topology Map.

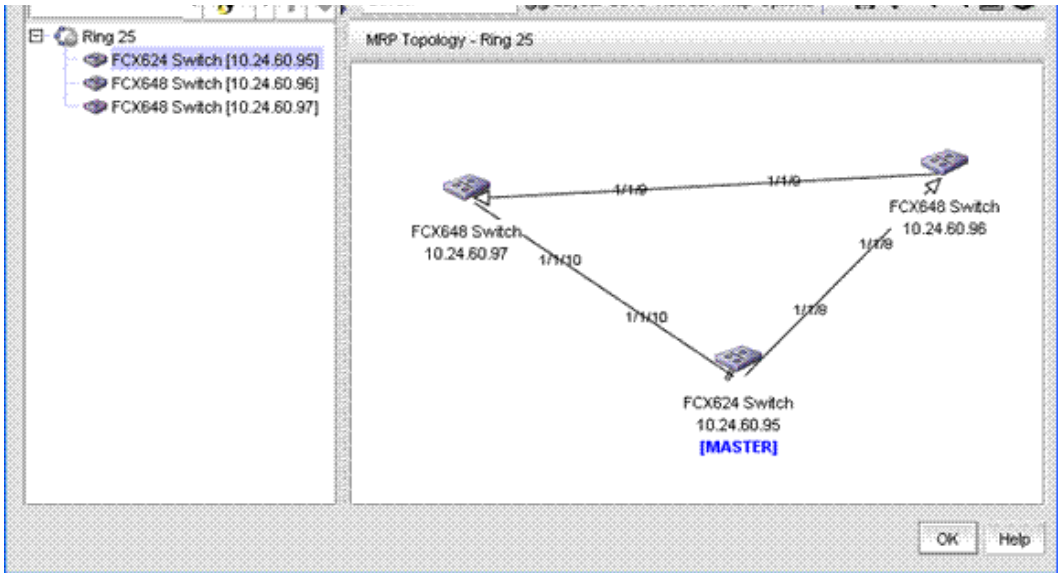


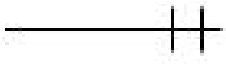
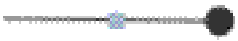
FIGURE 133 MRP Topology dialog box

MRP Topology maps are comprised of nodes (rings) and connections (devices). Table 35 displays the basic elements included in a MRP topology map.

TABLE 35 MRP Topology map elements

Element	Description
Device icon	Each device on the map displays its device name and IP address.
[MASTER]	Denotes the master device.
solid line	The nodes on the ring are connected and in normal operating state.
broken line	The two end points of an MRP link are disabled. To show a broken line on the topology, refer to "Configuring the application to show a dashed line" on page 335
link with arrow head	The port is in a pre-forwarding or forwarding state and shows the direction of the packet flow.

TABLE 35 MRP **Topology map elements**

Element	Description
 link with block	The port is in a blocking state or discarding.
 link with solid black circle	MRP is disabled on the port.
# or # / #	The forwarding or receiving port number of slot/port number. To make the forwarding and receiving port number data visible on the map, you must enable **Link Information Visibility** (default is disabled) on the **MRP Topology Options** dialog box. For instructions, refer to "Customizing the MRP Topology map" on page 339.
tool tips	Link tool tips — identifies the devices at each end of the link to help you locate the devices on the map. Node tool tips — identifies the device name and IP address of the node.

The Management application obtains MRP status by monitoring the MRP traps that devices send. These traps are reported in the Master Log. Make sure MRP traps are enabled on the devices that are members of an MRP ring. For the MRP Status to display correctly, you must discover a proper ring through the Management application. If the link (edge) or a device (Vertex) is missing, the status does not display correctly; however, the feature may work.

MRP ring status is defined by specific rules and represented by one of the following icons:

TABLE 36

Icon	Description
 Normal	MRP ring is in normal operation.
 Error	Both ports on a MRP-enabled device are disabled. No Master node on the MRP ring. Two or more Master nodes exist on the MRP ring.
 Warning	The Master node is in Forwarding or Forwarding state and none of the devices on the MRP ring are in an Error state.

The Topology toolbar is located at the top of the Topology Map and provides icons and buttons to perform various functions.

- Layout type list. Use to select the layout (Organic, Fast Organic, Hierarchical, Self Organizing, Circular, or Saved) of the Topology Map. For more information about layout types, refer to "Topology map layout" on page 317.
- **Layout** button. Use to set the layout selected from the Layout type list. For more information about layout types, refer to "Selecting a topology map layout" on page 335.
- **Save** button. Use to save changes to the MRP Topology map. For more information about layout types, refer to "Creating a customized layout" on page 338.
- **Map** button. Use to add a background image to the Topology Map. For more information about adding a background image, refer to "Adding a background image to a map" on page 324.

- **Options** button. Use to configure topology options.
- **Fit Window** icon. Use to scale the map to fit within the Topology Map area.
- **Actual Size** icon. Use to scale the map to fit within the Topology Map area.
- **Zoom In** icon. Use to zoom in on the Topology Map.
- **Zoom Out** icon. Use to zoom out on the Topology Map.
- **Export** icon. Use to export the topology to a PNG file. For export instructions, refer to "Exporting the topology" on page 325.
- **Print** icon. Use to print the current Topology Map image. For print instructions, refer to "Printing a map" on page 326.

Configuring the application to show a dashed line

To configure the application to show a dashed line when links are broken, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.
3. Click the **Preferences** tab.
4. Select the **Retain lost links __ hours (1 minimum)** option to configure how long to retain lost links on the topology maps and enter a value (from 1 through 9999) in the field.

   The default is 168 hours.

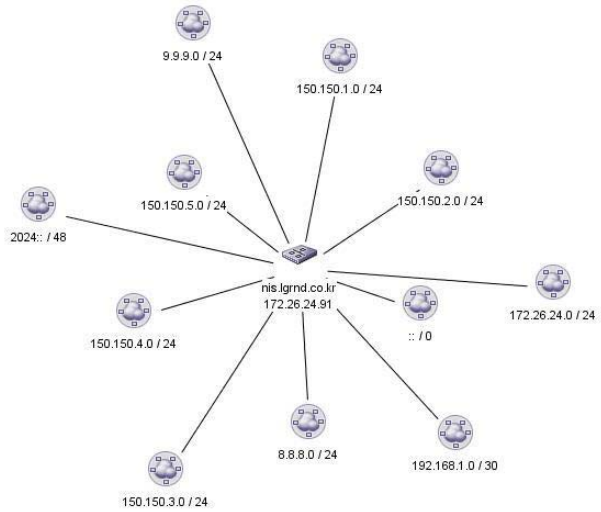
5. Click **Apply** to save your work.
6. Click **Close** to close the **Discover Setup - IP** dialog box.

Selecting a topology map layout

To change the topology layout, select one of the following topology layouts from the layout type list on the Topology Map toolbar.

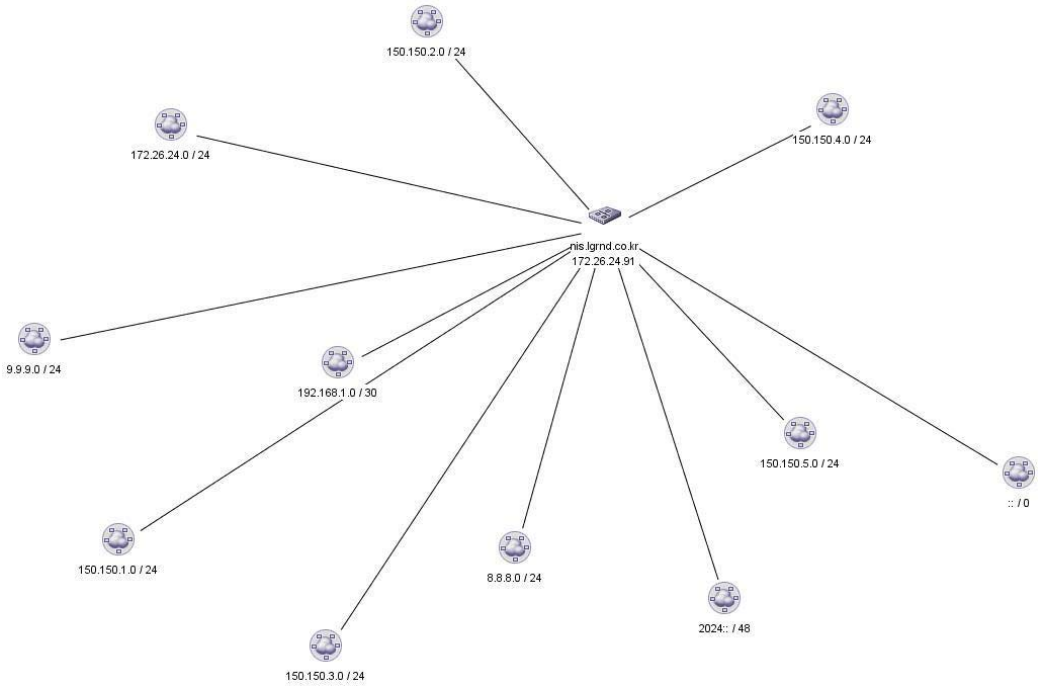
- Fast Organic

  The Fast Organic layout is a variation on the Organic layout; however, connections are drawn closer to the nodes. The time it takes to draw the Fast Organic layout is proportional to the number of nodes squared. Generally, this layout is best for smaller networks.



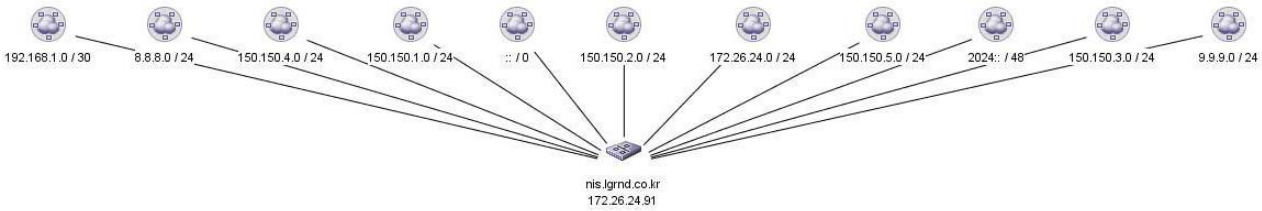
- Organic

  The Organic layout distributes the nodes evenly, makes connection lengths uniform, minimizes criss-crossing of connections, and tries to prevent nodes from touching each other.



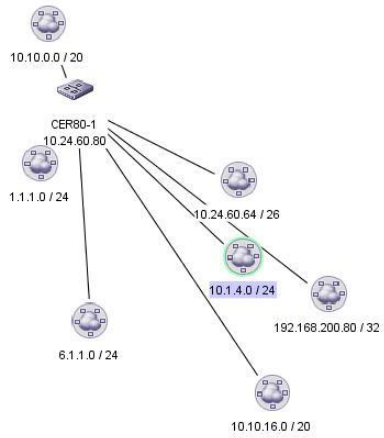
- Hierarchical

  The Hierarchical layout is best for a complex map. This layout might have a start point and end point, with some overall flow between those points.



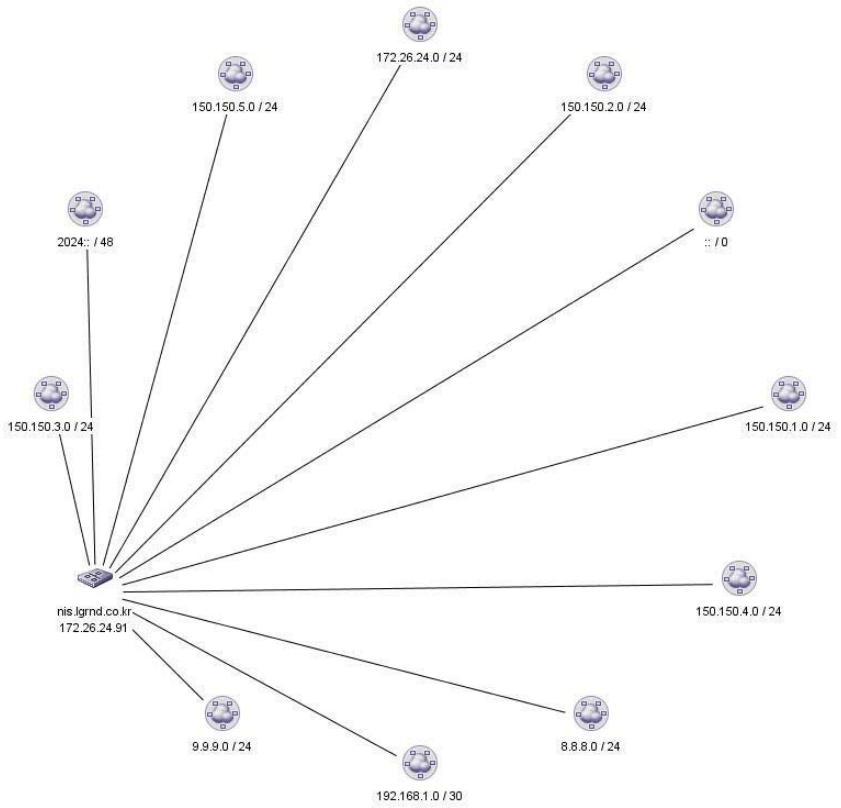
- Self Organizing

  The Self Organizing layout distributes nodes and connections evenly on the display area in a linear layout.



- Circular

  The Circular layout distributes all nodes in a circle, with equal spacing between each neighbor node.



- Saved

  This layout is the one you customized by repositioning the nodes on the map. If you have not customized the layout, this Saved option is disabled. Also, if you select the Saved Layout Preferred check box on the **Topology Options** dialog box, this layout takes precedence over the default layout.

  The Management application redraws the MRP Topology map. For more information about layout types, refer to "Topology map layout" on page 317.

Creating a customized layout

You can create one customized layout for each Ring node in each topology view.

To customize the layout for a topology map, complete the following steps.

1. Select the topology layout you want to customize from the layout type list on the Topology Map toolbar.
   - Fast Organic
   - Organic
   - Hierarchical
   - Self Organizing
   - Circular
2. Click a node and drag it to a new position on the map.

3. Repeat step 2 until you have repositioned all nodes.
4. Click **Save** on the MRP Topology map toolbar to retain the changes you made.

Customizing the MRP Topology map

To customize the MRP Topology map, complete the following steps.

1. Click **Options** on the MRP Topology map tool bar.

   The **MRP Topology Options** dialog box displays.

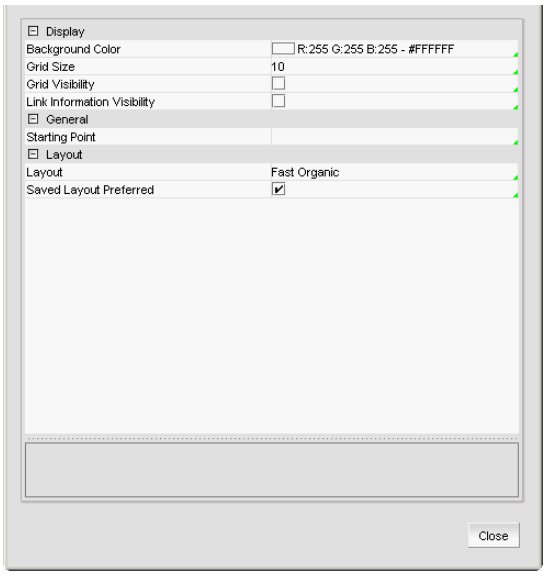


FIGURE 134 Topology Options dialog box

2. Change the background color by completing the following steps:
   a. Click the ellipsis button in the **Background Color** row.
   b. Select the color you want.
   c. Click **OK**.
3. Click the **Grid Size** row and select the size you want (5, 10, 15, or 20) from the list.
4. Select the **Grid Visibility** check box to make the grid visible in the topology map.

   Clear the check box to not display a grid.
5. Select the **Link Information Visibility** check box to make the forwarding and receiving port number data visible in the topology map.
6. Change the starting point of a MRP Topology Map by completing the following steps:

   By default, the first entry on the Product List is the starting point of a view. For example, if Ring 2 is the first ring on the Product List, then Ring 2 displays when you open the MRP Topology map.
   a. Click the **Starting Point** row.
   b. Enter the ring ID, for example, Ring 1.

7. Click the **Layout** row and select the layout you want from the list.
8. Select the **Saved Layout Preferred** check box to set the customized layout as the default for the topology group.

   This parameter supersedes the **Layout** parameter. If you select this parameter, the Saved layout displays even if a different layout is indicated in the **Layout** parameter.
9. Click **Close** on the **MRP Topology Options** dialog box.

Refreshing MRP Topology data

To refresh the MRP Topology data, click **Refresh**.

The MRP topology data syncs up with the data in the Management application server (not the switch). If you make MRP changes on the switch using the CLI, the Management application server uses the received traps to sync up the data. When the Management application receives traps, data collection for that specific object begins and once collection is complete the Management application server database is updated with the data. Note that data collection usually takes 2-3 minutes to finish depending on the network connectivity. However, data collection may take longer when network connectivity is slow or the switch is far away.

You can verify received traps through the Master Log. If no traps are received, data collection is triggered by the next lazy poll cycle. The lazy poll cycle is based on the configured network size (small = every 5 minutes; medium = every 15 minutes). The Management application server polls data collection from the switch and then updates the database.

Viewing MRP properties

To view MRP properties for a device, complete the following steps.

1. Right-click a device on the topology map and select **MRP Properties**.

   The **MRP Properties** dialog box displays.
2. Review the MRP property details:
   - **Hello Time** — The interval, in milliseconds, at which the Forwarding port on the ring's master node sends Ring Hello Packets (RHPs).
   - **Last Updated Time** — The date and time of the last update.
   - **Pre-forwarding Time** — The number of milliseconds an MRP interface that has entered the pre-forwarding state will wait before changing to the Forwarding state.
   - **Primary Port** — The primary port of the device.
   - **Primary Port Active** — The port number sending RHPs.
   - **Primary Port State** — The state (Pre-forwarding, Forwarding, Blocking, or Disabled) of the primary port.
   - **Primary Port Type** — The primary port type (Regular or Tunnel).
   - **RHP Received** — The number of RHPs received on the interface.
   - **RHPs Transmitted** — The number of RHPs sent on the interface.
   - **Ring ID** — The ring identifier.

- **Ring Name** — The MRP ring name.
- **Role** — The role (Master or Member) of the device.
- **Secondary Port** — The secondary port of the device.
- **Secondary Port Active** — The port number receiving RHPs.
- **Secondary Port State** — The state (Pre-forwarding, Forwarding, Blocking, or Disabled) of the secondary port.
- **Secondary Port Type** — The secondary port type (Regular or Tunnel).
- **State** — Whether MRP is enabled or disabled on the device.
- **State Changed** — The number of MRP interface state changes that have occurred.
- **TC RHPs Received** — The number of Topology Change RHPs received on the interface. A Topology Change RHP indicates that the ring topology has changed.
- **VLAN ID** — The VLAN ID or master VLAN ID in the topology group used by the ring.

3. Click **Close** on the **MRP Properties** dialog box.

Chapter

10

Call Home

In this chapter

Call Home overview

NOTE
Call Home is supported on Windows systems for all modem and e-mail Call Home centers and is supported on UNIX for the e-mail Call Home centers.

Call Home notification allows you to configure the Management application server to automatically send an e-mail alert or dial in to a support center to report system problems on specified devices (Fabric OS, IronWare, and Network OS switches, routers, and directors). If you are upgrading from a previous release, all of your Call Home settings are preserved.

Call Home supports multiple Call Home centers which allows you to configure different devices to contact different Call Home centers. When you make any Call Home configuration changes or a Call Home event trigger occurs, the Management application generates an entry to the Master Log.

You can configure Call Home for the following Call Home centers:

- Brocade E-mail (Windows and UNIX)
- EMC (Windows only)
- HP LAN (Windows only)
- IBM (Windows only)
- IBM E-mail (Windows and UNIX)
- NetApp E-mail (Windows and UNIX)
- Oracle E-mail (Windows and UNIX)

When configuring modem and HP LAN Call Home centers, you must enter the customer contact information in the device's Element Manager. You may also need to configure the Management application server IP address manually as an SNMP trap recipient for Fabric OS, IronWare, and Network OS devices.

Call Home allows you to automate tasks that occur when the Call Home event trigger is fired. When a Call Home event trigger occurs, the Management application generates the following actions:

- Sends an e-mail alert to a specified recipient or dials in to a support center.
- Triggers supportSave on the switch (if supportSave is enabled on the switch) prior to sending an alert. The supportSave location is included in the alert.

  NOTE
  The HP LAN Call Home alert displays the directory separation characters with a double backslash (\\) instead of a single backslash (\).

- Adds an entry to the Master Log file and screen display.
- Generates an XML report (only available with EMC Call Home centers) with the product details, which is sent with the e-mail alert.
- Generates an HTML report for e-mail-based Call Home centers.

For more information about Call Home events, refer to "Call Home Event Tables" on page 1275. For more information about events, refer to "Fault Management" on page 1141.

Call Home allows you to perform the following tasks:

- Assign devices to and remove devices from the Call Home centers.
- Define filters from the list of events generated by Fabric OS, IronWare, and Network OS devices.
- Edit and remove filters available in the Call Home Event Filters table.
- Apply filters to and remove filters from the devices individually or in groups.
- Edit individual Call Home center parameters to dial a specified phone number or e-mail a specific recipient.
- Enable and disable individual devices from contacting the assigned Call Home centers.
- Show or hide Call Home centers on the display.
- Enable and disable Call Home centers.

System requirements

Call Home (except for e-mail and HP LAN) requires the following hardware equipment:

- Any Windows server with an internal or external modem connection
- Analog phone line

Viewing Call Home configurations

To view Call Home center configurations, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays (Figure 135).

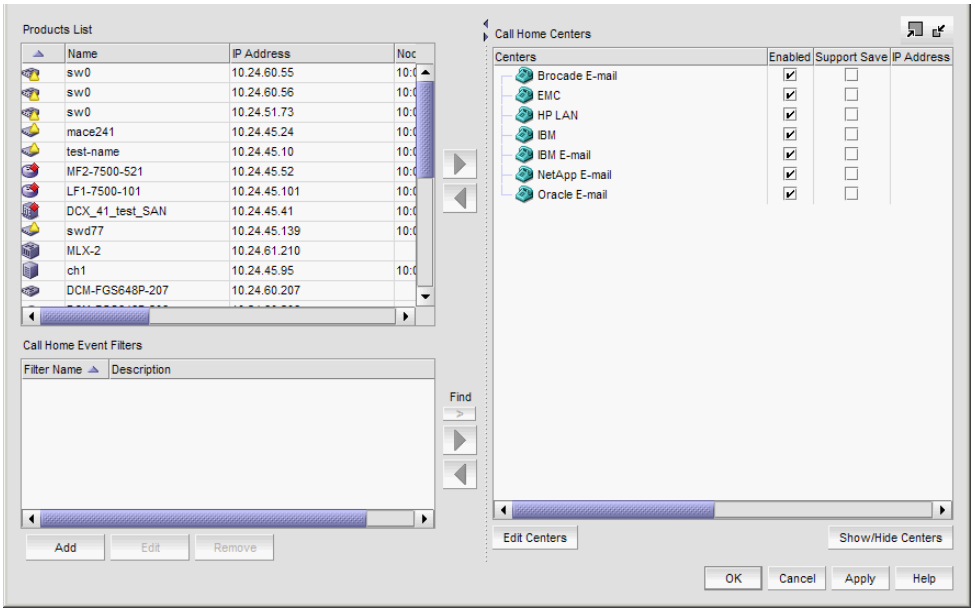


FIGURE 135 Call Home dialog box

The **Call Home** dialog box contains the following fields and components:

- **Products List** — Displays all discovered products. The list allows for multiple selections and manual sorting of columns. This list displays the following information:
  - **Product Icon —** The status of the products' manageability.
  - **Name —** The name of the product.
  - **IP Address** — The IP address (IPv4 or IPv6 format) of the product.
  - **Node WWN —** The node world wide name of the product.
  - **Fabric Name —** The name of the VCS.
  - **Vendor —** The vendor ID of the product.
  - **Call Home Status —** One of the following Call Home statuses for the product.
    - **Enabled** — The product is manageable and Call Home is enabled.
    - **Disabled** — The product is manageable and Call Home is disabled.
    - **Not Manageable** — The product is discovered but not manageable.
    - **Server Not Registered —** The server is not registered to receive Call Home events from the product.

    NOTE
    Call Home status only displays for Fabric OS, IronWare, and Network OS products.

  - **Domain/RBridge ID** — The domain or RBridge ID of the product.
  - **Product Type** — The type of product (switch, Layer 2 switch, router, or director).
- Right arrow buttons (top) — Click to assign the selected product to the selected Call Home center (refer to "Assigning a device to the Call Home center" on page 359). Disabled when no product is selected in the **Products List** or when more than one Call Home center is selected in the **Call Home Centers** list.
- Left arrow button (top) — Click to remove the selected product from the selected Call Home center (refer to "Removing a device from a Call Home center" on page 359). Disabled when no product or Call Home center is selected in the **Call Home Centers** list.
- **Call Home Event Filters** list — Displays all Call Home event filters. This list displays the following information:
  - **Filter Name** — The name of the event filter.
  - **Description** — The description of the event filter.
- **Add** button — Click to open the **Call Home Event Filter** dialog box and add an event filter (refer to "Defining an event filter" on page 360).
- **Edit** button — Click to open the **Call Home Event Filter** dialog box and edit an event filter (refer to "Defining an event filter" on page 360).
- **Remove** button — Click to remove the event filter (refer to "Removing an event filter from the Call Home Event Filters list" on page 363) from the **Call Home Event Filters** list.
- **Find** button (>) — Click to find all instances of the selected event filter in the **Call Home Centers** list.
- Right arrow button (bottom) — Click to assign the selected event filter (refer to "Assigning an event filter to a Call Home center" on page 361 or "Assigning an event filter to a device" on page 361) to the selected Call Home center or product. Disabled when no event filter is selected in the **Call Home Event Filters** list.

- Left arrow button (bottom) — Click to remove the selected event filter (refer to "Removing all event filter from a Call Home center" on page 362 or "Removing an event filter from a device" on page 363) from the selected Call Home center or product. Disabled when no event filter, product, or Call Home center is selected in the **Call Home Centers** list.
- **Call Home Centers** list — The Call Home centers, products assigned to the Call Home centers, and event filters assigned to the Call Home centers and products. This list displays the following information:
  - **Centers —** A tree with Call Home centers as the parent node, assigned products as subnodes, and event filters as the child node to the assigned products.
  - **Enabled** check box — Select the check box to enable the associated Call Home center or clear the check mark to disable the Call Home center. By default, all check boxes are selected during a fresh install.
  - **Support Save** check box — Select the check box to enable supportSave, which collects diagnostic information on Fabric OS switches.
  - **IP Address —** The IP address of the product.
  - **Node WWN —** The node WWN of the product.
  - **Fabric Name —** The name of the VCS.
  - **Vendor —** The vendor of the product.
  - **Call Home Status —** One of the following Call Home statuses for the product:
    - **Enabled** — The product is manageable and Call Home is enabled.
    - **Disabled** — The product is manageable and Call Home is disabled.
    - **Not Manageable** — The product is discovered but not manageable.
    - **Server Not Registered —** The server is not registered to receive Call Home events from the product.

  NOTE
  Call Home status only displays for Fabric OS, IronWare, and Network OS products.

  - **Domain/RBridge ID** — The domainor RBridge ID of the product.
  - **Product Type** — The type of product (switch, Layer 2 switch, router, or director).
- **Edit Centers** button — Select a call home center in the **Centers** list anc click **Edit** to open the **Configure Call Home Center** dialog box and modify Call Home center information (refer to "Editing a Call Home center" on page 349).
- **Show/Hide Centers** button — Click to open the **Centers** dialog box and add or delete a Call Home center (refer to "Showing a Call Home center" on page 348 or "Hiding a Call Home center" on page 348).

2. Click **OK** to close the **Call Home** dialog box.

Showing a Call Home center

To show a Call Home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Click **Show/Hide Centers** (beneath the **Call Home Centers** list).

   The **Centers** dialog box displays with a predefined list of Call Home centers (Figure 136).

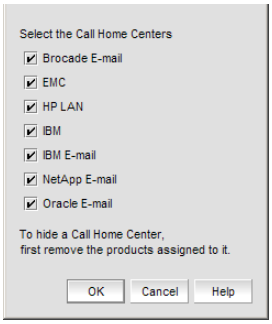


FIGURE 136 Centers dialog box

3. Select the check boxes of the Call Home centers you want to display.

   Clear the check box to hide the Call Home center.

4. Click **OK** on the **Centers** dialog box.

   The **Call Home** dialog box displays with the selected Call Home centers listed in the **Call Home Centers** list.

Hiding a Call Home center

NOTE
Before you can hide a Call Home center, you must remove all assigned products.

To hide a Call Home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Click **Show/Hide Centers** (beneath the **Call Home Centers** list).

   The **Centers** dialog box displays with a predefined list of Call Home centers.

3. Clear the check boxes of the Call Home centers you want to hide and click **OK**.

   The **Call Home** dialog box displays with only the selected Call Home centers listed in the **Call Home Centers** list.

Editing a Call Home center

To edit a Call Home center, select from the following procedures:

Editing the IBM Call Home center

To edit the IBM Call Home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Select **IBM** in the **Call Home Centers** list.

3. Click **Edit Centers** (beneath the **Call Home Centers** list).

   The **Configure Call Home Center** dialog box displays (Figure 137).

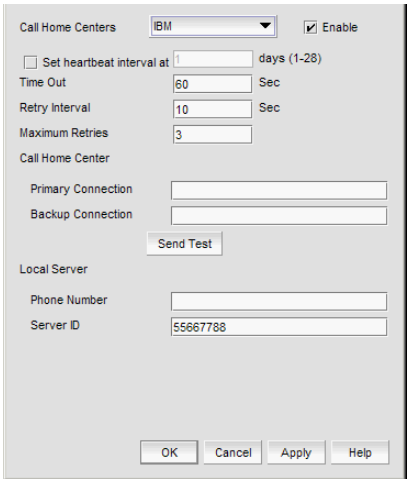


FIGURE 137 Configure Call Home Center dialog box (IBM option)

4. Make sure the Call Home center type you selected displays in the **Call Home Centers** list.

   If the Call Home center type is incorrect, select the correct type from the list.

5. Select the **Enable** check box to enable this Call Home center.

6. Set the time interval at which to check the Call Home center by selecting the **Set heartbeat interval at ___ days (1-28)** check box and entering the interval in the field.

7. Enter how long you want to wait before timing out the heartbeat interval in the **Time Out** field.

   The default is 60 seconds.

8. Enter how often you want to retry the heartbeat interval in the **Retry Interval** field.

   The default is 10 seconds.

9. Enter the maximum number of retries in the **Maximum Retries** field.

   The default is 3.

10. Enter the primary phone number or extension of the Call Home center in the **Call Home Center - Primary Connection** field.

11. Enter the backup phone number or extension of the Call Home center in the **Call Home Center - Backup Connection** field.

12. Enter the phone number or extension of the local server in the **Local Server - Phone Number** field.

13. Enter the identification number of the local server in the **Local Server - Server ID** field.

14. Click **Send Test** to test the phone number.

    The selected Call Home center must be enabled to test the phone number.

    A faked event is generated and sent to the selected Call Home center. You must contact the Call Home center to verify that the event was received and in the correct format.

15. Click **OK** to close the "Test Event Sent" message.

16. Click **OK**.

    The **Call Home** dialog box displays with the Call Home center you edited highlighted in the **Call Home Centers** list.

17. Click **OK** to close the **Call Home** dialog box.

Editing an e-mail Call Home center

E-mail Call Home centers are available for Brocade, IBM, NetApp, and Oracle. To edit one of these Call Home centers, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Select the Call Home center you want to edit (**Brocade E-mail**, **IBM E-mail**, **NetApp E-mail**, or **Oracle E-mail**) in the **Call Home Centers** table.

3. Click **Edit Centers** (beneath the **Call Home Centers** table).

   The **Configure Call Home Center** dialog box displays (Figure 138).

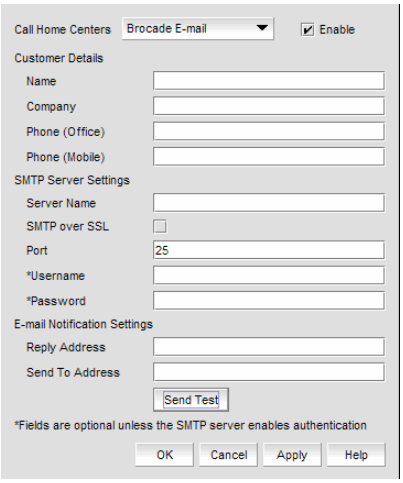


FIGURE 138 Configure Call Home Center dialog box (Brocade, IBM, NetApp, or Oracle E-mail option)

4. Make sure the Call Home center type you selected displays in the **Call Home Centers** list.

   If the Call Home center type is incorrect, select the correct type from the list.

5. Select the **Enable** check box to enable this Call Home center.
6. Enter your contact name in the **Customer Details - Name** field.
7. Enter your company name in the **Customer Details - Company** field.
8. Enter the phone number of the customer contact in the **Customer Details - Phone (Office)** field.
9. Enter the mobile phone number of the customer contact in the **Customer Details - Phone (Mobile)** field.
10. Enter the name of the e-mail server in the **SMTP Server Settings - Server Name** field.
11. Select the **SMTP over SSL** check box to enable secure communication between the SMTP server and the Management application.
12. Enter the port number of the server in the **SMTP Server Settings - Port** field.

    The default is 465 if SMTP over SSL is enabled; otherwise, the default is 25.

13. Enter a user name in the **SMTP Server Settings - Username** field.

    This is a required field when the SMTP server authentication is enabled.

14. Enter a password in the **SMTP Server Settings - Password** field.

    This is a required field when the SMTP server authentication is enabled.

15. Enter your e-mail address in the **E-mail Notification Settings - Reply Address** field.

    You can enter more than one e-mail address, separating each with a semi-colon. To send a text message or page by way of e-mail, use the following format: number@carrier.com (where number is your phone number and carrier.com is the SMS server; for example, 3035551212@txt.att.net (text message) or 3035551212@page.att.net (page)).

    NOTE
    Check with your carrier for the exact e-mail address format.

    This e-mail address must be a registered MyBrocade member.

16. Enter an e-mail address in the **E-mail Notification Settings - Send To Address** field.

    For Brocade E-mail Call Home centers, enter **callhomeemail@brocade.com**.

17. Click **Send Test** to test the mail server.

    The selected Call Home center must be enabled to test the mail server.

    A faked event is generated and sent to the selected Call Home center. You must contact the Call Home center to verify that the event was received and in the correct format. To see the content included in an e-mail message, refer to "Call Home alert e-mail messages" on page 352.

18. Click **OK** to close the "Test Event Sent" message.

19. Click **OK**.

    The **Call Home** dialog box displays with the Call Home center you edited highlighted in the **Call Home Centers** list.

20. Click **OK** to close the **Call Home** dialog box.

Call Home alert e-mail messages

When an event triggers a Call Home alert, an e-mail message is sent to the selected Call Home center. The e-mail message includes the following information:

- E-mail subject line — [*Severity* - *Event_Reason_Code* - *FRU_Code* or *Event_Type* - *Factory_Serial_Number*] Call Home Alert about product *IP_Address* with support save information

  A pontential e-mail subject line is shown in the following example:

  [3 - 1427 - FW-1427 - AMH0344D006] Call Home Alert about product 172.26.24.85 with support save information

- E-mail content — Provides the following information about the triggered event:
  - Event Description — Details about the event that triggered the alert. Includes the following data:
    - Product WWN
    - Product IP address
    - Time
    - SupportSave location
  - Management Server Information — Details about the Management server. Includes the following data:
    - Server Name
    - Server IP
    - Server Version
  - Contact Information — Customer contact information. Includes the following data:
    - Customer Name
    - Contact Name
    - Phone 1
    - Phone 2

- Source — Details about the product. Includes the following data:
  - Firmware Version
  - Supplier Serial number
  - Factory Serial number
  - IP Address
  - Model number
  - Type
  - Product Name
  - Product WWN
  - Ethernet IP
  - Ethernet IP Mask
  - FCIP
  - FCIP Mask
  - Product Type
  - Domain ID
  - Product Manufacturer
  - Product Type Number
  - Manufacturing Plant
  - Product Status
  - Status Reason
- Event — Details about the triggered event. Includes the following data:
  - Event Time
  - Event Severity
  - Event Reason Code
  - FRU Code/Event Type
  - Event Description
- Event Data — Information about the triggered event. Includes the following data:
  - Event level
  - Event number
  - Event count
  - Event time
  - Event Message Id
  - Event Description
- Last 30 Events on the Product (Brocade E-mail and NetApp E-mail only) — Table with the last 30 product and product status events. The first event is always the event that triggered the e-mail alert. Includes the following data for each event:
  - Event level
  - Event number
  - Count
  - Time
  - Message ID
  - Description

Editing the EMC Call Home center

To edit an EMC Call Home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Select the **EMC** Call Home center you want to edit in the **Call Home Centers** list.
3. Click **Edit Centers** (beneath the **Call Home Centers** list).

   The **Configure Call Home Center** dialog box displays (Figure 139).

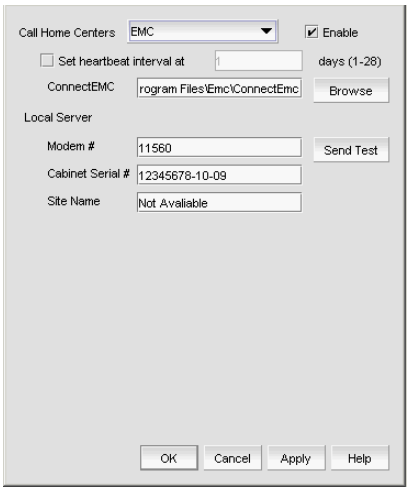


FIGURE 139 Configure Call Home Center dialog box (EMC option)

4. Make sure the **EMC** Call Home center type displays in the **Call Home Centers** list.

   If the Call Home center type is incorrect, select the correct type from the list.

5. Select the **Enable** check box to enable this Call Home center.
6. Set the time interval at which to check the Call Home center by selecting the **Set heartbeat interval at ___ days (1-28)** check box and entering the interval in the field.
7. Enter the path to the ConnectEMC application in the **ConnectEMC** field or browse to the ConnectEMC application location.
8. Enter the phone number or extension of the local server in the **Local Server - Modem #** field.
9. Enter the identification number of the local server in the **Local Server - Cabinet Serial #** field.
10. Enter the site name for the local server in the **Local Server - Site Name** field.
11. Click **Send Test** to test the Connect EMC application.

    The selected Call Home center must be enabled to test the ConnectEMC application.

    A faked event is generated and sent to the selected Call Home center. You must contact the Call Home center to verify that the event was received and in the correct format.

12. Click **OK** to close the “Test Event Sent” message.

13. Click **OK**.

    The **Call Home** dialog box displays with the Call Home center you edited highlighted in the **Call Home Centers** list.

14. Click **OK** to close the **Call Home** dialog box.

Editing the HP LAN Call Home center

To edit an HP LAN Call Home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Select the **HP LAN** Call Home center you want to edit in the **Call Home Centers** list.
3. Click **Edit Centers** (beneath the **Call Home Centers** list).

   The **Configure Call Home Center** dialog box displays (Figure 140).

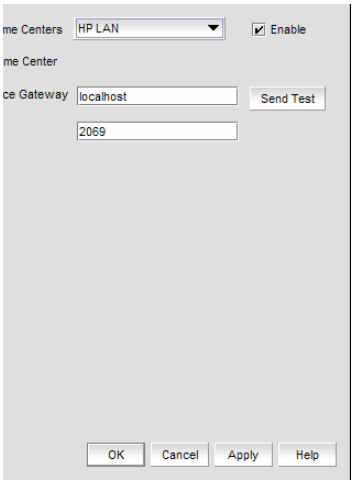


FIGURE 140 Configure Call Home Center dialog box (HP LAN option)

4. Make sure the **HP LAN** Call Home center type displays in the **Call Home Centers** list.

   If the Call Home center type is incorrect, select the correct type from the list.

5. Select the **Enable** check box to enable this Call Home center.
6. Enter the IP address of the Call Home center in the **Service Gateway** field.

The default is 2069.

7. Enter the port number of the Call Home center in the **Port** field.

8. Click **Send Test** to test the address.

   The selected Call Home center must be enabled to test the IP address.

   A faked event is generated and sent to the selected Call Home center. You must contact the Call Home center to verify that the event was received and in the correct format.

   NOTE
   The HP LAN Call Home alert displays the directory separation characters with a double backslash (\\) instead of a single backslash (\).

9. Click **OK** to close the "Test Event Sent" message.
10. Click **OK**.

    The **Call Home** dialog box displays with the Call Home center you edited highlighted in the **Call Home Centers** list.

11. Click **OK** to close the **Call Home** dialog box.

Enabling a Call Home center

To enable a Call Home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Select the **Enable** check box of the Call Home center you want to enable in the **Call Home Centers** list.
3. Click **OK** to close the **Call Home** dialog box.

Enabling supportSave

NOTE
SupportSave is only supported on products running Fabric OS 5.2 or later or Network OS 2.1.X or later.

When you enable supportSave through the Call Home center, all Call Home events trigger the supportSave operation and the supportSave stored location on the FTP server is transmitted with the Call Home event.

To enable a supportSave for a Call Home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Select the **Support Save** check box of the Call Home center or device for which you want to enable supportSave in the **Call Home Centers** list.
3. Click **OK** to close the **Call Home** dialog box.

Testing the Call Home center connection

Once you add and enable a Call Home center, you should verify that Call Home is functional.

To verify Call Home center functionality, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.
2. Click **Edit Centers** (beneath the **Call Home Centers** list).

   The **Configure Call Home Center** dialog box displays.
3. Select the Call Home center you want to check in the **Call Home Centers** list.
4. Make sure that the **Enabled** check box is selected.

   NOTE
   You must configure the Call Home center before you test the connection. To configure a Call Home center, refer to "Editing a Call Home center" on page 349.
5. Click **Send Test**.

   A faked event is generated and sent to the selected Call Home center. You must contact the Call Home center to verify that the event was received and in the correct format.
6. Click **OK** to close the "Test Event Sent" message.
7. Click **OK** to close the **Configure Call Home Center** dialog box.
8. Click **OK** to close the **Call Home** dialog box.

Disabling a Call Home center

When a Call Home center is disabled, no devices can send Call Home events to the Call Home center. However, the devices and event filters assigned to the disabled Call Home center are not removed. You can still perform the following actions on a disabled Call Home center:

- Edit Call Home center configuration.
- Add devices and event filters to the Call Home center.

To disable a Call Home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.
2. Clear the **Enable** check box of the Call Home center you want to disable in the **Call Home Centers** list.

   The selected Call Home center and its devices and event filters become unavailable. However, the Call Home center is not disabled until you save your changes. When a device is assigned to the Call Home center, a confirmation message displays.
3. Click **OK** to confirm.
4. Click **OK** to close the **Call Home** dialog box.

Viewing Call Home status

You can view Call Home status from the main Management application window or from the **Call Home Notification** dialog box.

The Management application enables you to view the Call Home status at a glance by providing a Call Home status icon on the status bar. Table 37 illustrates and describes the icons that indicate the current status of the Call Home function.

TABLE 37 Call Home icons

Icon	Description
	Normal — Displays when Call Home is enabled on all devices and no filters are applied.
	Degraded — Displays when Call Home is enabled on all devices and at least one filter is active.
	Disabled — Displays when any of the following conditions are met: • At least one device's Call Home is disabled. • At least one non-manageable device. • At least one device does not have the Management server registered as a trap recipient.

To view more detail regarding Call Home status, click the **Call Home** icon. The **Call Home Notification** dialog box displays the following information for the list of devices that have assigned filters or Call Home disabled:

- **Product** — The name of the device. Click to go to the device in the topology.
- **IP Address** — The IP address (IPv4 or IPv6 format) of the device.
- **Status** — The status of the device. The possible status options include:
  - **Enabled** — The device is manageable, Call Home is enabled, and a filter is applied.
  - **Disabled** — Call Home is disabled on at least one device or Call Home is disabled from the **Call Home** dialog box.
  - **Not Manageable** — Manageability is lost.
  - **Server Not Registered** — The server is not registered to receive Call Home events from this device.

NOTE
Call Home status only displays for Fabric OS, IronWare, and Network OS products.

- **Filter** — The name of the active event filter assigned to the device.
- **Call Home** button — Click to launch the **Call Home** dialog box, where you can configure Call Home centers.

Assigning a device to the Call Home center

Discovered devices (switches, routers, and directors) are not assigned to a corresponding Call Home center automatically. You must manually assign each device to a Call Home center before you use Call Home.

To assign a device or multiple devices to a Call Home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Select the devices you want to assign to a Call Home center in the **Products List**.
3. Select the Call Home center to which you want to assign the devices in the **Call Home Centers** list.

   You can only assign a device to one Call Home center at a time.

4. Click the right arrow button.

   The selected devices display beneath the selected Call Home center. Devices assigned to a Call Home center do not display in the **Products List**.

5. Click **OK** to close the **Call Home** dialog box.

Removing a device from a Call Home center

To remove a device or multiple devices from a Call Home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Select the Call Home center from which you want to remove devices in the **Call Home Centers** list.
3. Select the devices you want to remove from the selected Call Home center.
4. Click the left arrow button.

   A confirmation message displays.

5. Click **OK**.

   The selected devices are removed from the Call Home center and display in the **Products List**.

6. Click **OK** to close the **Call Home** dialog box.

Removing all devices and filters from a Call Home center

To remove all devices and filters from a Call Home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Select the Call Home center from which you want to remove devices and filters in the **Call Home Centers** list.

3. Click the left arrow button.

   A confirmation message displays.

4. Click **OK**.

   All devices assigned to the selected Call Home center display in the **Products List**. Any assigned filters are also removed.

5. Click **OK** to close the **Call Home** dialog box.

Defining an event filter

To define an event filter, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Click **Add** beneath the **Call Home Event Filter** list.

   The **Call Home Event Filter** dialog box displays.

3. Enter a name for the filter in the **Name** field.

4. Enter a name for the description in the **Description** field.

5. Select the check box for the events you want to include in the filter in the **Available Call Home Event Types** list.

   To exclude the event, clear the check box. By default, all check boxes are selected during a new installation. Click **Select All** to select all event types in the list or select **Unselect All** to clear the selected event types in the list. For more information about Call Home events, refer to Appendix B, "Call Home Event Tables".

   The **Available Call Home Event Types** list displays the following information:

   - **Description —** The description of the event.
   - **Type** — The type of firmware for the selected event.
   - **FRU Code/Event Type —** The field-replaceable unit (FRU) code and event type for the event.
   - **Severity —** The severity of the event.
   - **Event Reason Code —** The event reason code of the event.

6. Click **OK** on the **Call Home Event Filter** dialog box.

   The event filter name and the description are displayed in the **Call Home** dialog box.

   To assign event filters to a Call Home center or a device, refer to "Assigning an event filter to a Call Home center" on page 361 or "Assigning an event filter to a device" on page 361.

7. Click **OK** to close the **Call Home** dialog box.

Assigning an event filter to a Call Home center

Event filters allow Call Home center users to log in to a Management server and assign specific event filters to the devices. This limits the number of unnecessary or "acknowledge" events and improves the performance and effectiveness of the Call Home center.

You can only select one event filter at a time; however, you can assign the same event filter to multiple devices or Call Home centers. When you assign an event filter to a Call Home center, the event filter is assigned to all devices in the Call Home center. For more information about Call Home events, refer to Appendix B, "Call Home Event Tables".

NOTE
You cannot assign an event filter to a Call Home center that does not contain devices.

To assign an event filter to a Call Home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Select the event filters you want to assign in the **Call Home Event Filters** list.
3. Select the Call Home centers to which you want to assign the event filters in the **Call Home Centers** list.
4. Click the right arrow button.

   The selected event filters are assigned to the selected Call Home centers.

5. Click **OK** to close the **Call Home** dialog box.

Assigning an event filter to a device

To assign an event filter to a device, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Select the event filter you want to assign in the **Call Home Event Filters** list.

   For more information about Call Home events, refer to Appendix B, "Call Home Event Tables".

3. Select one or more devices to which you want to assign the event filter in the **Call Home Centers** list.
4. Click the right arrow button.

   The selected event filter is assigned to the selected devices. The event filter displays beneath the specified device or all of the devices under the specified Call Home center.

5. Click **OK** to close the **Call Home** dialog box.

Overwriting an assigned event filter

A device can only have one event filter at a time; therefore, when a new filter is applied to a device that already has a filter, you must confirm the new filter assignment.

To overwrite an event filter, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Select the event filter you want to apply in the **Call Home Event Filters** list.

   For more information about Call Home events, refer to Appendix B, “Call Home Event Tables”.

3. Select the devices to which you want to apply the event filter in the **Call Home Centers** list.

4. Click the right arrow button.

   For existing event filters, a confirmation messages displays.

5. Click **Yes**.

   The selected event filter is applied to the selected devices. The event filter displays beneath the specified device or all of the devices under the specified Call Home center.

6. Click **OK** to close the **Call Home** dialog box.

Removing all event filter from a Call Home center

To remove all event filters from a Call Home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Choose one of the following options in the **Call Home Centers** list:

   - Right-click a Call Home center and select **Remove Filters**.
   - Select a Call Home center and click the left arrow button.

     All event filters assigned to the Call Home center are removed.

3. Click **OK** to close the **Call Home** dialog box.

Removing an event filter from a device

To remove an event filter from a device, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Choose one of the following options in the **Call Home Centers** list:

   - Right-click a device to which the event filter is assigned and select **Remove Filter**.
   - Select an event filter assigned to a device and click the left arrow button. Press **CTRL** and click to select multiple event filters assigned to multiple devices.

   All event filters assigned to the device are removed.

3. Click **OK** to close the **Call Home** dialog box.

Removing an event filter from the Call Home Event Filters list

To remove an event filter from the Call Home Event Filters list, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Select the event filter you want to remove in the **Call Home Event Filters** list.

3. Click **Remove**.

   - If the event filter is not assigned to any devices, a confirmation message displays asking if you want to remove the event filter. Click **Yes**.
   - If the event filter is assigned to any devices, a confirmation message displays informing you that removing this event filter will remove it from all associated devices. Click **Yes**.

   The event filter is removed from any associated devices and the **Call Home Event Filters** list.

   To determine to which devices the event filter is assigned, select the event filter and then click the **Find** button (>).

4. Click **OK** to close the **Call Home** dialog box.

Searching for an assigned event filter

To find all devices to which an event filter is assigned, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Select the event filter you want to find in the **Call Home Event Filters** list.

3. Click the **Find** button (**>**).

   All instances of the event filter are highlighted in the **Call Home Centers** list.

   If the selected event filter is not assigned to any devices in the **Call Home Centers** list, a not found message displays.

Chapter

11

Third-party tools

In this chapter

About third-party tools

NOTE
Installing tools is only available with the Trial and Licensed version versions.

You can open other software products (such as, Firefox, Windows Explorer, Web Tools, Element Managers, FCR Configuration, HCM Agent and so on) you frequently use from the **Tools** menu or shortcut menus.

You can add third-party tools to the **Tools** menu or shortcut menus to open other software products (such as, Firefox, Windows Explorer, Web Tools, Element Managers, FCR Configuration, HCM Agent and so on) you frequently use.

Starting third-party tools from the application

You can open third-party tools from the **Tools** menu or a device's shortcut menu. Remember that you cannot open a tool that is not installed on your computer. You must install the tool on your computer and add the tool to the **Tools** menu or the device's shortcut menu.

NOTE
Installing tools is only available with the Trial and Licensed version versions.

To open an application, complete the following steps.

1. Select the device.
2. Use one of the following techniques:
   - Select **Tools > Product Menu >** *Tool_Name*.
   - Select **Tools >** *Tool_Name*.
   - Right-click the device, and select the tool from the menu.

     If the third-party tool is a web-based application, you must enter the IP address of the applications server as a parameter to be able to open the application. For step-by-step instructions about entering the IP address of the server, refer to "Entering the server IP address of a tool" on page 368.

Launching a Telnet session

You can use Telnet to log in and issue command line-based commands to a device.

NOTE
The device must have a valid IP address. If the device does not have a valid IP address, the Telnet selection will not be available on the shortcut menu. You must right-click the device icon, select **Properties,** and enter the device's IP address before you can open a Telnet session.

Launching an Telnet session from the IP tab

To launch a telnet session, complete the following steps.

On the Topology Map, right-click a device and select **CLI through Server**.

Launching an Element Manager

Element Managers are used to manage Fibre Channel switches and directors. You can open a device's Element Manager directly from the application.

To launch a device's Element Manager, complete the following steps.

On the Connectivity Map, double-click the device you want to manage.

The Element Manager displays.

OR

On the Connectivity Map, right-click the device you want to manage and select **Element Manager > Hardware**.

The Element Manager displays.

OR

1. Select a device.
2. Select **Configure > Element Manager > Hardware**.

   The Element Manager displays.

OR

1. Select a device.
2. Click the Element Manager icon on the toolbar.

   The Element Manager displays.

Launching HCM Agent

Use Fabric OS HCM Agent to enable and manage Fabric OS HBAs. You can open HCM Agent directly from the application. For more information about HCM Agent, refer to the *HCM Agent Administrator's Guide.* For more information about Fabric OS HBAs, refer to the documentation for the specific device.

To launch a Fabric OS HBA's Element Manager, complete the following steps.

NOTE
You must have Element Manager - Product Administration privileges for the selected device to launch HCM Agent. If you do not have Element Manager - Product Administration privileges, you will need to enter those credentials to launch HCM Agent. For more information about privileges, refer to "User Privileges" on page 1283.

On the Connectivity Map, double-click the Fabric OS HBA or CNA device you want to manage.

HCM Agent displays.

OR

On the Connectivity Map, right-click the Fabric OS HBA or CNA device you want to manage and select **Element Manager**.

HCM Agent displays.

OR

1. Select a Fabric OS HBA or CNA.
2. Select **Configure > Element Manager > HCM**.

   HCM Agent displays.

Adding a tool

You can specify third-party tools so they appear on the **Setup Tools** dialog box. From there, you can add them to the **Tools** menu and then open the tools directly from the Management application.

To add a tool, complete the following steps.

1. Select **Tools > Setup**.

   The **Setup Tools** dialog box displays.
2. Click the **Tools Menu** tab.
3. Click **Define**.

   The **Define Tools** dialog box displays (Figure 141).

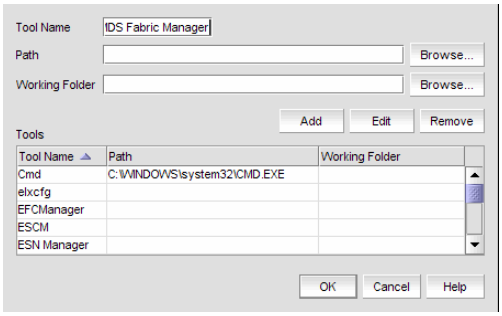


FIGURE 141 Define Tools dialog box

4. Type the tool's name in the **Tool Name** field as you want it to appear on the **Tools** menu.
5. Type or browse to the path of the executable file in the **Path** field.
6. Type or browse to the path of the folder that you want to set as your working folder in the **Working Folder** field.
7. Click **Add** to add the tool.

   The **Setup Tools** dialog box displays with the new tool added to the **Tools Menu Item** table.

   NOTE
   You must click **Add** before clicking **OK**; otherwise, your changes will be lost.

8. Click **OK** to save your work and close the **Define Tools** dialog box.

   To add this tool to the **Tools** menu, refer to "Adding an option to the Tools menu" on page 369.
9. Click **OK** to save your work and close the **Setup Tools** dialog box.

Entering the server IP address of a tool

If the third-party tool is a web-based application, you must enter the IP address of the applications server as a parameter to be able to open the application.

To enter the server IP address, complete the following steps.

1. Select **Tools > Setup**.

   The **Setup Tools** dialog box displays.
2. Click the **Tools Menu** tab.

   The **Tool Menu Items** table displays all configured tools, including the tool name as it displays on the **Tools** menu, parameters, and keystroke shortcuts.
3. Select the tool you want to edit in the **Tool Menu Items** table.

   The settings for the selected tool display in the fields at the top of the dialog box.
4. Edit the IP address of the server (for example, `http://`*IP_Address* or `http://`*IP_Address*`:`*Port_Number*) in the **Parameters** field.
5. Click **Edit**.

NOTE
You must click **Edit** before clicking **OK**; otherwise, your changes will be lost.

6. Click **OK** to save your work and close the **Setup Tools** dialog box.

Adding an option to the Tools menu

You can add third-party tools to the **Tools** menu which enables you to launch tools directly from the application.

To add a option to the tools menu, complete the following steps.

1. Select **Tools > Setup**.

   The **Setup Tools** dialog box displays.

2. Click the **Tools Menu** tab.

   The **Tool Menu Items** table displays all configured tools, including the tool name as it displays on the **Tools** menu, parameters, and keystroke shortcuts (Figure 142).

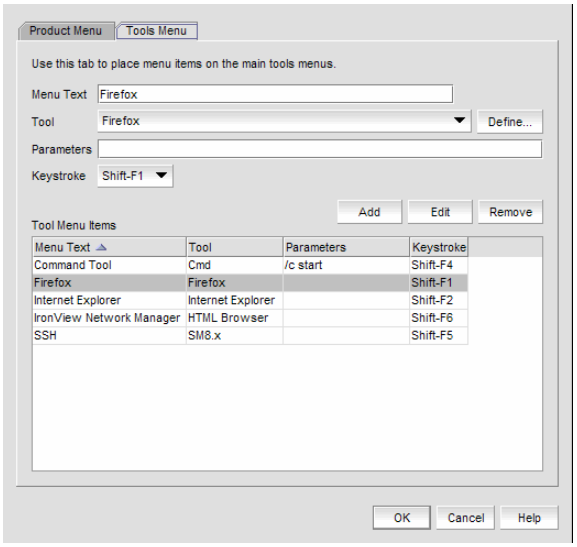


FIGURE 142 Setup Tools dialog box (Tools menu tab)

3. Type a label for the option as you want it to appear on the **Tools** menu in the **Menu Text** field.
4. Select the application from the **Tool** list, or click **Define** if you want to specify a new tool.

   To specify a new tool, refer to "Adding a tool" on page 367.

5. (Optional) Enter parameters, such as a URL, in the **Parameters** field.
6. (Optional) Select a keyboard shortcut in the **Keystroke** list.

NOTE
You cannot assign the same keyboard shortcut to two different tools.

7. Click **Add**.

The new tool displays in the **Tool Menu Items** table.

NOTE
You must click **Add** before clicking **OK**; otherwise, the new menu option is not created.

8. Click **OK** to save your work and close the **Setup Tools** dialog box.

   The tool you configured now displays on the **Tools** menu.

Changing an option on the Tools menu

You can edit parameters for third-party tools that display on the **Tools** menu.

To edit a option to the tools menu, complete the following steps.

1. Select **Tools > Setup**.

   The **Setup Tools** dialog box displays.

2. Click the **Tools Menu** tab.

   The **Tool Menu Items** table displays all configured tools, including the tool name as it displays on the **Tools** menu, parameters, and keystroke shortcuts.

3. Select the tool you want to edit in the **Tool Menu Items** table.

   The settings for the selected tool display in the fields at the top of the dialog box.

4. Edit the label for the option as you want it to appear on the **Tools** menu in the **Menu Text** field.
5. Select the application from the **Tool** list.
6. Edit the parameters, such as a URL, in the **Parameters** field.
7. Select a new keyboard shortcut in the **Keystroke** list.
8. Click **Edit**.

NOTE
You must click **Edit** before clicking **OK**; otherwise, your changes will be lost.

9. Click **OK** to save your work and close the **Setup Tools** dialog box.

Removing an option from the Tools menu

You can remove a tool from the third-party tool list.

To remove a option to the tools menu, complete the following steps.

1. Select **Tools > Setup**.

   The **Setup Tools** dialog box displays.

2. Click the **Tools Menu** tab.
3. Select the row of the tool you want to remove in the **Tools Menu Items** table.
4. Click **Remove**.

If the tool is not being utilized, no confirmation message displays.

5. Click **Update** to remove the tool.
6. Click **OK** to save your work and close the **Setup Tools** dialog box.

Adding an option to a device's shortcut menu

You can add an option to a device's shortcut menu.

To add an option to the device's shortcut menu, complete the following steps.

1. Select **Tools > Setup**.

   The **Setup Tools** dialog box displays.

2. Click the **Product Menu** tab.

   The **Product Popup Menu Items** table displays all configured shortcut menu options.

3. Type or select the text in the **Menu Text** list as you want it to appear on the menu.
4. Choose one of the following options:
   - To display the menu option only for devices that meet the conditions listed, select the **Match Conditions** option.
   - To display the menu option on the shortcut menus for all devices, select the **All** option.

     If you select **All**, skip to step 8. Otherwise, continue to step 5.
5. Select the appropriate type in the **Condition 1 Property** name list.
6. Enter the appropriate value for the selected property in the **Condition 1 Value** field.
7. (Optional) Select the **Condition 2 Property** type and enter the **Value** for that property type (Condition 1 AND Condition 2 must be true) to define a second condition to be simultaneously true.

   NOTE
   To set up a condition where Condition 1 OR Condition 2 must be true, define two menu items, one for each condition.

8. Select the tool that you want to launch from the **Tool** list, or click **Define** to add a tool.

   To specify a new tool, refer to "Adding a tool" on page 367.

9. Select the **Append device ID** check box to specify the parameter used when opening the tool.
   - To specify that the device's IP address should be used when opening the tool, select the **IP Address** option.
   - To specify that the device's Node WWN should be used when opening the tool, select the **Node WWN** option.
10. Click **Add** to add the new menu item.

    It displays in the **Product Popup Menu Items** table.

    NOTE
    You must click **Add** before clicking **OK**; otherwise, your changes will be lost.

11. Click **OK** to save your work and close the **Setup Tools** dialog box.

Changing an option on a device's shortcut menu

You can change the parameters for a tool that displays on a device's shortcut menu.

To edit an option to the device's shortcut menu, complete the following steps.

1. Select **Tools > Setup**.

   The **Setup Tools** dialog box displays.

2. Click the **Product Menu** tab.

   The **Product Popup Menu Items** table displays all configured shortcut menu options.

3. Select the menu item you want to change in the **Product Popup Menu Items** table.

   The settings for the selected menu item display in the fields at the top of the dialog box.

4. Edit or select the text in the **Menu Text** list as you want it to appear on the menu.

5. Choose one of the following options:

   - To display the menu option only for devices that meet the conditions listed, select the **Match Conditions** option.
   - To display the menu option on the shortcut menus for all devices, select the **All** option.

     If you select **All**, skip to step 8. Otherwise, continue to step 5.

6. Change the type in the **Condition 1 Property** name list.

7. Change the value for the selected property in the **Condition 1 Value** field.

8. (Optional) Change the **Condition 2 Property** type or edit the **Value** for that property type (Condition 1 AND Condition 2 must be true) to edit a second condition to be simultaneously true.

   NOTE
   To set up a condition where Condition 1 OR Condition 2 must be true, define two menu items, one for each condition.

9. Select the tool from the **Tool** list that you want to launch, or click **Define** to add a tool.

   To specify a new tool, refer to "Adding a tool" on page 367.

10. Select the **Append device ID** check box to specify the parameter used when opening the tool.

    - To specify that the device's IP address should be used when opening the tool, select the **IP Address** option.
    - To specify that the device's Node WWN should be used when opening the tool, select the **Node WWN** option.

11. Click **Edit**.

    NOTE
    You must click **Edit** before clicking **OK**; otherwise, your changes will be lost.

12. Click **OK** to save your work and close the **Setup Tools** dialog box.

Removing an option from a device's shortcut menu

You can remove a tool that displays on a device's shortcut menu.

To remove an option to the device's shortcut menu, complete the following steps.

1. Select **Tools > Setup**.

   The **Setup Tools** dialog box displays.

2. Click the **Product Menu** tab.

   The **Product Popup Menu Items** table displays all configured menu options.

3. Select the menu item you want to remove in the **Product Popup Menu Items** table.
4. Click **Remove**.
5. Click **OK** to save your work and close the **Setup Tools** dialog box.

Chapter

12

Server Management Console

In this chapter

Server Management Console overview

The Server Management Console (SMC) is an automatically installed, stand-alone application for managing the Management application server. You can perform the following tasks using the SMC:

- From the Services tab, you can start, stop, refresh, and restart services on the server.
- From the Ports tab, you can view the Management application server or web server port number.
- From the AAA Settings tab (Enterprise Licensed version only), you can configure an authentication server (LDAP or Radius server), and establish authentication policies.
- From the Restore tab, you can restore server application data.
- From the Technical Support Information tab, you can collect information for technical support.
- From the HCM Upgrade tab, you can upgrade the Management application to use a new version of Host Connectivity Manager (HCM).
- From the SMI Agent Configuration Tool tool, you can configure the SMI Agent settings, such as security, CIMOM, and certificate management as well as launch Management application dialog boxes.

Launching the SMC on Windows

Open the **Server Management Console** from the **Start** menu on the Management application server.

You can also drag the SMC icon onto your desktop as a short cut.

Launching the SMC on Linux

NOTE
The Server Management Console is a graphical user interface and should be launched from the XConsole on Linux systems.

Perform the following steps to launch the Server Management Console on Linux systems.

1. On the Management application server, go to the following directory:

   Install_Directory/bin

2. Type the following at the command line:

```
./smc
OR
sh smc
```

Services tab

You must be logged in at the administrator (Windows systems) or root (UNIX systems) level to stop, start, and restart the Management application services. Stopping and restarting the Management application services causes clients connected to the server to lose connection, and they must re-log in to the server.

Monitoring and managing Management application services

To monitor the status of the Management application services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab (Figure 143).

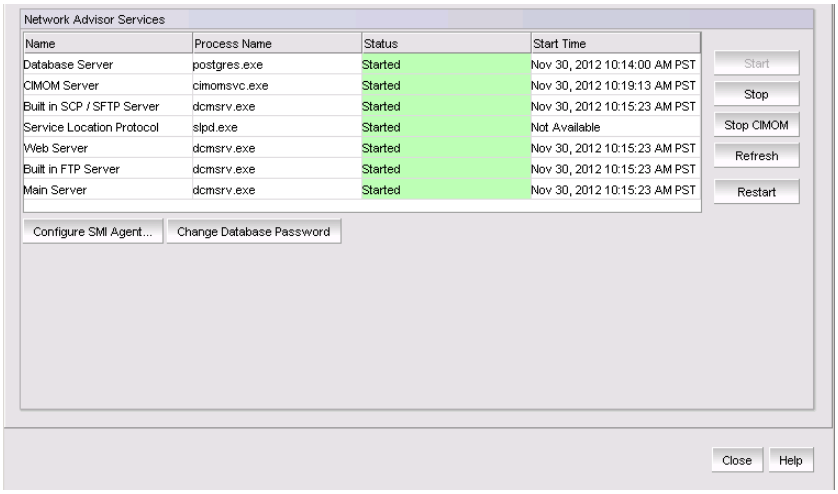


FIGURE 143 Services tab

3. Review the following information for each available service.
    - **Name** — The name of the server; for example, FTP Server or Database Server.
    - **Process Name** — The name of the process; for example, postgres.exe (Database Server).
    - **Status** — The status of the service; for example, started or stopped.
    - **Start Time** — The date and time the service started. The Start Time for Service Location Protocol displays as 'Not Available'.
4. Click **Close** to close the Server Management Console.

Refreshing the server status

To refresh the server status for each of the Management application services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab.
3. Click **Refresh** to update the table with the latest status of the services in case the services were stopped or restarted outside of the Server Management Console.
4. Click **Close** to close the Server Management Console.

Stopping all services

To stop all services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab.
3. Click **Stop** to stop all services.

    Note that clicking **Restart** stops and then restarts all services.
4. Click **Close** to close the Server Management Console.

Stopping the CIMOM services

To stop the CIMOM (Common Information Model Object Manager) services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab.
3. Click **Stop CIMOM**.
4. Click **Close** to close the Server Management Console.

Starting all services

NOTE
The **Start** button restarts running services in addition to starting stopped services which causes client-server disconnect.

To start all services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab.
3. Click **Start** to start all services.

   NOTE
   If the server is configured to use an external FTP server, the Server Management Console does not attempt to start the built-in FTP service.

4. Click **Close** to close the Server Management Console.

Restarting all services

To stop and restart all services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab.
3. Click **Restart** to stop then restart all services.

   NOTE
   If the server is configured to use an external FTP server, the Server Management Console does not attempt to start the built-in FTP service.

4. Click **Close** to close the Server Management Console.

Changing the database password

Requires User Management read and write privilege.

1. Launch the Server Management Console.
2. Click the **Services** tab.
3. Click **Change Database Password**.

   The authentication **Login** dialog box displays.

4. Enter your Management application user name and password.
5. Click **OK**.

   The **Database Password** dialog box displays.

6. Select the database user name for which you want to change the password in the **User Name** field.

   Options include dcmadmin and dcmuser.

   Changing the dcmadmin password requires all Management application services, except for the database server, to be stopped and then re-started.

   Changing the dcmuser password requires all ODBC remote client sessions to be restarted.
7. Enter your current password in the **Old Password** field.
8. Enter you new password in the **New Password** and **Confirm New Password** fields.
9. Click **OK**.
10. Click **Yes** on the warning message.

Ports tab

Use the **Ports** tab of the Server Management Console to view the Management application server and Web server port numbers. The default Web Server port number is 80 (HTTP) or 443 (HTTPS). The Management application server default port number is 24600.

Viewing server port numbers

To view the Management application server or web server port number, complete the following steps.

1. Choose one of the following options:
   - For Windows systems, open the **Server Management Console** from the **Start** menu on the Management application server.
   - For Linux systems, on the Management application server, go to the *Install_Directory*/bin directory and type the following at the command line:

     ```
     ./smc
     OR
     sh smc
     ```
2. Click the **Ports** tab.
3. Review the following information for each available service.
   - *Management_Application_Name* **Server Port** text box — The Management application Server Port number. The default is 24600.
   - **Web Server Port # (HTTPS)** text box — The Web Server Port number for HTTPS. The default is 443.

     You can configure the server port settings from the **Options** dialog box (**Server Port** pane). For instructions, refer to "Configuring the server port" on page 177.

     You can also configure the server port settings from the configuration wizard. For instructions, refer to "Launching the Configuration Wizard" on page 5.
4. Click **Close** to close the Server Management Console.

AAA Settings tab

Authentication enables you to configure an authentication server and establish authentication policies. You can configure the Management application to authenticate users against the local database (Management application server), an external server (RADIUS, LDAP, CAC or TACACS+), or a switch. Authentication is configured to the local database by default. When you use an external server, the Management application sends the login information to the external server to make sure the name and password are valid.

If you configure primary authentication to an external or switch authentication, you can also configure secondary authentication to the local server. When you log in to the Management application, if the primary server is unavailable, the Management application attempts with the next configured primary server. If all primary servers are unavailable, then the Management application falls back to the secondary authentication. Fall back can occur when the server is unavailable, authentication fails, or the user is not found.

Configuring Radius server authentication

If you are using a Radius server for authentication, make the following preparations first:

- Make sure that the server you want to use is on the network that the Management application manages.
- Make sure that the external server and its user accounts have been properly configured. For example, you must define roles and areas of responsibility (AOR) in the external server to match the Management application roles and AOR.
- Select an **Authentication Type** (you will be prompted to provide a type in the **Add or Edit Radius Server** dialog box). The **Authentication Type** is the authentication policy you choose for handling authentication. The options are PAP and CHAP.
  - PAP, password protected protocol, is based on password verification. Passwords are not encrypted, and are not secure from eavesdroppers during transmission.
  - CHAP, challenge handshake protocol, uses a three-way handshake method of verification based on a shared secret. If you are using CHAP, have the shared secret available to you. You will need to type it in as a configuration parameter.
- Know the Shared Secret.
- Have the IP address of the server available.
- Know the TCP port you are using and make sure it is open in the firewall. For Radius servers, ports 1812 or 1813 (actually UDP ports) are commonly used. Some older Radius server use 1645 or 1646 instead of 1812 and 1813; check with the Radius server vendor if you are not sure which port to specify.
- Know how long you want to wait between attempts to reach the server if it is busy. This is expressed as a timeout value (default is 3 seconds) in seconds. Values are between 1 and 15.
- Determine how many attempts (default is 3 times) to make to reach the server before stopping and assuming it is unreachable. Values are between 1 and 5.
- If possible, establish an active connection with the Radius server before configuration. This enables you to test the connection as part of the configuration procedure.

1. Select the **AAA Settings** tab.
2. Select **Radius Server** from the **Primary Authentication** list.

3. Add or edit a Radius server by referring to "Configuring a Radius server" on page 381.
4. Rearrange the Radius servers in the table by selecting a server and click the **Up** or **Down** button to move it.
5. Delete a Radius server by selecting the server and click **Delete**.
6. Test the established active connection with the Radius server by clicking **Test**.

   Test attempts to contact the Radius server by issuing a **ping** command.
7. Set secondary authentication by selecting one of the following options from the **Secondary Authentication** list:
   - **Local Database**
   - None
8. Set the fall back condition to secondary authentication by selecting one of the following options from the **Fail Over Option** list:
   - Radius Servers Not Reachable
   - Radius Authentication Failed
9. Set the authorization preference by selecting one of the following options from the **Authorization Preference** list:
   - Local Database
   - Primary Authentication Server
10. Click **Apply** to save the configuration.

    To display the authentication audit trail, refer to "Displaying the client authentication audit trail" on page 391.
11. Click **Close** to close the Server Management Console.

Configuring a Radius server

To add or edit a Radius server, complete the following steps.

1. Choose one of the following options from the **AAA Settings** tab:
   - Click **Add**.
   - Select an existing Radius server and click **Edit**.

     The **Add or Edit Radius Server** dialog box displays (Figure 144).

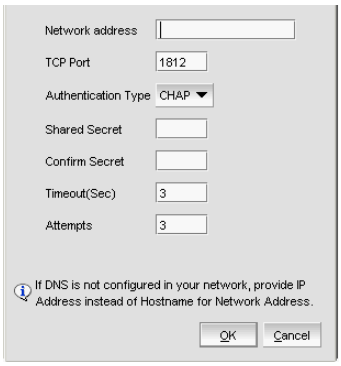


FIGURE 144 Add or Edit Radius Server

2. Enter the radius server's IP address in the **IP Address** field.
3. Enter the TCP port, if necessary, used by the Radius server in the **TCP Port** field.

   Default is 1812.
4. Select the authentication policy (PAP or CHAP) from the **Authentication Type** field.

   Default is CHAP.
5. Enter the shared secret in the **Shared Secret** and **Confirm Secret** fields.
6. Enter the timeout timer value (in seconds) that specifies the amount of time to wait between retries when the server is busy in the **Timeout (Sec)** field.

   Default is 3 seconds.
7. Enter the number of attempts to be made to reach a server before assuming it is unreachable in the **Attempts** field.

   Default is 3 attempts.
8. Click **OK** to return to the **AAA Settings** tab.

   The **Radius Servers and Sequence** table displays the following information:

   - **Network Address** — The network address of the Radius server.
   - **Authentication Type** — The authentication type (such as, CHAP).
   - **TCP Port** — The TCP port number of the Radius server.
   - **TimeOut (Sec)** — The timeout value in seconds specified when sending an authentication request to the server. Default is 3.
   - **Attempts** — The number of attempts made to reach a server before determining it is unreachable. Default is 3.

Configuring LDAP server authentication

NOTE
You cannot configure multiple Active Directory groups (domains) for the LDAP server.

NOTE
You cannot enter *Domain\User_Name* in the Management application dialog box for LDAP server authentication.

If you are using an LDAP server for authentication, make the following preparations first:

- Make sure that the LDAP server you want to use is on the network that the Management application manages.
- Have the IP address of the server available.
- Know the TCP port you are using. The LDAP server uses Transport Layer Security (TLS). LDAP over TLS generally uses port 389. If security is enabled the port number is 636. Check with the LDAP server administrator if you are not sure which port to specify.
- Know how long you want to wait between attempts (default is 3 seconds) to reach the server if it is busy. This is expressed as a timeout value in seconds. Values are between 1 and 15.
- Determine how many attempts (default is 3 times) to make to reach the server before stopping and assuming it is unreachable. Values are between 1 and 5.

NOTE
If the LDAP server's IP address is entered in the Management application, the LDAP server's hostname (if any) must still be known to the Management application host OS. The Management application server must be using a DNS server that knows the LDAP server's hostname, or you must manually add the LDAP server's hostname to the local hosts file (for Linux the file is located in /etc/hosts and for Windows the file is located in C:\Windows\System32\drivers\etc\hosts for Windows).

To configure an LDAP server for authentication, complete the following steps.

1. Select the **AAA Settings** tab.
2. Select **LDAP Server** from the **Primary Authentication** list.

   If you configure the external LDAP server as the primary authentication server, make the following preparations first:

   - Make sure that the external LDAP server and its user accounts have been properly configured (refer to "Creating an AD user account" on page 203). For example, you must define roles and areas of responsibility (AOR) in the external server to match the Management application roles and AOR.
   - Make sure to configure the custom attributes "NmRoles" and "NmAors" on the LDAP server (refer to "Configuring roles and AORs on the external LDAP server" on page 204). NmRoles defines the Management application user roles (such as Host Administrator, IP System Administrator, Network Administrator, Operator, Report User Group, SAN System Administrator, Security Administrator, Security Officer, and Zone Administrator). NmAors defines the areas of responsibility (such as, All Fabrics, All IP Products).
3. Add or edit a LDAP server by referring to "Configuring an LDAP server" on page 384.

   The **LDAP Servers and Sequence** table displays the following information:

   - **Network Address** — The network address of the LDAP server.
   - **Authentication Type** — The authentication type (such as, CHAP).
   - **Security** — Whether or not security is enabled.
   - **TCP Port** — The TCP port number of the LDAP server.
   - **TimeOut (Sec)** — The timeout value in seconds specified when sending an authentication request to the server. Default is 3.
   - **Attempts** — The number of attempts made to reach a server before determining it is unreachable. Default is 3.
4. Rearrange the LDAP servers in the table by selecting a server and click the **Up** or **Down** button to move it.
5. Delete a LDAP server by selecting the server and click **Delete**.
6. Test the established active connection with the LDAP server by clicking **Test**.

   The **Test Authentication** dialog box displays.
7. Enter your user name and password and click **OK**.

   Test attempts to contact the LDAP server by issuing a **ping** command and verifies the following:

   - Verifies connections to the LDAP Server
   - Verifies authentication with the LDAP Server

- Verifies user privileges on the Local database

8. Set secondary authentication by selecting one of the following options from the **Secondary Authentication** list:
   - **Local Database**
   - None
9. Set the fall back condition to secondary authentication by selecting one of the following options from the **Switch to secondary authentication when** list:
   - LDAP Servers Not Reachable
   - LDAP Authentication Failed
   - User Not Found in LDAP
10. Set the authorization preference by selecting one of the following options from the **Authorization Preference** list:
    - Local Database
      - Use the LDAP server for authentication and the Management application local database for authorization.
      - The user name in the local database must match the LDAP user name (password does not need to match) and must have the appropriate roles and AORs. If the Management application user name and LDAP user name do not match, create the user and assign the respective roles and AORs (refer to "User Account Management" on page 181).
    - Primary Authentication Server
      - Use the LDAP server for authentication and authorization.
      - In the LDAP server, create new custom attributes (NmRoles & NmAors) in the AD server and assign the appropriate Roles and AORs (refer to "Configuring roles and AORs on the external LDAP server" on page 204).
        If this user already exists in the local database, the roles and AORs are overwritten with the new roles and AORs configured in the LDAP Server.
    - LDAP Authorization
      - Use to assign roles and AORs to user groups and not to individual users.
      - When roles and AORs are assigned to a group, all AD users in the group can obtain the roles and AORS assigned to the group. To assign roles and AORs to an AD Group, refer "Assigning roles and AORs to an AD group" on page 201.
        You do not need to create users in the local database.
11. Click **Apply** to save the configuration.

    To display the authentication audit trail, refer to "Displaying the client authentication audit trail" on page 391.
12. Click **Close** to close the Server Management Console.

Configuring an LDAP server

To add or edit a LDAP server, complete the following steps.

1. Select the **AAA Settings** tab.
2. Select **LDAP Server** from the **Primary Authentication** list.

3. Choose one of the following options:
   - Click **Add**.
   - Select an existing LDAP server and click **Edit**.

     The **Add or Edit LDAP Server** dialog box displays (Figure 145).

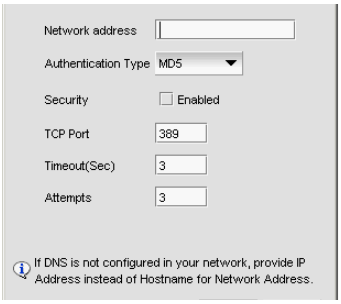


FIGURE 145 Add or Edit LDAP server

4. Enter the LDAP server's hostname in the **Network address** field.

   If DNS is not configured in your network, provide an IP address instead of the hostname.

5. Enable security by selecting the **Security Enabled** check box.

   When you enable security, the TCP port number automatically changes to port 636 and you must enable certificate services on the LDAP server.

6. Enter the TCP port used by the LDAP server in the **TCP Port** field.

   Default is 389 if security is not enabled. Default is 636 if security is enabled.

7. Enter the timeout timer value (in seconds) that specifies the amount of time to wait between retries when the server is busy in the **Timeout (Sec)** field.

   Default is 3 seconds.

8. Enter the number of attempts to be made to reach a server before assuming it is unreachable in the **Attempts** field.

   Default is 3 attempts.

9. Click **OK** to return to step 4 on the **AAA Settings** tab.

Configuring TACACS+ server authentication

If you are using a TACACS+ server for authentication, make the following preparations first:

- Make sure that the server you want to use is on the network that the Management application manages.
- Make sure that the external server and its user accounts have been properly configured. For example, you must define roles and areas of responsibility (AOR) in the external server to match the Management application roles and AOR.

To configure TACACS+ server authentication, complete the following steps.

1. Select the **AAA Settings** tab.
2. For **Primary Authentication**, select **TACACS+ Server**.

3. Add or edit a TACACS+ server by referring to "Configuring a TACACS+ server" on page 386.
4. Rearrange the TACACS+ servers in the table by selecting a server and click the **Up** or **Down** button to move it.
5. Delete a TACACS+ server by selecting the server and click **Delete**.
6. Test the established active connection with the TACACS+ server by clicking **Test**.

   The **Test Authentication** dialog box displays.
7. Enter your user ID and password and click **Test**.

   Test verifies your user ID and password for the local database and verifies user privileges on the Management application server.
8. Set secondary authentication by selecting one of the following options from the **Secondary Authentication** list:
   - **Local Database**
   - None
9. Set the fall back condition to secondary authentication by selecting one of the following options from the **Fail Over Option** list:
   - TACACS+ Server Not Reachable
   - TACACS+ Server Authentication Failed
10. Set the authorization preference by selecting one of the following options from the **Authorization Preference** list:
    - Local Database
    - Primary Authentication Server
11. Click **Apply** to save the configuration.

    To display the authentication audit trail, refer to "Displaying the client authentication audit trail" on page 391.
12. Click **Close** to close the Server Management Console.

Configuring a TACACS+ server

To add or edit a TACACS+ server, complete the following steps.

1. Choose one of the following options from the **AAA Settings** tab:
   - Click **Add**.
   - Select an existing TACACS+ server and click **Edit**.

     The **Add or Edit TACACS+ Server** dialog box displays (Figure 145).

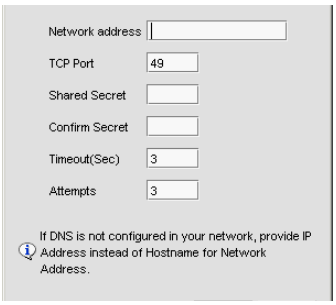


FIGURE 146 Add or Edit TACACS+ Server

2. Enter the TACACS+ server's hostname in the **Network Address** field.

   If DNS is not configured in your network, provide an IP address instead of the hostname.

3. Enter the TCP port used by the TACACS+ server in the **TCP Port** field.

   Default is 49.

4. Enter the shared secret in the **Shared Secret** and **Confirm Secret** fields.

5. Enter the timeout timer value (in seconds) that specifies the amount of time to wait between retries when the server is busy in the **Timeout (Sec)** field.

   Default is 3 seconds.

6. Enter the number of attempts to be made to reach a server before assuming it is unreachable in the **Attempts** field.

   Default is 3 attempts.

7. Click **OK** to return to the **AAA Settings** tab.

   The **Radius Servers and Sequence** table displays the following information:

   - **Network Address** — The network address of the TACACS+ server.
   - **TCP Port** — The TCP port number of the LDAP server.
   - **TimeOut (Sec)** — The timeout value in seconds specified when sending an authentication request to the server. Default is 3.
   - **Attempts** — The number of attempts made to reach a server before determining it is unreachable. Default is 3.

Configuring Common Access Card authentication

NOTE
Common Access Card (CAC) authentication does not support SMI Agent and launch-in-context dialog boxes.

NOTE
CAC authentication is only supported on Windows systems.

Common Access Card (CAC) authentication requires the following preparations:

- Make sure to connect the CAC reader to the Management application client workstation.

- Make sure to obtain and install the active client library on the client workstation. The active client library is not shipped with the Management application.
- Make sure to log in to the Management application client using a smartcard.
- Make sure that the Active Directory (AD) server you want to use is on the network that the Management application manages.
- Make sure that the Management application server and client system clocks are synchronized even if they are in different time zones.
- Make sure that the AD server you want to use is connected to the Management application client.
- Make sure you have the username and password of the Management application service account configured on the AD server to which the client is connected. It is recommended that you create and use the following name for this account: NetworkMangementSVC.

NOTE
If there are Management application clients from different domains, then each client's AD server must be configured with same user account and Kerberos Service Principal Name (SPN)

- Make sure you have the Kerberos SPN that is configured on the Key Distribution Center (KDC) of the AD server and map it to the Management application server account. It is recommended that you create and use the following name for this account: NetworkMangementSPN.

  If you need to add a Kerberos SPN to the KDC of the AD server, use the following command on the Management application client or the AD server to which the client is connected:

  `setspn -S` *<SPN>/<Management application server host name with domain name><AD server user account>*

  For example: setspn -S NetworkManagementSPN/DCM-VNext-65.JCB.com NetworkManagementSvc

NOTE
If there are multiple Management application servers, then a Kerberos Service Principal Name must be added for each server.

To configure CAC authentication, complete the following steps.

1. Select the **AAA Settings** tab.
2. Select **CAC** from the **Primary Authentication** list.
3. Set the authorization preference by selecting one of the following options from the **Authorization Preference** list:
   - **Local Database** — Uses the AD server for authentication and the Management application local database for authorization.
   - **Primary Authentication Server** — Uses the AD server for authentication and authorization.

   If you select Primary Authentication Server or LDAP Authorization, CAC authentication uses the same AD servers for authentication and authorization.
4. Enter the username for the Management application service account configured on the AD server in the **Username** field.

5. Enter the password for the Management application service account configured on the AD server in the **Password** and **Confirm Password** fields.
6. Enter the Kerberos SPN in the **Kerberos Service Principal Name** field.

   The SPN name uses the following syntax: <*Service_Name*>/<*Hostname*>, where hostname is the Management application server's host name with domain name. For example: NetworkManagementSPN/DCM-VNext-65.JCB.COM
7. Test the established active connection with the server by clicking **Test**.

   The **Test Authentication** dialog box displays. Test performs the following functions and verifications:

   - Obtains the Kerberos Ticket Granting Ticket (TGT) of the currently logged in user from Windows cached credentials.
   - Sends the TGT to the AD server to which the Management application server is connected and requests the session ticket for the SPN configured on AD server.

     Kerberos encryptsthe session ticket with the credentials of the AD server user account mapped to this SPN.
   - Logs on to the AD of the Management application server using the AD server single-sign-on (SSO) service account.
   - Verifies the service ticket by decrypting it using AD server SSO service account credentials.
8. Click **Apply** to save the configuration.

   To display the authentication audit trail, refer to "Displaying the client authentication audit trail" on page 391.
9. Click **Close** to close the Server Management Console.

Configuring switch authentication

Switch authentication enables you to authenticate a user account against the switch database and the Management application server. You can configure up to three switches and specify the fall back order if one or more of the switches is not available.

NOTE
Switch authentication is only supported on Fabric OS devices.

To configure switch authentication, complete the following steps.

1. Select the **AAA Settings** tab.
2. For **Primary Authentication**, select **Switch**.
3. Click **Add**.
4. Enter the switch IP address and click **OK**.

   You can add up to three switches.
5. Select a switch and click the **Up** or **Down** button to set the fall back order.
6. Select a switch and click **Delete** to remove a switch from the list.
7. Set secondary authentication by selecting one of the following options from the **Secondary Authentication** list:

- **Local Database**
- None

8. Click **Test**.

   The **Test Authentication** dialog box displays.

9. Enter your user ID and password and click **Test**.

   Test verifies your user ID and password on the switch and verifies user privileges on the Management application server.

10. Click **Apply** to save the configuration.

    To display the authentication audit trail, refer to "Displaying the client authentication audit trail" on page 391.

11. Click **Close** to close the Server Management Console.

Configuring Windows authentication

Windows authentication enables you to authenticate a user account against the Windows user accounts and the Management application server when running on Windows hosts.

The following list details the supported Windows authentication types and the associated platforms:

- NT domain authentication — supported on Windows XP/2003/2008 platforms only
- Windows Workgroup authentication — supported on Windows XP/2003/2008 platforms only
- Windows local user accounts — supported on Windows XP/2003/2008 platforms only.

To configure Windows authentication, complete the following steps.

1. Select the **AAA Settings** tab.
2. For **Primary Authentication**, select **Windows Domain**.
3. Enter the domain name in the **Windows Domain Name** field.
4. Set secondary authentication by selecting one of the following options from the **Secondary Authentication** list:
   - **Local Database**
   - None
5. Click **Test**.

   The **Test Authentication** dialog box displays.

1. In the **User ID** field, choose one of the following options:
   - To authenticate a user account against the current domain, enter your user name.
   - To authenticate a user account against a different domain, enter *Domain\User_Name*.
2. Enter your password in the **Password** field and click **OK**.

   Test verifies your user ID and password on the Windows domain and verifies user privileges on the Management application server.

3. Click **Apply** to save the configuration.

To display the authentication audit trail, refer to "Displaying the client authentication audit trail" on page 391.

4. Click **Close** to close the Server Management Console.

Configuring local database authentication

Local database authentication enables you to authenticate a user account against the local database and the Management application server.

To configure local database authentication, complete the following steps.

1. Select the **AAA Settings** tab.
2. For **Primary Authentication**, select **Local Database**.
3. Click **Test**.

   The **Test Authentication** dialog box displays.
4. Enter your user ID and password and click **Test**.

   Test verifies your user ID and password for the local database and verifies user privileges on the Management application server.
5. Click **Apply** to save the configuration.

   To display the authentication audit trail, refer to "Displaying the client authentication audit trail" on page 391.
6. Click **Close** to close the Server Management Console.

Displaying the client authentication audit trail

All responses to authentication requests coming from clients are logged to an audit trail log file. This file is automatically backed up on the first day of every month.

1. Select the **AAA Settings** tab.
2. Click **Display** next to **Authentication Audit Trail**.

   The **Login** dialog box displays.
3. Enter your username and password in the appropriate fields and click **OK**.

   The defaults are Administrator and password, respectively.

   The **Authentication Audit Trail** log displays.

   The audit trail shows user names that have attempted to log in to the Management application, and changes to user authentication.
4. Click the **Client to Server Authentication** tab to view the client to server authentication status.
5. Click the **Authentication Settings Changes** tab to view the previous authentication changes.

Restore tab

The **Restore** tab enables you to restore the application data files used by the Management application server.

Restoring the database

To restore application data files, you must know the path to the backup files. This path is configured from the **Server > Options** dialog box. For more information about backup, refer to "Server Data backup" on page 128.

NOTE
You cannot restore data from a previous version of the Management application.

NOTE
You cannot restore data from a higher or lower configuration (Trial or Licensed version) of the Management application.

NOTE
You cannot restore data from a different package of the Management application.

To restore the application data files, complete the following steps.

1. Click the **Services** tab.
2. Stop all services.
3. Click the **Restore** tab.
4. Click **Browse** to select the path (defined in the **Output Directory** field on the **Options** dialog box - **Backup** pane) to the database backup location.
5. Click **Restore**.

   Upon completion, a message displays the status of the restore operation. Click **OK** to close the message and the Server Management Console. For the restored data to take effect, re-launch the Configuration Wizard using the instructions in "Launching the Configuration Wizard" on page 5.

Technical Support Information tab

The **Technical Support Information** tab of the SMC allows you to capture technical support information for the Management application as well as the configuration files for all switches in discovered fabrics. This information is saved in a *zip* file in a location that you specify.

Capturing technical support information

To capture technical support information, complete the following steps.

1. Select the **Technical Support Information** tab.
2. Select the **Include database** check box to capture database server support save files and choose one of the following options:

- Select the **Partial** option to exclude historical data and events from the database capture.
- Select the **Full** option to include historical data and events from the database capture.

NOTE
It is recommended that you only capture the partial database.

NOTE
You should only capture the full database when you need to debug Historical Performance Management or Historical Events issues.

3. Enter the path where you want to save the support data and a name for the support save file in the **Output Path** field.

   For example, *Full_Path\Support_Save_File_Name*.zip. You can also browse to the location you want to save the support data and append the file name to the path when you return to the **Technical Support Information** tab.

   If you do not specify an output path, the Management application automatically saves the data to the *Install_Home*/support directory. The default name of the Server Support Save is DCM-SS-*Time_Stamp*.

   NOTE
   For Linux systems, you cannot have blank spaces in the output path (target directory). If the output path contains blank spaces, the supportShow files are not complete.

4. Click **Capture**.

   A confirmation message displays when the capture is complete.

5. Click **OK**.

HCM Upgrade tab

The **HCM Upgrade** tab enables you to upgrade the Management application to include a new version of HCM.

Upgrading HCM on the Management server

To upgrade HCM, complete the following steps.

1. Select the **HCM Upgrade** tab.

FIGURE 147 HCM Upgrade tab

2. Click **Browse** to select the HCM installation folder location (for example, C:\Program Files\BROCADE\Adapter on Windows systems and /opt/brocade/adapter on Linux systems).
3. Click **Upgrade**.
4. Click **Close**.

SMI Agent Configuration Tool

The **SMIA Configuration Tool** enables you to configure SMI Agent settings, such as security, CIMOM, and certificate management. This tool is automatically installed with the Management application as part of the Server Management Console. This **SMIA Configuration Tool** consists of the following tabs:

- Home tab — enables you to access Management application features such as, fabric and host discovery, role-based access control, application configuration and display options, server properties, as well as the application name, build, and copyright.
- Authentication tab — enables you to configure mutual authentication for Client, CIMMOM server, and Indication using a secure protocol.
- CIMOM tab — enables you to configure the CIMOM server port, the CIMOM Bind Network Address, and the CIMOM log.
- Certificate Management tab — enables you to import Client and Indication certificates, export Server certificates, as well as view and delete current certificates.
- Summary tab — enables you to view the CIMOM server configuration and current configuration.

Launching the SMIA configuration tool on Windows

NOTE
All Management application services must be running before you can log into the **SMIA Configuration Tool**. To start the Management application services, click **Start** on the **Server Management Console dialog box.**

1. Launch the **Server Management Console** from the **Start** menu on the Management application server.

   You can also drag the SMC icon onto your desktop as a short cut.

2. Click **Configure SMI Agent on the Server Management Console dialog box.**

   The **Log In** dialog box displays.

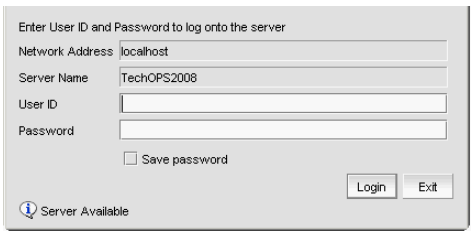


FIGURE 148 Log In dialog box

3. Enter your username and password in the appropriate fields.

   The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.

4. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.

5. Click **Login**.

   The **SMIA Configuration Tool** dialog box displays.

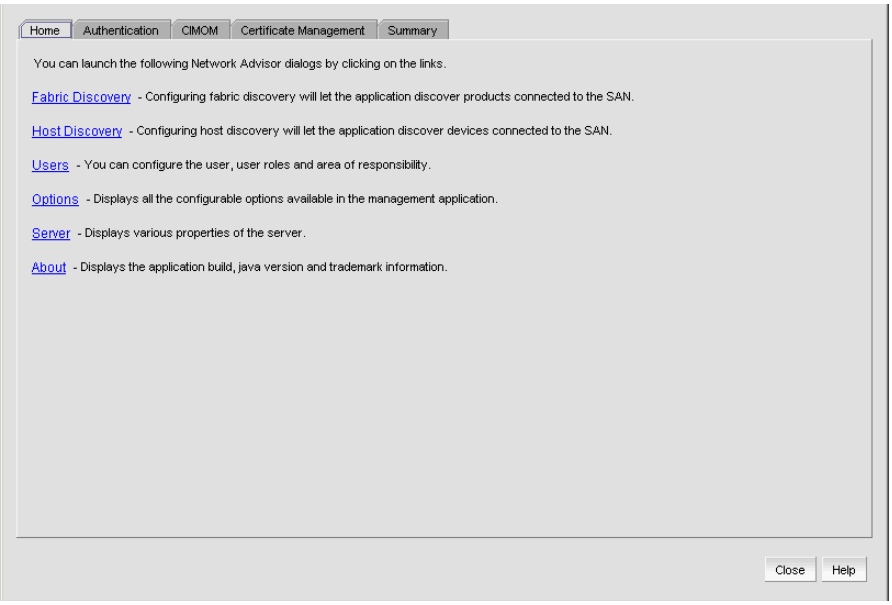


FIGURE 149 SMIA Configuration Tool dialog box

Launching the SMIA configuration tool on Unix

NOTE
All Management application services must be running before you can log into the **SMIA Configuration Tool**. To start the Management application services, click **Start** on the **Server Management Console dialog box.**

Perform the following steps to launch the Server Management Console on Unix systems.

1. On the Management application server, go to the following directory:

   Install_Directory/bin

2. Type the following at the command line:

   ```
   ./smc
   OR
   sh smc
   ```

3. Click **Configure SMI Agent on the Server Management Console dialog box.**

   The **Login** dialog box displays.

4. Enter your username and password in the appropriate fields and click **OK**.

   The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.

   The **SMIA Configuration Tool** dialog box displays.

Launching a remote SMIA configuration tool

To launch a remote SMIA configuration tool, complete the following steps.

1. Open a web browser and enter the IP address of the Management application server in the **Address** bar.

   If the web server port number does not use the default (443 if is SSL Enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address. For example, *IP_Address*:*Web_Server_Port_Number*.

   The Management application web start screen displays.

2. Click the SMIA configuration tool application web start link.

   The **Log In** dialog box displays.

3. Enter your user name and password.

   The defaults are **Administrator** and **password**, respectively.

   NOTE
   Do not enter *Domain**User_Name* in the **User ID** field for LDAP server authentication.

4. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.

5. Click **Login**.

   The **SMIA Configuration Tool** dialog box displays

Service Location Protocol (SLP) support

The Management application SMI Agent uses Service Location Protocol (SLP) to allow applications to discover the existence, location, and configuration of WBEM services in enterprise networks.

You do not need a WBEM client to use SLP discovery to find a WBEM Server; that is, SLP discovery might already know about the location and capabilities of the WBEM Server to which it wants to send its requests. In such environments, you do not need to start the SLP component of the Management application SMI Agent.

However, in a dynamically changing enterprise network environment, many WBEM clients might choose to use SLP discovery to find the location and capabilities of other WBEM Servers. In such environments, start the SLP component of the Management application SMI Agent to allow advertisement of its existence, location, and capabilities.

SLP installation is optional and you can configure it during Management application configuration. Once installed, SLP starts whenever the Management application SMI Agent starts.

SLP support includes the following components:

- slpd script starts the slpd platform
- slpd program acts as a Service Agent (SA). A different slpd binary executable file exists for UNIX and Windows systems.
- slptool script starts the slptool platform-specific program
- slptool program can be used to verify whether SLP is operating properly or not. A different slptool exists for UNIX and Windows.

By default, the Management application SMI Agent is configured to advertise itself as a Service Agent (SA). The advertised SLP template shows its location (IP address) and the WBEM Services it supports. The default advertised WBEM services show the Management application SMI Agent:

- accepts WBEM requests over HTTP without SSL on TCP port 5988
- accepts WBEM requests over HTTPS using SSL on TCP port 5989

slptool commands

Use the following slptool commands to verify whether the SLP is operating properly.

- slptool findsrvs service:service-agent

  Use this command to verify that the Management application SMI Agent SLP service is properly running as a Service Agent (SA).

  Example output: service:service-agent://127.0.0.1,65535

- slptool findsrvs service:wbem

  Use this command to verify that the Management application SMI Agent SLP service is properly advertising its WBEM services.

  Example outputs:

  service:wbem:https://10.0.1.3:5989,65535

  service:wbem:http://10.0.1.3:5988,65535

  This output shows the functionalities of the Management application SMI Agent:

  - accepts WBEM requests over HTTP using SSL on TCP port 5989
  - accepts WBEM requests over HTTP without SSL on TCP port 5988

- slptool findattrs service:wbem:https://*IP_Address*:*Port*

  NOTE
  Where *IP_Address*:*Port* is the IP address and port number that display when you use the slptool findsrvs service:wbem command.

  Use this command to verify that Management application SMI Agent SLP service is properly advertising its WBEM SLP template over the HTTP protocol.

  Example output:

```
Install_Home\cimom\bin>slptool findattrs service:wbem:http://10.24.35.61:5988
(template-type=wbem),(template-version=1.0),(template-description=This
template describes the attributes used for advertising WBEM Servers),
(template-url-syntax=http://10.24.35.61:5988),(service-hi-name=WBEM Solutions
J WBEM Server),(service-hi-description=WBEM Solutions J WBEM Server),
(service-id=WBEMSolutions:f1f65c3b-27f1-4b70-9ced-e412e93a8d5e),(Communicatio
nMechanism=CIM-XML),(OtherCommunicationMechanismDescription =null),
(InteropSchemaNamespace=interop),(ProtocolVersion=1.2),
(FunctionalProfilesSupported=Basic Read,Basic Write,Schema Manipulation,
Instance Manipulation,Association Traversal,Query Execution,Qualifier
Declaration,Indications),(FunctionalProfileDescriptions=null),(MultipleOperat
ionsSupported=true),(AuthenticationMechanismsSupported=Basic),(Authentication
MechanismDescriptions=null),(Namespace=root/brocade1,interop),(Classinfo=0,0)
```

```
,(RegisteredProfilesSupported=SNIA:SMI-S,DMTF:Profile Registration,SNIA:FC
HBA,DMTF:LaunchInContext,SNIA:Fan,SNIA:Fabric,SNIA:Switch,DMTF:Role Based
Authorization,SNIA:Power Supply,SNIA:Sensors,SNIA:Server)
```

- slptool findattrs service:wbem:http://*IP_Address*:*Port*

NOTE
Where *IP_Address*:*Port* is the IP address and port number that display when you use the slptool findsrvs service:wbem command.

Use this command to verify that the Management application SMI Agent SLP service is properly advertising its WBEM SLP template over the HTTPS protocol.

Example output:

```
Install_Home\cimom\bin>slptool findattrs service:wbem:
https://10.24.35.61:5989(template-type=wbem),(template-version=1.0),(template
-description=This template describes the attributes used for advertising WBEM
Servers),(template-url-syntax=https://10.24.35.61:5989),(service-hi-name=WBEM
Solutions J WBEM Server),(service-hi-description=WBEM Solutions J WBEM
Server),(service-id=WBEMSolutions:f1f65c3b-27f1-4b70-9ced-e412e93a8d5e),(Comm
unicationMechanism=CIM-XML),(OtherCommunicationMechanismDescription
=null),(InteropSchemaNamespace=interop),(ProtocolVersion=1.2),(FunctionalProf
ilesSupported=Basic Read,Basic Write,Schema Manipulation,Instance
Manipulation,Association Traversal,Query Execution,Qualifier Declaration,
Indications),(FunctionalProfileDescriptions=null),
(MultipleOperationsSupported=true),(AuthenticationMechanismsSupported=Basic),
(AuthenticationMechanismDescriptions=null),(Namespace=root/brocade1,interop),
(Classinfo=0,0),(RegisteredProfilesSupported=SNIA:SMI-S,DMTF:Profile
Registration,SNIA:FC HBA,DMTF:LaunchInContext,SNIA:Fan,SNIA:Fabric,
SNIA:Switch,DMTF:Role Based Authorization,SNIA:Power Supply,SNIA:Sensors,
SNIA:Server)
```

SLP on UNIX systems

This section describes how to verify the SLP daemon on UNIX systems.

SLP file locations on UNIX systems

- SLP log — *Install_Home*/cimom /cfg/slp.log
- SLP daemon — *Install_Home*/cimom /cfg/slp.conf

  You can reconfigure the SLP daemon by modifying this file.
- SLP register — *Install_Home*/cimom /cfg/slp.reg

  You can statically register an application that does not dynamically register with SLP using SLPAPIs by modifying this file. For more information about these files, read the comments contained in them, or refer to http://www.openslp.org/doc/html/UsersGuide/index.html.

Verifying SLP service installation and operation on UNIX systems

1. Open a command window.
2. Type % su root and press **Enter** to become the root user.
3. Type # *Install_Home*/cimom/bin/slptool findsrvs service:service-agent and press **Enter** to verify the SLP service is running as a Service Agent (SA).

4. Type # *Install_Home*/cimom/bin/slptool findsrvs service:wbem and press **Enter** to verify the SLP service is advertising its WBEM services.
5. Choose one of the following options to verify the SLP service is advertising the WBEM SLP template over its configured client protocol adapters.
   - Type # *Install_Home*/cimom /bin/slptool findattrs service:wbem:http://*IP_Address:Port* and press **Enter**.
   - Type # *Install_Home*/cimom /bin/slptool findattrs service:wbem:https://*IP_Address:Port* and press **Enter**.

NOTE
Where *IP_Address:Port* is the IP address and port number that display when you use the slptool findsrvs service:wbem command.

SLP on Windows systems

This section describes how to verify the SLP daemon on Windows systems.

SLP file locations on Windows systems

- SLP log — *Install_Home*\cimom \cfg\slp.log
- SLP daemon — *Install_Home*\cimom\cfg\slp.conf

  You can reconfigure the SLP daemon by modifying this file.
- SLP register — *Install_Home*\cimom\cfg\slp.reg

  You can statically register an application that does not dynamically register with SLP using SLPAPIs by modifying this file. For more information about these files, read the comments contained in them, or refer to http://www.openslp.org/doc/html/UsersGuide/index.html.

Verifying SLP service installation and operation on Windows systems

1. Launch the Server Management Console from the **Start** menu.
2. Click **Start** to start the SLP service.
3. Open a command window.
4. Type cd c:*Install_Home*\cimom \bin and press **Enter** to change to the directory where slpd.bat is located.
5. Type > slptool findsrvs service:service-agent and press **Enter** to verify the SLP service is running as a Service Agent.
6. Type > slptool findsrvs service:wbem and press **Enter** to verify the SLP service is advertising its WBEM services.
7. Choose one of the following options to verify the SLP service is advertising the WBEM SLP template over its configured client protocol adapters.
   - Type > slptool findattrs service:wbem:http://*IP_Address:Port* and press **Enter**.
   - Type > slptool findattrs service:wbem:https://*IP_Address:Port* and press **Enter**.

NOTE
Where *IP_Address:Port* is the IP address and port number that display when you use the slptool findsrvs service:wbem command.

Home tab

The **Home** tab of the **SMIA Configuration Tool** enables you to access the following Management application features or information:

- **Fabric Discovery** — enables you to view discovered fabrics, discover new fabrics, as well as edit the default SNMP configuration.
- **Host Discovery** — enables you to view discovered hosts, discover new hosts, as well as edit the default SNMP configuration. For step-by-step instructions, refer to "Host discovery" on page 93.
- **Users** — enables you to create or delete Management application users with System Administrator privileges. For step-by-step instructions, refer to "User accounts" on page 185.
- **Options** — enables you to configure the Management application settings. For step-by-step instructions, refer to "Application Configuration" on page 127.
- **Server** — enables you to view server properties. For step-by-step instructions, refer to "Viewing server properties" on page 9.
- **About** — enables you to display information about the Management application, including the build number, Java version, and trademark information.
- **Upgrade** button (Trial version only) — enables you to upgrade from managing 2560 switch ports to 9000 switch ports. For step-by-step instructions, refer to "Upgrading the Management application" on page 38.

Accessing Management application features

To access Management application features such as, fabric and host discovery, role-based access control, application configuration and display options, server properties, as well as the application name, build, and copyright, complete the following steps.

1. Click the **Home** tab, if necessary.
2. Select from the following to access the feature or dialog box.
    - Fabric Discovery
    - Host Discovery
    - Users
    - Options
    - Server
    - About
    - **Upgrade** (Trial version only)
3. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Authentication tab

NOTE
You must have User Management Read and Write privileges to make changes on the CIMOM tab. For more information about privileges, refer to "User Privileges" on page 1283.

The **Authentication** tab enables you to configure mutual authentication for Client and Indication using a secure protocol.

Enabling or disabling CIM client and indication mutual authentication

When you enable client mutual authentication, all CIM client and indication requests to the SMI Agent must pass credentials (KeyStore and TrustStore) to validate the requests. The KeyStore file provides the credentials and the TrustStore file verifies the credentials. When you enable indication mutual authentication, both the CIM client and the CIMOM server maintain the TrustStore files.

The CIM client KeyStore file sends credentials to be validated by the CIMOM server TrustStrore file for any communication from the CIM client to the CIMOM server and the CIMOM server KeyStore file sends credentials to be validated by the CIM client TrustStrore file for any communication from the CIMOM server to the CIM client

To enable or disable CIM client and indication mutual authentication, complete the following steps.

1. Click the **Authentication** tab.

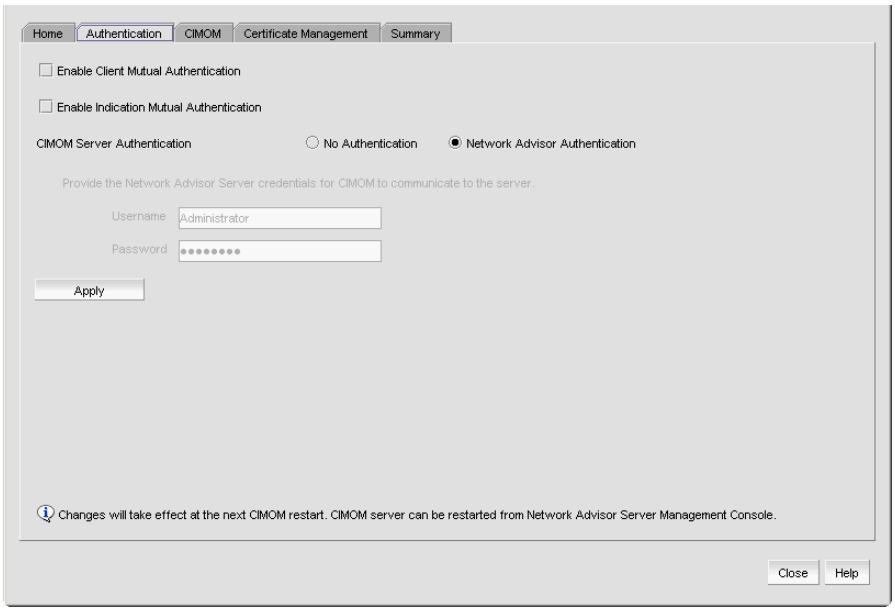


FIGURE 150 Authentication tab

2. Select the **Enable Client Mutual Authentication** check box, as needed.

   If the check box is checked, CIM client mutual authentication is enabled. If the check box is clear (default), client mutual authentication is disabled.

3. Select the **Enable Indication Mutual Authentication** check box, as needed.

   If the check box is checked, indication mutual authentication is enabled. If the check box is clear (default), indication mutual authentication is disabled.

4. Click **Apply**.

NOTE
Changes on this tab take effect after the next CIMOM server restart.

NOTE
You can only restart the server using the Server Management Console (**Start > Programs >** *Management_Application_Name* **12.X.X > Server Management Console**).

5. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Configuring CIMOM server authentication

CIMOM server authentication is the authentication mechanism between the CIM client and the CIMOM Server. You can configure the CIMOM server to allow the CIM client to query the CIMOM server without providing credentials; however, the CIMOM server requires the Management application credentials to connect to the Management application server to retrieve the required data. Therefore, if you select no authentication, you must provide Management application credentials to retrieve data from the Management application server.

To configure CIMOM server authentication, complete the following steps.

1. Click the **Authentication** tab.
2. Choose from one of the following options:
   - Select **No Authentication** to allow the CIM client to query the CIMOM server without providing credentials; however, note that the CIMOM server requires the Management application credentials to connect to the Management application server to retrieve the required data. To provide Management application credentials, complete the following steps.
     a. Enter the Management application user name in the **Username** field.
     b. Enter the Management application user password in the **Password** field.
   - Select *Management_Application* **Authentication** to allow the CIM client to query the CIMOM server and the Management application server using the credentials configured on the **Users** tab.
3. Click **Apply**.

NOTE
Changes on this tab take effect after the next CIMOM server restart.

NOTE
You can only restart the server using the Server Management Console (**Start > Programs >** *Management_Application_Name* **12.X.X > Server Management Console**).

4. Click **Close** to close the **SMIA Configuration Tool** dialog box.

CIMOM tab

NOTE
You must have SAN - SMI Operation Read and Write privileges to view or make changes on the CIMOM tab. For more information about privileges, refer to "User Privileges" on page 1283.

The **CIMOM** tab enables you to configure the CIMOM server port, the CIMOM Bind Network Address, and the CIMOM log.

Configuring the SMI Agent port number

To configure the SMI Agent port number, complete the following steps.

1. Click the **CIMOM** tab.

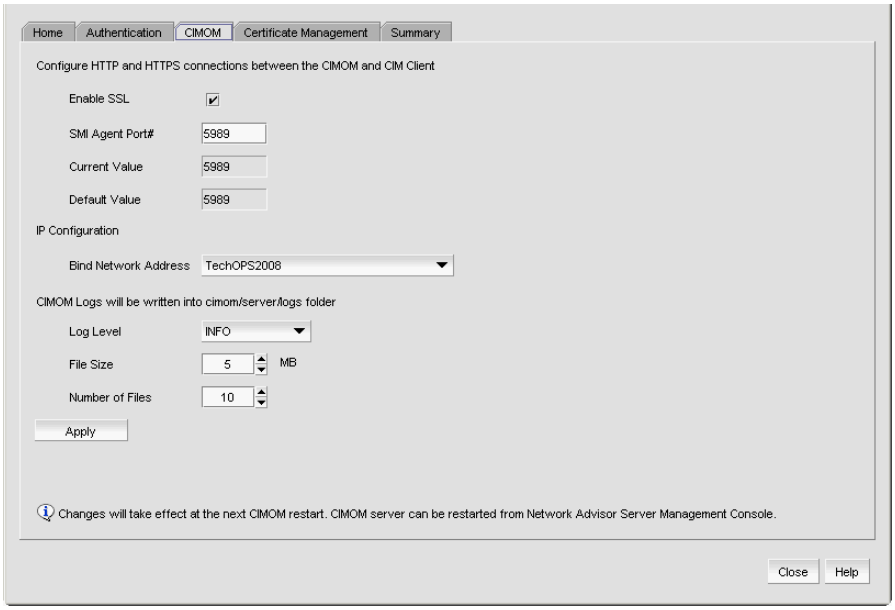


FIGURE 151 CIMOM tab

2. Select or clear the **Enable SSL** check box, to enable or disable SSL for the SMI Agent.

NOTE
Disabling SSL will disable Indication and Client Mutual Authentication.

If the check box is checked (default), SSL is enabled. If the check box is clear, SSL is disabled.

3. Enter the SMI Agent port number in the **SMI Agent Port #** field.

This port number must be within the range of 1 through 65535. Defaults are 5989 with SSL enabled and 5988 with SSL disabled.

4. Click **Apply**.

NOTE
Changes on this tab take effect after the next CIMOM server restart.

NOTE
You can only restart the server using the Server Management Console (**Start > Programs >** *Management_Application_Name* **12.X.X > Server Management Console**).

If you disabled SSL, a confirmation message displays. Click **Yes** to continue.

5. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Configuring the CIMOM Bind Network Address

NOTE
You must have SAN - SMI Operation Read and Write privileges to view or make changes on the CIMOM tab. For more information about privileges, refer to "User Privileges" on page 1283.

To configure the network bind address, complete the following steps.

1. Click the **CIMOM** tab.
2. Select a network address from the **IP Configuration Bind Network Address** list to which you want to bind the CIMOM server.

   The default network address is the host system name.

3. Click **Apply**.

NOTE
Changes on this tab take effect after the next CIMOM server restart.

NOTE
You can only restart the server using the Server Management Console (**Start > Programs >** *Management_Application_Name* **12.X.X > Server Management Console**).

4. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Configuring the CIMOM log

NOTE
You must have SAN - SMI Operation Read and Write privileges to view or make changes on the **CIMOM** tab. For more information about privileges, refer to "User Privileges" on page 1283.

To configure the CIMOM log, complete the following steps.

1. Click the **CIMOM** tab.
2. Select a log category from the **Log Level** list to start logging support data for the server.

   Options include the following:

   - Off — select to turn off logging support data.
   - Severe — select to only log support data that indicates serious failures which prevent normal program operation.
   - Warning — select to only log support data that indicates a potential problem.
   - Info (default) — select to only log support data for informational messages.
   - Config — select to only log support data for static configuration messages used to assist in debugging problems associated with particular configurations.
   - Fine — select to only log message data used to provide trace information.
   - Finer — select to only log message data used to provide detailed trace information.
   - Finest — select to only log message data used to provide highly detailed trace information.
   - All — select to log support data for all messages.
3. Click **Apply**.

   NOTE
   Changes on this tab take effect after the next CIMOM server restart.

   NOTE
   You can only restart the server using the Server Management Console (**Start > Programs >** *Management_Application_Name* **12.X.X > Server Management Console**).
4. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Certificate Management tab

NOTE
You must have SMI Operation Read and Write privileges to view or make changes on the **Certificate Management** tab. For more information about privileges, refer to "User Privileges" on page 1283.

The **Certificate Management** tab enables you to manage your CIM client and Indication authentication certificates. Using this tab, you can perform the following operations:

- "Importing a certificate"
- "Viewing a certificate"
- "Exporting a certificate"
- "Deleting a certificate"

Importing a certificate

To import a certificate, complete the following steps.

1. Click the **Certificate Management** tab.

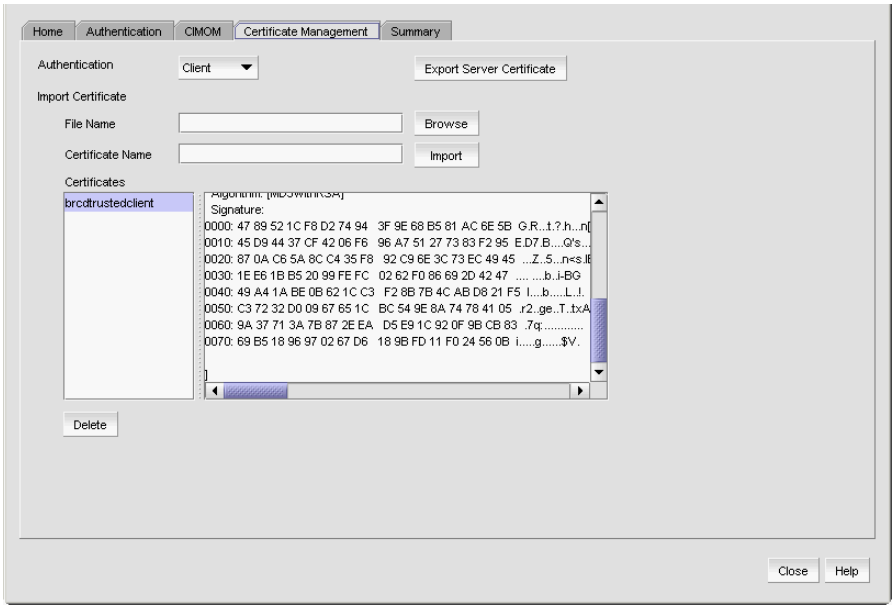


FIGURE 152 Certificate Management tab

2. Select the **Client** or **Indication** from the **Authentication** list.

   The appropriate certificates display in the **Certificates** list.

3. Enter the full path or browse to the certificate you want to import (for example, on Windows the path is C:\Certificates\cimom-indication-auth2.cer and on Linux the path is opt/Certificates/cimom-indication-auth2.cer).

   You can only import certificate files with the CER extension (.cer).

4. Enter a name for the certificate in the **Certificate Name** field.

5. Click **Import**.

   The new certificate displays in the **Certificates** list and text box.

   If the certificate location is not valid, an error message displays. Click **OK** to close the message and reenter the full path to the certificate location.

   If you did not enter a certificate name, an error message displays. Click **OK** to close the message and enter a name for the certificate.

   If the certificate file is empty or corrupted, an error message displays. Click **OK** to close the message.

6. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Viewing a certificate

NOTE
You must have SMI Operation Read and Write privileges to view the **Certificate Management** tab. For more information about privileges, refer to "User Privileges" on page 1283.

To view a certificate, complete the following steps.

1. Select **Client** or **Indication** from the **Authentication** list.

   The appropriate certificates display in the **Certificates** list.

2. Select the certificate you want to view in the **Certificates** list.

   The certificate details display in the **Certificates** text box.

3. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Exporting a certificate

NOTE
You must have SMI Operation Read and Write privileges to view or make changes to the **Certificate Management** tab. For more information about privileges, refer to "User Privileges" on page 1283.

To export a certificate, complete the following steps.

1. Click the **Certificate Management** tab.
2. Select **Client** or **Indication** from the **Authentication** list.

   The appropriate certificates display in the **Certificates** list.

3. Select the certificate you want to export in the **Certificates** list.
4. Click **Export Server Certificate.**

   The **Save As** dialog box displays.

5. Browse to the directory where you want to export the certificate.
6. Edit the certificate name in the **File Name** field, if necessary.
7. Click **Save**.
8. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Deleting a certificate

NOTE
You must have SMI Operation Read and Write privileges to view or make changes to the **Certificate Management** tab. For more information about privileges, refer to "User Privileges" on page 1283.

To delete a certificate, complete the following steps.

1. Click the **Certificate Management** tab.
2. Select **Client** or **Indication** from the **Authentication** list.

   The appropriate certificates display in the **Certificates** list.
3. Select the certificate you want to delete in the **Certificates** list.
4. Click **Delete**.
5. Click **Yes** on the confirmation message.

   The selected certificate is removed from the **Certificates** list.
6. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Summary tab

The **Summary** tab enables you to view summary information about the Server configuration and the current configuration.

Viewing the configuration summary

To view summary information about the Server configuration and the current configuration, complete the following steps.

NOTE
Server configuration changes in the **Summary** tab only take effect after the CIMOM restart.

NOTE
You can only restart the server using the Server Management Console (**Start > Programs >** *Management_Application_Name* **12.X.X > Server Management Console**).

1. Click the **Summary** tab.

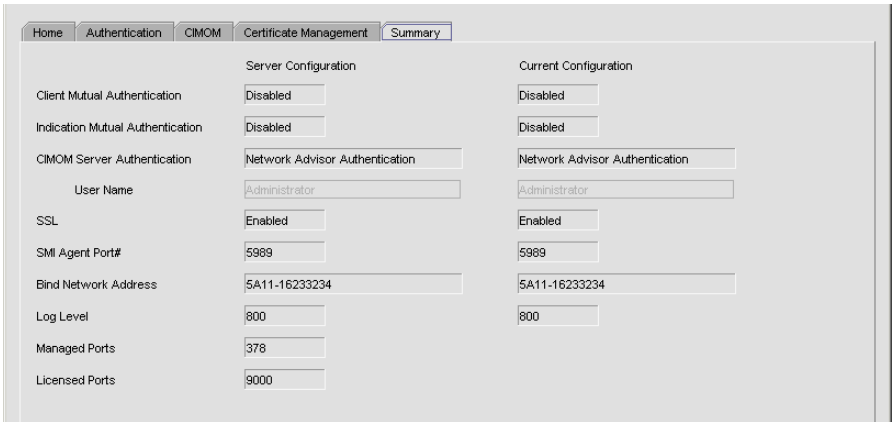


FIGURE 153 Summary tab

2. Review the summary.

NOTE
When the CIMOM server is stopped, the server configuration information does not display on the **Summary** tab.

The following information is included in the summary.

TABLE 38

Field/Component	Description
Client Mutual Authentication	Displays whether or not the client mutual authentication is enabled or disabled for the Server Configuration and the Current Configuration.
Indication Mutual Authentication	Displays whether or not the indication mutual authentication is enabled or disabled for the Server Configuration and the Current Configuration.
CIMOM Server Authentication	Displays whether or not the CIMOM server authentication is enabled or disabled for the Server Configuration and the Current Configuration.
User Name	Displays the user name for the Server Configuration and the Current Configuration. Only enabled if **CIMOM Server Authentication** is No Authentication.
SSL	Displays whether or not the SSL is enabled or disabled for the Server Configuration and the Current Configuration.
SMI Agent Port #	Displays the SMI Agent port number for the Server Configuration and the Current Configuration.
Bind Network Address	Displays the Bind Network address for the Server Configuration and the Current Configuration.

TABLE 38

Field/Component	Description
Log Level	Displays the log level for the Server Configuration and the Current Configuration. Options include the following: • 10000 — Off • 1000 — Severe • 900 — Warning • 800 — Info (default) • 700 — Config • 500 — Fine • 400 — Finer • 300 — Finest • 0 — All
Managed Ports	Displays the number of managed ports. For more information about managed port count rules, refer to "Managed count" on page 35.
Licensed Ports	Displays the number of licensed ports.

3. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Chapter

13

Wireless Management

In this chapter

Wireless management overview

Wireless controllers manage access points by providing centralized management of system wide wireless LAN functions, such as security policies, intrusion prevention, and RF management. The controller applies rules or actions to all devices on the wireless network. The controller also collects management data from the individual access points and transfers that data to a centralized controller.

Wireless access points allow wireless devices, such as laptops and smart phones, to connect to a wired network. Access points receive data from wireless devices and forward the data to the Ethernet switch.

The Management application supports some management operations of the wireless devices in the network. However, the Management application does not provide full feature access for wireless controllers and access points. This chapter details the management features currently available for wireless controllers and standalone access points.

Wireless devices

The Management application supports three models of wireless controllers.

TABLE 39 Wireless controller models

Device Name	Firmware required
RFS 4000	Mobility 5.3 or later
RFS 6000	Mobility 5.3 or later
RFS 7000	Mobility 5.3 or later

The Management application supports four models of wireless access points.

TABLE 40 Wireless access points

Device Name	Firmware required
AP 650	Mobility 4.1.1 (standalone mode) Mobility 5.1 [1] (adaptive mode)
AP 7131	Mobility 4.1.1 (standalone mode) Mobility 5.1 [1] (adaptive mode)
AP 7131N	Mobility 4.1.1 (standalone mode) Mobility 5.1 [1] (adaptive mode)
AP 5181	Mobility 2.5.X (standalone mode) Mobility 5.1 [1] (adaptive mode)
AP 6511	Mobility 4.1.1 (standalone mode) Mobility 5.1 [1] (adaptive mode)

1 The Management application cannot discover or manage wireless access points running Mobility 5.1.

Wireless device discovery

The Management application enables you to discover individual wireless devices or multiple wireless devices using a discovery profile.

NOTE
Wireless access points in adaptive mode cannot be discovered by the Management application.

Instructions for discovering IP devices are detailed in Chapter 3, “Discovery” and include information about the following:

- “Configuring a discovery profile” on page 64
- “Adding an IP device to discovery” on page 84

After discovery, the Management application inspects the SNMP trap recipient and syslog recipient registration on wireless controllers. If there is an error with the registration, a Master Log event displays as a Warning event. The Warning event provides the reason for the error to enable you to fix the problem.

Wireless devices on the dashboard

Wireless controllers and standalone access points display in the following dashboard widgets:

- IP Inventory
- IP Status
- AP Status
- Status

NOTE
Wireless access points in adaptive mode do not display in the dashboard.

For more information about the Dashboard, refer to Chapter 7, "Dashboard Management" which includes information about the following:

- "Dashboard overview" on page 211
- "Status widgets" on page 224
- "Performance monitors" on page 237
- "User-defined performance monitors" on page 264

Port groups

Port groups allow you to group ports together across network devices to perform common port-based configuration and monitoring activities.

Once configured you can use port groups to perform the following:

- Deploy common configurations to all ports in a group.
- Collect port usage data for all ports in a group.

You can see all port groups; however, under each group, you can only see devices that belong to your area of responsibility (AOR). You can only see user-defined port groups that belong to your AOR.

Instructions for managing port groups are detailed in Chapter 4, "Management Groups" and include information about the following:

- "Creating a port group" on page 122
- "Editing a port group" on page 123
- "Duplicating a port group" on page 124
- "Viewing port group properties" on page 125
- "Deleting a port group" on page 126

View management

Wireless controllers and standalone access points display in the Network Objects, L2 Topology, IP Topology, and VLAN Topology views.

NOTE
Wireless access points in adaptive mode do not display in the topology.

Instructions for managing customized views of the topology are detailed in Chapter 8, "View Management" and include information about the following:

- "Displaying topology views" on page 306
- "Network Objects view" on page 307
- "IP Topology view" on page 309
- "L2 Topology view" on page 309
- "VLAN Topology view" on page 310

Wireless device properties

NOTE
Wireless access points in adaptive mode do not display in the Management application.

The Management application enables you to view properties for individual devices as well as device group properties.

Instructions for viewing wireless device properties are detailed in the following sections:

- "Viewing product group properties" on page 120
- "Viewing IP device and port properties" on page 1314

Element Manager

NOTE
Wireless access points in adaptive mode do not display in the Management application.

The Management application enables you to perform additional configuration of the wireless devices using an Element Manager (web-based graphical user interface (GUI)) or command line interface (CLI).

The Element Manager (Brocade Mobility) is a software management application that allows full control of all managed features for the wireless devices in your IP network. For more information about the Element Manager, refer to the *Brocade Mobility RFS4000, RFS6000, and RFS7000 System Reference Guide* available at http://www.brocade.com.

The CLI also enables you to configure, monitor, and troubleshoot wireless controllers. For more information about the command line interface and a list of available commands, refer to the *Brocade Mobility RFS4000, RFS6000, and RFS7000 CLI Reference Guide* available at http://www.brocade.com.

Browser and system requirements

The Element Manager requires a browser supporting Adobe Flash Player 10. The system accessing the Element Manager should have a minimum of 512Mb RAM for the Element Manager to display and function properly.

The following browsers have been validated with the Element Manager:

- Firefox 3.6
- Internet Explorer 7.x
- Internet Explorer 8.x

NOTE
Leading and trailing spaces are not allowed in any text fields in the Element Manager. In addition, the Element Manager does not support the "?" character in text fields.

Launching the Element Manager

NOTE
Wireless access points in adaptive mode do not display in the Management application.

To launch the Element Manager, complete the following steps.

1. On the Product List, right-click the device you want to manage and select **Element Manager > Web**.

   OR

   On the Topology Map (L2 or IP only), right-click the device you want to manage and select **Element Manager > Web**.

   If the device credentials match the credentials provided in discovery, the Element Manager displays.

   If the device credentials do not match the credentials provided in discovery, the Element Manager login dialog box displays. Continue with step 2.

2. Enter your user name in the **Username** field.

   The default user name is admin.

3. Enter your password in the **Password** field.

   The default password admin123.

4. Click **Login**.

   The Element Manager displays.

OR

1. Select a device in the Product List.
2. Select **Configure > Element Manager > Web**.

   The Element Manager login dialog box displays.

3. Enter your user name in the **Username** field.

   The default user name is admin.

4. Enter your password in the **Password** field.

   The default password admin123.

5. Click **Login**.

   The Element Manager displays.

OR

1. Select **Reports > Wired Products** from the main menu.

   The **Wired Products** report displays.

2. Click the IP address of a product in the **IP Address** column.

   The Element Manager displays.

Launching a Telnet session

NOTE
Wireless access points in adaptive mode do not display in the Management application.

You can use Telnet to log in and issue command line-based commands to a device.

NOTE
The device must have a valid IP address. If the device does not have a valid IP address, the Telnet selection will not be available on the Tools menu or the shortcut menu. You must right-click the device icon, select **Properties**, and enter the device's IP address before you can open a Telnet session.

To launch the CLI, complete the following steps.

On the Product List or Topology Map (L2 or IP only), right-click a device and select **CLI through Server**.

The Telnet session window displays.

Configuration repository and backup management

NOTE
Requires Mobility 5.3 or later.

Configuration repository and backup allows you to display each product configuration, including the name of the product, the version number of the configuration, the software release the product is running, and the product type, compare configurations, and backup configurations to the management server.

Instructions for configuration repository and backup are detailed in "Configuration Repository and Backup" on page 743 and include information about the following:

- "Saving the configuration status" on page 746
- "Viewing the configuration" on page 748
- "Restoring a configuration" on page 750 (You can only restore configurations as startup.)
- "Searching the configuration repository" on page 751

CLI configuration management

CLI configuration provides a text-based interface that allows you to enter command line interface (CLI) commands to create configurations and reports for IronWare and Network OS devices. You can deploy the configurations and reports on demand or at a scheduled time.

Instructions for creating product and monitoring configurations are detailed in Chapter 25, "CLI Configuration Management" and include information about the following:

- "Creating a new product configuration" on page 779
- "Creating a monitoring configuration" on page 795
- "Editing the Motorola Controller CLI responses properties file" on page 792

Some controller CLI commands require you to confirm command execution. By default, the Management application confirms "Yes" to all confirmation commands. If you want to change the confirmation command to "No" or "Abort", complete the following steps.

1. Open the ipConfig.properties (located in Install_Home\conf\) file in a text editor.
2. Edit the flags, as needed.

```
# This flag will control the execution of Network OS and Controller
confirmation CLI commands.
# For example, reload or copy running-config startup-config. With this option
# you can pass either yes(1) or no(2) or stop the execution(3)
#
CLIConfigManager.ValueForConfirmationCLICommands=1
CLIConfigManager.ValueForConfirmationCLICommands.MinInt=1
CLIConfigManager.ValueForConfirmationCLICommands.MaxInt=3
CLIConfigManager.ValueForConfirmationCLICommands.IsDisplay=false
```

3. Save and close the file.

Cluster mode

A cluster is a set of wireless controllers working collectively to provide redundancy and load sharing. You can discover wireless controllers in cluster mode.

To verify that the wireless controller is in cluster mode, check the following:

1. Check the **Properties** dialog box.

   Right-click the wireless controller and select **Properties**.

   The **Properties** dialog box displays.

   - If the controller is the active controller, the Access Points tab is included.
   - If the controller is the standby controller, the Access Points tab is not included.

2. Check the Detailed AP Products report (refer to "AP Products report" on page 422).

   For wireless controllers in cluster mode, it should show the cluster name ("Detailed AP Products report" on page 423)

3. Check the Wired Products report (refer to "IP Wired Products report" on page 1233).

   In the Wired Products report, click the controller in cluster mode to display the Cluster details:

   - **Cluster Name** — The cluster name.
   - **Cluster Mode** — The cluster mode of the AP. Options include Active and Standby.
     - If the controller is the active controller, the cluster mode is Active.
     - If the controller is the standby controller, the cluster mode is Standby.
   - **Cluster members** — The IP address of the controllers in cluster mode.

4. Check the port group ("Port Groups" on page 122) connected to the AP.

   The port group should only show the port information for the active controller in clustering mode.

VLAN management

You can use VLAN Manager to view existing Virtual Local Area Network (VLAN) configurations on the wireless products and the network.

Instructions for configuring policy monitors are detailed in Chapter 27, "VLAN Management" and include information about the following:

"Displaying a list of VLANs" on page 822

"VLAN Manager tabs" on page 822

"Displaying VLANs in the VLAN view" on page 823

"Displaying VLANs by products" on page 825

Performance management

NOTE
Wireless access points in adaptive mode do not display in the Management application.

Historical performance enables you to collect data from managed wireless devices. You can use the provided data collectors or create your own data collectors.

Instructions for collecting historical performance data are detailed in "IP historical performance monitoring" on page 995.

Policy Monitors

Use this feature to provide best practice guidelines for network setup at the fabric, switch, port and device level as well as software configurations at the product and the Management application level.

Instructions for configuring policy monitors are detailed in Chapter 36, "Policy Monitor" and include information about the following:

- "Adding a policy monitor" on page 1108
- "Editing a policy monitor" on page 1115
- "Configuration rules" on page 1116
- "Running a policy monitor" on page 1135
- "Viewing a policy monitor report" on page 1136

Fault management

Fault management enables you to monitor your network using the following methods:

- Monitor logs for specified conditions and notify you or run a script when the specified condition is met.
- Create event-based policies, which contain an event trigger and action.
- Configure E-mail event notification.

Instructions for configuring fault management are detailed in Chapter 37, "Fault Management".

AP Products report

The **AP Products** report displays general and detailed configuration information about AP products that are under the management server.

The information on the report comes from the software image version that is in the management application for that product. To ensure that the latest configuration information is in the management application, run the Discovery process or resynchronize the product.

To view the AP Products report, select **Reports > AP Products** from the main menu.

The **AP Products** report displays.

The **AP Products** report contains the fields and components detailed in Table 41.

TABLE 41 AP Products report

Field/Component	Description
AP Products Count	The number of AP products in the report.
Product status	Whether the AP is online (green icon), offline (red icon), or pending adoption (gray icon).
Name	The name of the product. Click to launch the **Detailed AP Report** (refer to Table 42).
Connected Switch	The name, IP address, and port number of the switch connected to the AP.
Controller	The name and IP address of the controller managing the AP.
Cluster Name	Controller cluster name.
MAC Address	The AP product MAC. Click to launch the **Detailed AP Report** (refer to Table 42).
Model	The model of the AP.
RF Domain Name	The RF domain name set for the AP.
Profile Name	The AP profile name.
Serial Number	The serial number of the AP.
Firmware	The firmware level of the AP.
Client Count	Number of wireless clients or stations connected to or associated with the AP.
Last Scanned	The date and time the last time the AP was scanned.
Export list	Click to export the report. For more information, refer to "Exporting and saving IP reports to a file" on page 1232.
E-mail list	Click to e-mail the report. For more information, refer to "Exporting IP reports to e-mail recipients" on page 1232.

The **Detailed AP Products** report contains the fields and components detailed in Table 42.

TABLE 42 Detailed AP Products report

Field/Component	Description
Status	Whether the AP is online (green icon), offline (red icon), or pending adoption (gray icon).
Name	The device name used to identify AP.
MAC Address	The AP device MAC.
Model	The model of the AP.
Serial Number	The serial number of the AP.
Firmware version	The firmware level of the AP.
Connected Switch	IP address of the controller or switch connected to the AP. Also displays the port number if the AP is directly connected.
Controller	IP address of the controller which manages the AP. Also displays the port number if the AP is directly connected.
Cluster Name	The controller cluster name.
Profile Name	The AP profile name.
RF Domain Name	The RF domain name set for the AP.
Location	The location set for the AP.
Contact	The contact set for the AP.
Time Zone	The time zone set for the AP.
Country	The country set for the AP.
VLAN for Control Traffic	The VLAN for control traffic set for the AP.
Client count	The number of wireless clients or stations connected or associated to the AP.
Export list	Click to export the report. For more information, refer to "Exporting and saving IP reports to a file" on page 1232.
E-mail list	Click to e-mail the report. For more information, refer to "Exporting IP reports to e-mail recipients" on page 1232.

Chapter

VCS Management

14

In this chapter

VCS

Network OS VCS™ technology is a Layer 2 Ethernet technology that allows you to create flatter, virtualized, and converged data center networks. VCS technology is scalable, permitting you to expand your network at your own pace.

VCS technology comprises the following concepts:

- Ethernet fabric
- Distributed intelligence
- Logical chassis

When two or more VCS mode-enabled switches are connected together, they form an Ethernet fabric and exchange information among each other to implement distributed intelligence. To the rest of the network, the Ethernet fabric appears as a single logical chassis.

VCS mode types

Beginning with Network OS 4.0, VCS mode encompasses two mode types:

- Fabric cluster mode (shown in Figure 154)—The data path for nodes is distributed, but the configuration path is not distributed. Each node maintains its configuration database independently.
- Logical chassis cluster mode (shown in Figure 155)—Both the data and configuration paths are distributed. The entire cluster can be configured from the principal node. Logical chassis mode requires Network OS 4.0 or later.

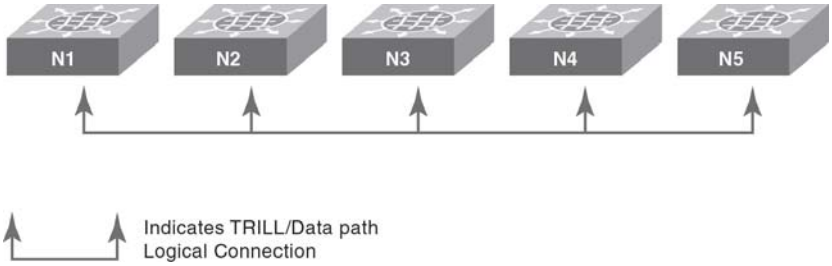


FIGURE 154 Fabric cluster mode

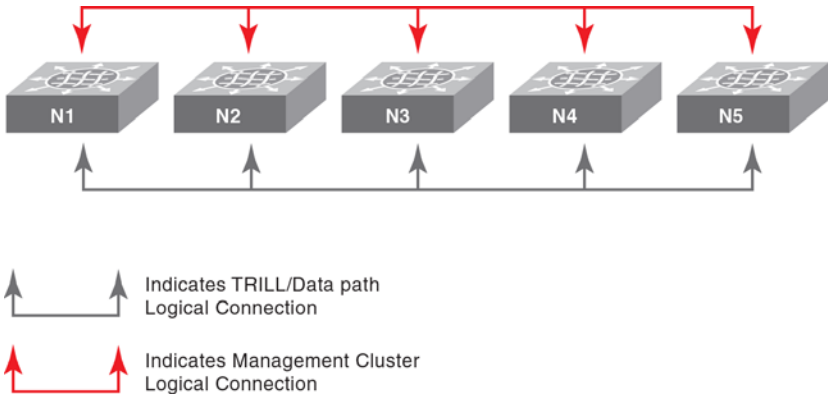


FIGURE 155 Logical chassis cluster mode

For more information about fabric cluster and logical chassis cluster modes, refer to the *Network OS Administrator's Guide*.

The term *VCS mode* refers to both fabric cluster mode and logical chassis cluster mode unless otherwise indicated.

Ethernet Fabrics view management

The Ethernet Fabrics view displays a map of the traffic for VCS devices on your network. To view the fabric members and Transparent Interconnection of Lots of Links (TRILL) connections for a fabric, double-click the fabric in the Product List. To display the topology map for Ethernet Fabrics, you must have the Main Display - Ethernet Fabric privilege. For more information about privileges, refer to "User Privileges" on page 1283.

The Ethernet Fabrics view Product List contains all the VCS fabrics known to the system. Within each VCS fabric, nodes that are part of that VCS fabric display. You can only view one VCS fabric at a time. Missing TRILL links are not displayed in the Ethernet Fabrics topology.

Logical chassis cluster operations

This section contains these topics:

- "Logical chassis cluster mode discovery"
- "Administratively removing a node from a logical chassis cluster"
- "How the Management application handles a cluster mode change"

Logical chassis cluster mode discovery

The **State** column of the **Discover Setup - IP** Dialog (Figure 156) is applicable only to nodes that are members of a logical chassis cluster. The possible node states are described later in this section.

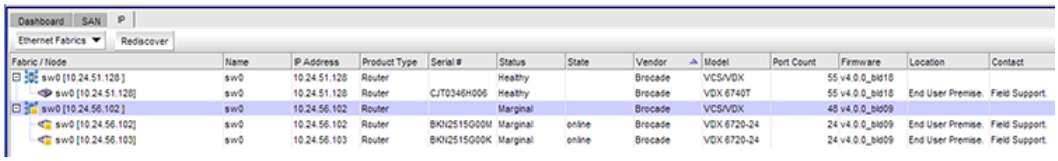


FIGURE 156 Discovery Setup - IP dialog box with node state for logical chassis cluster

Logical chassis cluster discovery includes the following behavior:

- Manual- or profile-based discovery is the same as for a cluster in fabric cluster mode.
- Uses the IP address of any member of the logical chassis cluster for discovery.
- Sets the cluster IP address to the IP address of the principal node.

NOTE
You can change the principal node for the cluster by running the **logical-chassis principal-priority** command from the Network OS prompt. For more information, refer to the *Network OS Command Reference*.

- Principal-switch failover does not occur if the cluster is unstable (for example, if the chassis had been disabled for maintenance) because refresh collection will fail.
- If the cluster is configured with a virtual IP address before its discovery, and then discovery is initiated, the cluster IP displays the virtual IP address instead of the IP address of the principal node.

- If the cluster is configured with a virtual IP address after it is discovered by the Management application, the virtual IP address is collected and saved in the database for the next lazy polling or next adaptive collection.
- If another switch becomes the principal switch, the Management application sets the cluster IP address to that of the new principal switch at the next lazy polling or next adaptive collection.
- The **State** column in the **Discover Setup - IP** dialog applies only to nodes that are in logical chassis mode. Refer to Figure 156. Possible states are:
  - Online—A node that is currently connected and operational.
  - On discovery, only online members are considered active cluster members. The Management application server collects the device, port, and LAG information of active cluster members. The the Management application client displays the member node as a cluster member in the Ethernet Fabrics topology.
  - Offline—A cluster member node that cannot be reached by the primary cluster node.
  - On refresh, if the member was an active member of a cluster and is now offline, the member is marked as missing. If the member is not online after three consecutive short ticks, auto-discovery gets initiated. If auto-chasing fails, the member remains missing.
  - Rejoining—A node that is in the process of rejoining its cluster.
  - On refresh, if the member was an active member of the cluster and is now rejoining, then the member is marked as missing. If the member is not online after three consecutive short ticks, auto discovery gets initiated. If auto chasing fails, the member remains missing.
  - Replacing—A node that is being replaced.
  - On refresh, if a member node is in the Replacing state, the member is shown as missing.
  - If the member is in the Replacing state for more than three consecutive short ticks, auto-discovery gets initiated. If auto-chasing fails, the member remains missing.

Administratively removing a node from a logical chassis cluster

You can remove a node from a logical chassis cluster by using the Network OS command line interface. For instructions, refer to the *Network OS Administrator's Guide* and the *Network OS Command Reference*, versions 4.0 or later.

Once the node is removed, all configurations corresponding to that node are removed from the cluster configuration database.

The deleted node gets rebooted automatically and boots in VCS-disabled mode.

The deleted node also gets marked as missing in the cluster.

The Management application initiates auto-discovery immediately, and the deleted node gets rediscovered in its current state.

As an example, Figure 157 shows the **Discover Setup - IP** dialog box before the administrator removes a node from the cluster.

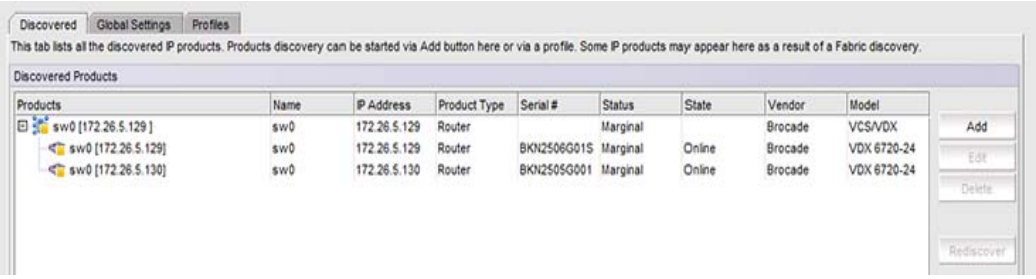


FIGURE 157 Discover Setup - IP dialog box before removal of node

Figure 158 shows the **Discover Setup - IP** dialog box after the administrator has removed the node with the IP address of 172.26.5.130 from its logical chassis cluster.

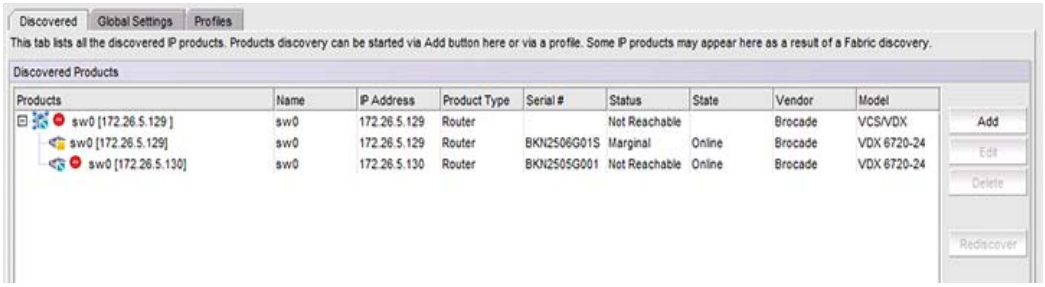


FIGURE 158 Discover Setup - IP dialog box after disabling the node from logical chassis cluster

Figure 159 shows the **Discover Setup - IP** dialog box after The Management application has performed rediscovery. The node with the IP address of 172.26.5.130 is shown as a degraded link.

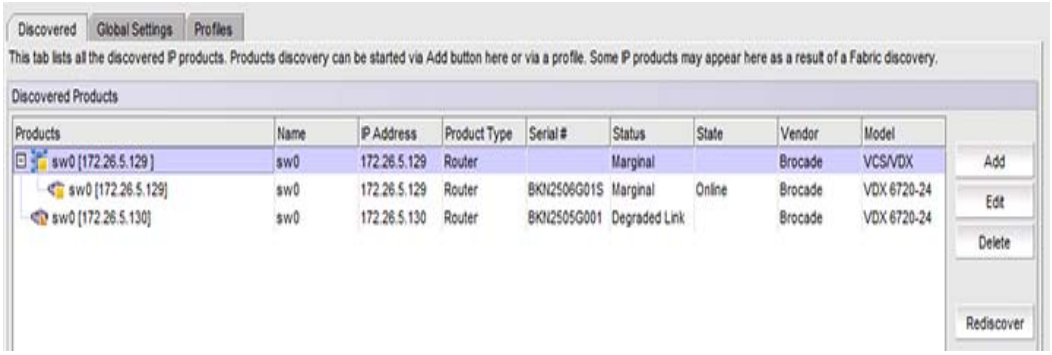


FIGURE 159 Discover Setup - IP dialog box after rediscovery

How the Management application handles a cluster mode change

In Network OS release 4.0, an administrator can change the mode of a cluster from fabric cluster mode to logical chassis cluster mode, and vice versa. For instructions, refer to the *Network OS Administrator's Guide* and the *Network OS Command Reference*.

NOTE
All cluster-specific configurations are lost during a cluster-mode change.

On refresh collection, the Management application detects the mode change and retains all database entries related to the cluster.

Serial firmware update and activation for Network OS devices

With Network OS release 4.0, you can update and activate firmware on an entire cluster (either logical chassis mode or fabric cluster mode), on selected nodes in the cluster, or on nodes in standalone mode, by performing the following steps.

1. Click the **IP** tab in the upper-left corner of the Management application.
2. Select **Ethernet Fabrics** from the view list on the Product List toolbar.

   Cluster node members (or root node) are displayed, depending on your configuration.
3. Select the desired node or nodes for firmware updates and activation.
4. Right-click the highlighted nodes, then select **Firmware > Firmware Management.**

   NOTE
   If you are performing a firmware activation (but not a serial update) on only one node, you can highlight this node, then perform a right-click and select **Firmware > Firmware Activate.** If this is the only action you want to perform, you are done and do not need to continue with the steps below.
5. In the **Firmware Management** dialog box, click the **Unified Firmware Images** tab.
6. Click **Update**.
7. From the **Hardware Type** list, select **VDX**.
8. Use the **Serial Update** and **Firmware Activate** check boxes as desired. For example:
   - You can select both boxes and enable the **Firmware Activate** check box to activate firmware on each node in a serial process.
   - You can leave the **Serial Update** check box clear and enable the **Firmware Activate** check box to activate firmware on each node in a parallel process.
   - You can select the **Serial Update** check box and leave the **Firmware Activate** check box unselected to begin the firmware download serially on selected nodes while delaying firmware activation on each node.
9. Click **Next**.
10. Follow any additional online instructions, and the procedure(s) that you selected begin.

Support for Network OS VDX 2740 embedded switch

The Network OS VDX 2740 switch is a 10GB VDX, embedded Network OS switch module for IBM Pure System Chassis. The VDX 2740 switch gets discovered by the Management application in the same manner as any other device. Upon discovering this switch, the Management application registers as the Element Manager for the VDX 2740 switch. The Management application as Element Manager is available only for the VDX 2740 switch.

To launch the Management application as Element Manager, enter the IP address of the Network OS VDX 2740 switch in a browser address bar and hit Return.

NOTE
The Network OS VDX 2740 switch requires firmware version *nos4.0.0_bbd* .

Network OS

Network OS is a scalable network operating system available for the Network OS data center switching portfolio products, including the VDX product line. Purposely built for mission-critical, next-generation data centers, Network OS supports the following capabilities:

- Simplified network management

  Network OS VCS technology, a fabric-based Layer 2 Ethernet technology that includes virtual fabric switching, simplifies network management in next-generation virtualized data centers with auto-provisioning and self-healing capabilities.

- High resiliency

  VCS-based distributed computer service improves network resiliency using proven link state routing.

- Improved network utilization

  TRILL-based Layer 2 routing service provides equal-cost multipaths in the network, resulting in improved network utilization.

- Server virtualization

  Automatic Migration of Port Profiles (AMPP) functionality provides fabric-wide configuration of Ethernet policies, achieves per-port profile forwarding, and enables network-level features to support virtual machine (VM) mobility.

  Refer to "Port profile configuration using the management application" on page 435 for information about AMPP configuration.

- Network convergence

  The Data Center Bridging (DCB)-based lossless Ethernet service provides isolation between IP and storage traffic over a unified network infrastructure. Multi-hop Fibre Channel over Ethernet (FCoE) allows an FCoE initiator to communicate with an FCoE target that is a number of hops away.

  Refer to "DCB configuration management" on page 486 for information about lossless Ethernet services.

VCS product groups

The standalone Network OS switches and the VCS fabric are treated as a single Layer 2 (L2) switch for both static and dynamic product groups. The product group membership cannot contain fabric members. The standalone Network OS VDX switches are shown in Table 43.

TABLE 43 Network OS-supported hardware

Device name	Firmware level required
Network OS VDX 2730 10 Gbps connection blade	v2.1.1_fuj
Network OS VDX 2740 switch	nos4.0.0_bbd
Network OS VDX 6710 switch	2.1 or later
Network OS VDX 6720-24 switch	2.1 or later
Network OS VDX 6720-60 switch	2.1 or later
Network OS VDX 6730-32 switch	2.1 or later
Network OS VDX 6730-76 switch	2.1 or later
Network OS VDX 8770-4 switch	3.0 or later
Network OS VDX 8770-8 switch	3.0 or later
Network OS VDX 6740 switch	4.0 or later
Network OS VDX 6740T switch	4.0 or later

Static product group

The standalone VDX switch and the VCS fabric can be added as a static product group member. The fabric members, however, are not included in the available product panel.

Dynamic product group

The standalone VDX switch and the VCS fabric are included when the dynamic product group is defined. The criteria search and filter the fabrics based on user-defined search criteria. The search criteria do not consider fabric members.

Port profiles

A port profile is a collection of network policies supported by the switch. By configuring port profiles on the Network OS VDX switch (refer to Table 43 for a list of supported VDX switches), the virtual machine (VM) that is configured on the virtual network interface card (vNIC) can migrate to any other port on that switch, but still retain the same network policies.

The default port profile, shown in Figure 160, contains the entire configuration needed for a VM to obtain access to the LAN and SAN.

NOTE
FCoE sub-profiles can be applied on default port profiles only and are supported on Network OS version 2.1 and later. You can view the FCoE profile association on Network Advisor version 11.3.0 and later.

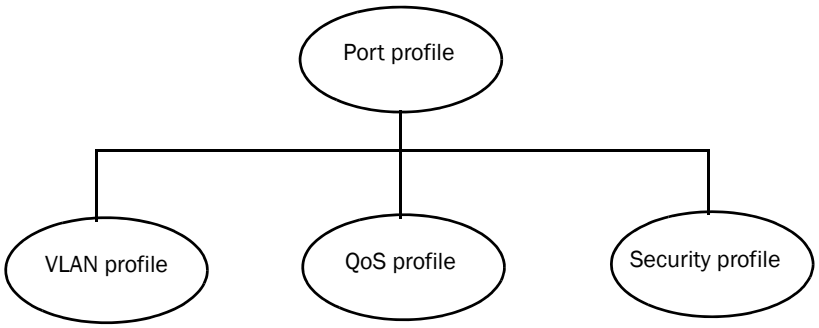


FIGURE 160 Port profile contents

NOTE
A port profile does not contain some of the interface-level configurations, such as LLDP, SPAN, LAG, and so on.

AMPP characteristics

Note the following points regarding the Automatic Migration of Port Profiles (AMPP) feature:

- Port groups and port profiles are collections of network policies. The vNICs inherit these network policies.
- Port profiles are associated with physical switches.
- VMs can have one or more vNICs, and port profiles are applied on the switch ports where vNICs are learned.
- Port profiles are reapplied to a new switch port if the same vNIC is learned on a new port.
- When a port is configured in port profile mode, the downlink profile is activated on the ports. A properly configured downlink profile enables all vNIC traffic to pass through, allowing the switch to perform MAC learning. There is one downlink profile per switch and the downlink profile cannot be deleted.

Life of a port profile

A port profile during creation goes through multiple states. Port profiles go through the following states:

- Created — This state specifies that a port profile is created but may not be complete when the port profile is created or modified.
- Activated — This state specifies that a port profile is activated and is available for MAC address-to-port profile association. If the created port profile is not complete, the activation fails. You must resolve any conflicts or dependencies and reactivate the port profile.

- Associated — This state specifies that one or more MAC addresses have been associated with this port profile within the fabric.
- Applied — This state indicates that the port profile is applied on the profiled port where the associated MAC address appears. Configuration of two different port profiles can coexist on a profiled port, but the application of the later port profile fails if there is a conflict.

The port profile states are configured using the Network OS command line interface. For complete configuration details, refer to the *Network OS Command Reference*.

AMPP events and behavior

Table 44 describes the AMPP events and the applicable failure behaviors.

For complete information about configuring AMPP, refer to the *Network OS Administrator's Guide* and the *Network OS Command Reference*.

TABLE 44 AMPP behavior and failure descriptions

AMPP event	Applicable behavior and failures
Create port profile	If the port profile does not exist, then it is created. If it exists, then it is available for modification (if it is not yet activated).
Activate port profile	If the port profile configuration is not complete, activation fails. Unless the port profile is activated, it is not applied on any switch port. If all the dependency validations succeed, the port profile is in the active state and is ready for association.
De-activate port profile	This event removes the applied port profile configuration from all the profiled ports. De-activation is allowed even if there are MAC addresses associated with the port profile.
Modify port profile	A port profile can be edited only in the pre-activation stage. The port profile is set to the inactive state if any conflicting attributes are configured or some dependent configuration is not completed, and any attempt to associate the port profile to a MAC address may not be allowed.
Associate MAC addresses to a port profile	If mapping already exists with another port profile, AMPP does not allow a MAC address to be mapped to multiple port profiles. If mapping does not exist, the port is configured to allow the MAC address with all the policies specified in the port profile applied to that MAC address on that port or switch.
De-associate MAC addresses from a port profile	If mapping exists, all the policies configured for a specific MAC address are removed from that port or switch.
Deleting a port profile	An in-use error is generated if the port profile is in an activated state. AMPP forces you to de-activate the profile before deleting. If the port profile is in an inactive state, then deletion of the port profile removes all the MAC address associations as well.
Modifying port profile content when in an associated state	An in-use error is generated if the port profile is already activated.
Moving the VM MAC address and notifying the fabric	All policies associated with the port profile ID are mapped on the MAC address and applied to the new port in the fabric.
Unused port profile	You must manually remove the MAC address mapping to remove any MAC address association.

Port profile configuration using the management application

You can manage MAC addresses and port profiles from the **Port Profiles** tab of the **Fabric_Name Properties** dialog box, as shown in Figure 161.

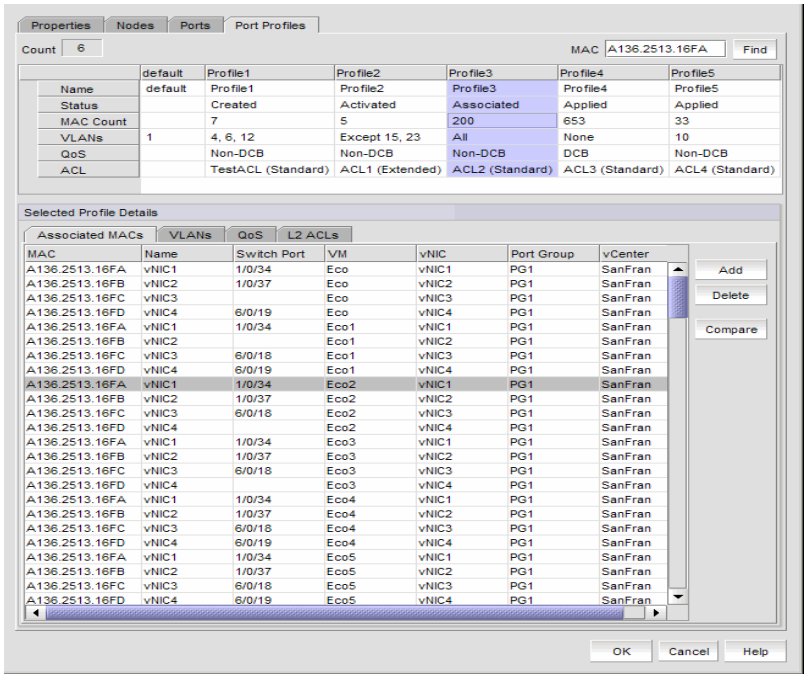


FIGURE 161 Fabric_Name Properties dialog box — Port Profile tab

Assigning MAC addresses to a port profile

Use the **Assign MACs** dialog box to select discovered Media Access Control (MAC) addresses and assign them to the selected port profiles. A maximum of 16,000 MAC addresses can be assigned to a port profile.

NOTE
MAC addresses cannot be added until the profile is activated. You must use the command line interface to activate the port profile. Refer to the *Network OS Command Reference* for instructions.

1. Select a VCS-capable switch from the device tree.
2. Right-click and select **Properties**.

   The **Fabric Properties** dialog box displays.
3. Click the **Port Profiles** tab.
4. In the **Selected Profile Details** area, click the **Associated MACs** tab.
5. Click **Add**.

   The **Assign MACs** dialog box displays, as shown in Figure 162.

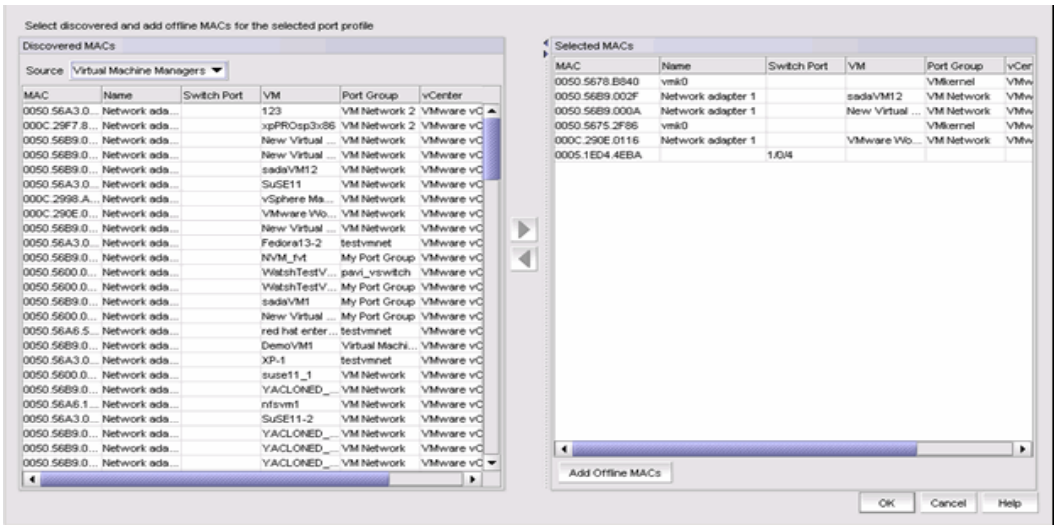


FIGURE 162 Assign MACs dialog box

6. From the **Source** list, select **Virtual Machine Managers** or **Switch Port Connectivity** as the source of the discovered MAC address.
7. Select a discovered MAC address to assign to the port profile and click the right arrow button to add it to the **Selected MACs** list.
8. Click **OK**.

Related topics

- "Comparing port profiles"
- "Deploying port profiles"

Managing offline MAC addresses

To add unique MAC addresses to the **Discovered MACs** list where you can assign them to a port profile, complete the following steps.

1. Select a VCS-capable switch from the device tree.
2. Right-click and select **Properties**.

   The **Fabric Properties** dialog box displays.
3. Click the **Port Profiles** tab.
4. In the **Selected Profile Details** area, click the **Associated MACs** tab.
5. Click **Add**.

   The **Assign MACs** dialog box displays.
6. Click **Add Offline MACs**.

   The **Assign Offline MACs** dialog box displays, as shown in Figure 163. Use this dialog box to add, remove, or import offline MAC addresses.

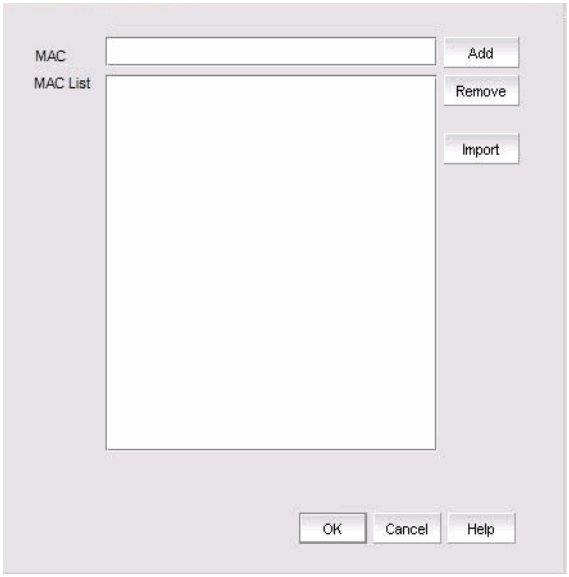


FIGURE 163 Assign Offline MACs dialog box

7. To manage offline MAC addresses, perform one of the following tasks:
   - To assign an offline MAC address to the selected, activated profile, enter the MAC address in the **MAC** list and click **Add**. Alternatively, select an offline MAC address from the **MAC List** and click **Add** to assign it to the Port Profile list.
   - To remove a MAC address from the **MAC List**, select it from the list and click **Remove**.
   - To select and import a CSV file, click **Import**.
8. Click **OK** to save the changes.

Comparing port profiles

To summarize differences between the original port profiles and profiles on other switches, complete the following steps.

NOTE
A MAC address can be associated with only one profile at a time.

1. Select a VCS-capable switch from the device tree.
2. Right-click and select **Properties**.

   The **Fabric Properties** dialog box displays.
3. Click the **Port Profiles** tab.
4. In the **Selected Profile Details** area, click the **Associated MACs** tab.

   If the associated MAC address is not selected, the **MAC Match** button is disabled under the **Profile Comparison Summary** dialog box.

5. Click **Compare**.

   The **Profile Comparison Summary** dialog box displays, as shown in Figure 164.

NOTE
A green circle icon in the comparison summary indicates a complete match to the MAC address on the target switch; a yellow triangle icon indicates a partial match.

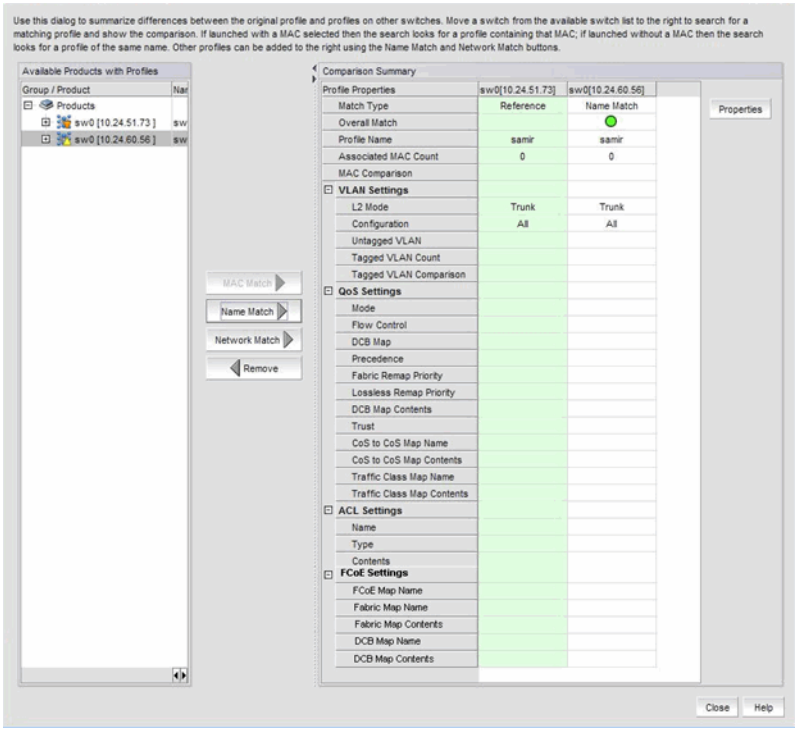


FIGURE 164 Profile Comparison Summary dialog box

6. Select a product from the **Available Products with Profiles** list and click one of the following match options as the comparison criteria. You can select multiple switches and fabrics.

   - **MAC Match** — Compares the MAC addresses in the reference profile to the MAC addresses contained in the target profile (one profile at a time). The MAC address comparison displays the following possible values:
     - Same — The MAC addresses in the reference and matched profiles are the same.
     - All Present — All of the MAC addresses in the reference profile are contained in the target profile, but the target profile has some additional MAC addresses.
     - Some Present — Some of the MAC addresses in the reference profile are contained in the target profile, but the target profile has more or fewer MAC addresses.
     - None Present — None of the MAC addresses in the reference profile are contained in the target profile.

- **Name Match** — Compares the original profile with the profile with the same name on the target switch.
- **Network Match** — Finds a profile on the target switch to provide the same networking settings on the target switch.

NOTE
Select a column or multiple columns in the **Comparison Summary** list, as shown in Table 45, and click **Remove** to remove it as matching criteria. The **Reference Profile** column cannot be removed.

TABLE 45 Profile Comparison Summary list

Field/Component	Description
Profile Properties	• Match Type — The type of comparison criteria: MAC match, name (profile name) match, or network match • Overall Match — The icon that signals if there is an exact match (green circle icon) or a partial match (yellow triangle icon) • Profile Name — The profile name that is compared against the target MAC address • Associated MAC Count — The number of associated MAC addresses • MAC Comparison — Indicates whether the compared MAC addresses are the same or different
VLAN Settings	• L2 Mode — The switch port mode of the port profile (access or trunk) • Configuration — One of the following VLAN configuration options: - All — Indicates that the port profile will allow all VLAN IDs - None — Indicates that the port profile will not allow any VLAN IDs - All Except <*VLAN IDs*> — Indicates that the port profile will allow any packet except the VLAN IDs specified - <*VLAN IDs*> — Indicates that the port profile will allow any packet with the VLAN IDs specified • Untagged VLAN — The port VLAN assigned to the interface as untagged • Tagged VLAN Count — The number of port VLANs assigned to the interface as tagged • Tagged VLAN Comparison — Indicates whether the compared tagged VLANs are the same or different

TABLE 45 Profile Comparison Summary list (Continued)

Field/Component	Description
QoS Settings	• Mode — The mode of Quality of Service (QoS) assigned to the port • Flow Control — Non-DCB mode. The Ethernet priority flow control mode of the port. Possible modes are Off, 802.3x pause, Tx On or Off, Rx On or Off. The default flow control mode is Off • DCB Map — The details about the CoS map and the Traffic Class map • Precedence — DCB mode. The map's priority • Fabric Remap Priority — DCB mode. The fabric remap priority of the port • Lossless Remap Priority — DCB mode. The FCoE lossless remap priority of the port • DCB Map Contents — DCB mode • Trust — Non-DCB mode. Whether the Ethernet trust of the port is enabled or disabled • CoS to CoS Map Name — Non-DCB mode • CoS to CoS Map Contents — Non-DCB mode • Traffic Class Map Name — Non-DCB mode • Traffic Class Map Contents — Non-DCB mode
ACL Settings	• Name — The name of the access control list (ACL) • Type — The ACL type (Extended or Standard) • Contents — The contents of the ACL
FCoE Settings NOTE: FCoE sub-profiles can be applied on default port profiles only and are supported on Network OS version 2.1 and later. You can view the FCoE profile association on Network Advisor version 11.3.0 and later.	• FCoE Map Name — The name of the FCoE map • Fabric Map Name — The name of the Fabric map • Fabric Map Contents — The parameters within the Fabric map • DCB Map Name — The name of the DCB map • DCB Map Contents — The parameters within the DCB map

Deploying port profiles

The **Deploy Port Profiles to Products** dialog box allows you to commit switch-level configuration changes to one or more target switches.

1. Select a VCS-capable switch from the device tree.
2. Right-click and select **Properties**.

   The **Fabric Properties** dialog box displays.
3. Click the **Port Profiles** tab.
4. Configure the port profile and click **OK** to launch the **Deploy Port Profiles to Products** dialog box, shown in Figure 165.

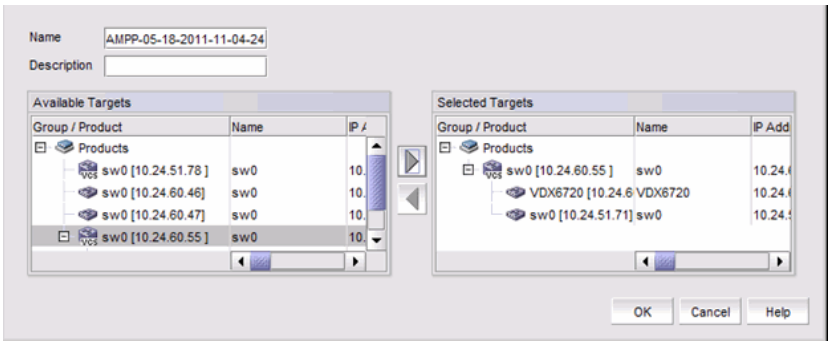


FIGURE 165 Deploy Port Profiles to Products dialog box

5. Select an available target from the **Available Targets** list and click the right arrow button to move the target selected for configuration deployment to the **Selected Targets** list.

NOTE
If a fabric is selected and moved in a VCS fabric, all members are moved to the **Selected Targets** list. Individual members of a VCS fabric can be added and removed from the **Selected Targets** list.

6. Click **OK**.

   The **Deployment Status** dialog box displays.

7. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected devices.
8. Click **Close** to close the **Deployment Status** dialog box.

System Monitor support on Network OS VDX platforms

System Monitor supports the Network OS VDX switches shown in Table 43. The following System Monitor features are supported on Network OS VDX platforms:

- FRU monitoring
- System thresholds
- Alert notifications
- Resource monitoring
- SFP monitoring
- Security monitoring
- Port statistics monitoring

Refer to the *Network OS Administrator's Guide* and *Network OS Command Reference* for configuration information.

FRU monitoring

System Monitor monitors the health of each component of the switch. The following FRUS and components are monitored:

- **Fan** — Configures fan settings
- **Power** — Configures power settings
- **Temp** — Displays the threshold for the temperature sensor component
- **CID-card** — Displays the threshold for the CID card component
- **SFP —** Displays the threshold for the small form factor pluggable (SFP) device
- **compact-flash** — Displays the threshold for the compact flash device
- **MM** — Displays the threshold for the management module
- **LineCard —** Displays the threshold for the line card
- **SFM** — Displays the threshold for the switch fabric module

System thresholds

System Monitor monitors the health of each component and, based on the threshold value, each component can be in a marginal state or a down state. Possible states for all monitored FRUs are removed, inserted, on, off, and faulty. A state of none indicates the switch is not configured. If the FRU is removed, inserted, or goes into a faulty state, System Monitor sends a RASlog message or an e-mail alert.

Refer to the "RAS System Messages" chapter of the *Network OS Message Reference* for details about each RASlog message.

Alert notifications

System Monitor provides event notifications by way of RASlog messages or e-mail alerts, depending on the configuration.

- **RASlog** — If a component is in a marginal state or a down state, System Monitor generates a RASlog message to alert the user. It also generates a separate RASlog message for the overall health of the switch.
- **Email** — An e-mail alert sends information about a switch event to a specified e-mail address. The e-mail specifies the threshold and describes the event, much like an error message.

Resource monitoring

System Monitor monitors CPU and memory usage of the system and alerts the user when configured thresholds are exceeded. When the CPU usage exceeds the limit, a system monitor alert is triggered. The default CPU limit is 75 percent. When configuring memory, the limit specifies a usage limit as a percentage of available resources.

When used to configure memory, monitoring the limit value must be greater than the low limit and less than the high limit. Three thresholds are supported for memory monitoring:

- High_limit — Specifies an upper usage limit for memory as a percentage of available memory. This value must be greater than the value set by the -limit parameter. The maximum is 90 percent. When memory usage exceeds this limit, System Monitor generates a CRITICAL RASlog message. The default is 80 percent.

- Limit — Specifies the default CPU limit. When the limit is exceeded, System Monitor sends out a RASlog WARNING message. When usage returns below the limit, System Monitor sends a RASlog INFO message. Valid values range from 0 to 80 percent, and the default value is different for different systems.
- Low_limit — Specifies a lower usage limit for memory as a percentage of available memory. This value must be less than the value set by the -limit parameter. When memory usage exceeds or falls below this limit, System Monitor generates a RASlog INFO message. The default for all platforms is 50 percent.

SFP parameter monitoring

System Monitor monitors the SFP parameters shown in Table 46.

TABLE 46 SFP parameter descriptions

SFP parameter	Description	Suggested SFP impact
Temperature	Measures the physical temperature of the SFP transceiver, in degrees Celsius.	High temperature suggests the SFP transceiver might be damaged.
Receive Power (RXP)	Measures the amount of incoming laser, in uWatts.	Describes the condition of the SFP transceiver. If this parameter exceeds the threshold, the SFP transceiver is deteriorating.
Transmit Power (TXP)	Measures the amount of outgoing laser, in uWatts.	Describes the condition of the SFP transceiver. If this parameter exceeds the threshold, the SFP transceiver is deteriorating.
Current	Measures the amount of supplied current to the SFP transceiver.	Indicates hardware failures.
Voltage	Measures the amount of voltage supplied to the SFP transceiver.	A value higher than the threshold indicates the SFP transceiver is deteriorating.

Security monitoring

System Monitor monitors all attempts to breach your SAN security, helping you fine-tune your security measures. If there is a security breach, System Monitor sends a RASlog alert. The following security areas are monitored:

- Telnet violation, which occurs when a Telnet connection request reaches a secure switch from an unauthorized IP address.
- Login violation, which occurs when a secure fabric detects a login failure.

Port statistics monitoring

System Monitor monitors port statistics on all external Gigabit Ethernet interfaces: 1 Gb, 10 Gb, and 40 Gb. When any monitored error crosses the configured high or low thresholds, an alert is generated.

Interface error types

Table 47 describes the interface counters that System Monitor monitors on external interfaces.

TABLE 47 Interface errors monitored by System Monitor

Interface error	Description	Port Fence support	Threshold defaults
CRC Align Errors	The total number of frames received that had a length (excluding framing bits but including Frame Check Sequence (FCS) octets) of from 64 through 1518 octets. The error indicates either a bad FCS with an integral number of octets (an FCS error) or a bad FCS with a non-integral number of octets (an Alignment error).	No	Low 12 Buffer 0 High 300
RX Symbol Error	The interface detects an undefined (invalid) symbol received. Large symbol errors indicate a bad device, cable, or hardware.	No	Low 0 Buffer 0 High 5
RX IFG Violated	A minimum-length interframe gap (IFG) between successive frames is violated. A typical IFG is 12 bytes.	Yes	Low 5 Buffer 0 High 100
RX Missing Termination Characters	The number of frames that terminated by anything other than the Terminate character; this includes termination due to the Error character.	No	Low 12 Buffer 0 High 300

NOTE
The default settings for the above high threshold, above low threshold, below high threshold, and below low threshold actions are None.

Ethernet fabric traceroute

NOTE
All nodes in the VCS cluster must have the NETCONF interface availability for L2TraceRoute and must be running Network OS 3.0.0 or later.

Traceroute diagnostics enables you to determine the connectivity, path, and reachability of the Ethernet fabric between a source port and a destination port within an individual VCS fabric. You can perform traceroute diagnostics from any RBridge where the source MAC address is learned in the VCS cluster and that RBridge becomes the starting node for the traceroute packet. Once configured, the traceroute request identifies the Equal Cost Multi-Path (ECMP) path a packet takes from the source address to a destination address. Traceroute performs a hop-by-hop inspection between two end-device MAC addresses to identify the traffic loss and any points of congestion in the path.

Tracing Ethernet fabric routes

1. To diagnose traceroute, you can do either of the following:
   - Select **Monitor > Diagnostics > Traceroute**.
   - Right-click the VM and select **Diagnostics > Traceroute**.
   - Right-click the VCS and select **Diagnostics > Traceroute**.

     The **Traceroute** dialog box displays (see Figure 166). The **Source** field displays the corresponding VM MAC addresses by default and the **Destination** field is blank.

     If you do not have the privilege to lauch traceroute, the following warning message displays:
     You do not have privilege to perform this operation.
     Click **OK** to close the warning message.

     If VCS is not managed or discovered by the Management application, the following error message displays:
     Unable to launch Traceroute dialog because the selected VM is not connected to VCS or the VCS is not managed by Network Advisor.
     Click **OK** to close the error message.

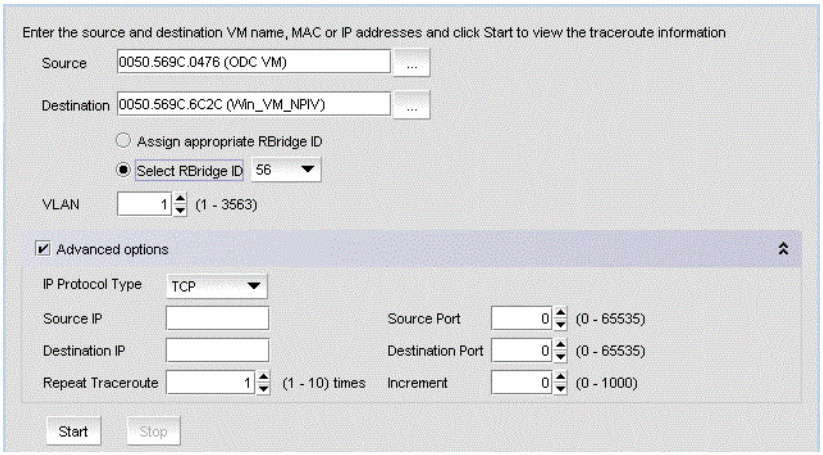


FIGURE 166 Traceroute dialog box

2. Enter a MAC address, VM name, or IP address in the **Source** field or click the Source button to select or search for a source address from the **Select Source - Traceroute** dialog box (see Figure 167).

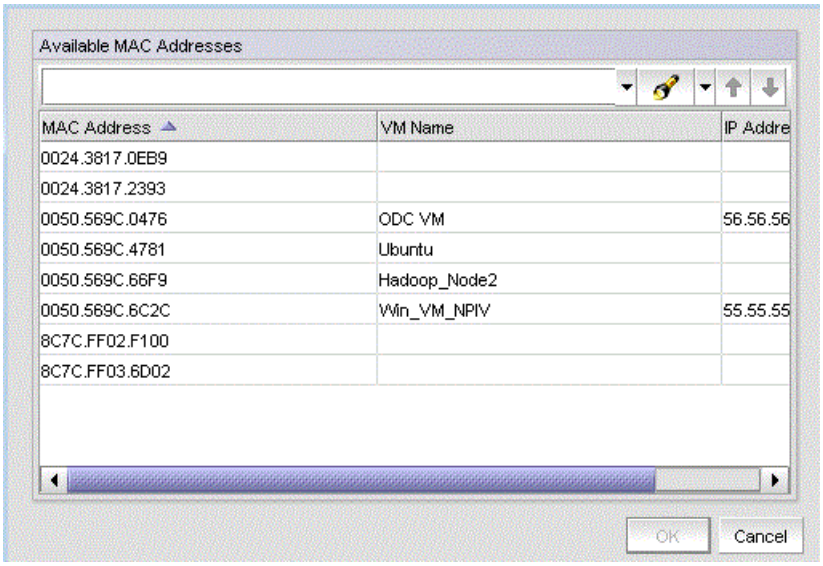


FIGURE 167 Select Source - Traceroute dialog box

In the **Select Source - Traceroute** dialog box, you can either search from the **Available MAC Addresses** list or select a row containing the required source MAC address, VM name, or IP address and click **OK**. This list contains all the discovered port MAC addresses (host or device) connected to the VCS cluster.

The format of the selected source address is displayed based on the conditions in the following table.

Source address format	Condition
MAC address (VM name) - if VM name exists	When a MAC address is entered and the focus is lost.
MAC address (VM name) - if VM name exists	When a VM name is entered and the focus is lost.
IP address (VM name) - if VM name exists	When an IP address is entered and the focus is lost.

3. Enter a MAC address, VM name, or IP address in the **Destination** field or click the Destination button to select or search for a destination address from the **Select Destination - Traceroute** dialog box.

In the **Select Destination - Traceroute** dialog box, you can either search from the **Available MAC Addresses** list or select a row containing the required destination MAC address, VM name, or IP address and click **OK**. This list contains all the discovered port MAC addresses (host or device) connected to the VCS cluster.

4. Choose one of the following options:
   - **Assign appropriate RBridge ID** — Select this option to use Address Finder to identify the RBridge ID of the source.

     The Management application finds the RBridge ID on which the MAC address is learned.
   - **Select RBridge ID** — Select this option to select an RBridge ID from the list of the RBridge IDs currently present in the cluster.

     Before you select an RBridge ID from the list, you must know on which RBridge ID the MAC address is learned.
5. Select a VLAN from the **VLAN** list.

   Valid values are from 1 through 3583.

   NOTE
   Both the source and destination must be on the same VLAN.

   To customize the traceroute packet, continue with step 6.

   To start the traceroute, go to step 14.
6. Select the **Advanced options** check box.
7. Choose one of the following options from the **IP Protocol Type** list:
   - **TCP**
   - **UDP**
8. Enter a source IP address (IPv4 only) in the **Source IP** field.
9. Enter a source port number in the **Source Port** field.

   Valid values are from 0 through 65535.
10. Enter a destination IP address (IPv4 only) in the **Destination IP** field.
11. Enter a destination port number in the **Destination Port** field.

    Valid values are from 0 through 65535.
12. Enter the number of times you want to repeat the traceroute request on the fabric in the **Repeat Trace Route** field.

    Valid values are from 1 through 10. The default is 1. There is a one-second delay between the requests.
13. Enter a value with which to increment the source and destination port numbers on each repeated request in the **Increment** field.

    Valid values are from 0 through 1000. The default is 1. If you do not want to increment the port on each repeated request, enter 0.

    For example, if you configure the source port to 5, the destination port to 7, the repeat count to 5, and the increment ports to 5, the port numbers shown in Table 48 are sent on each traceroute request.

TABLE 48 Trace Route example

Request	Source port number	Destination port number
1	5	7
2	10	12
3	15	17
4	20	22
5	25	27

14. Click **Start** to initiate the traceroute request.

    Click **Stop** to cancel the traceroute request.

NOTE
The traceroute request is not automatically cancelled on the switch. The switch continues until the request is complete.

The traceroute results display in table format at the bottom of the **Ethernet Fabrics Traceroute for** *Ethernet_Fabric* dialog box.

15. To review diagnostic results, select a traceroute request from the list on the **Diagnostics Results** tab.

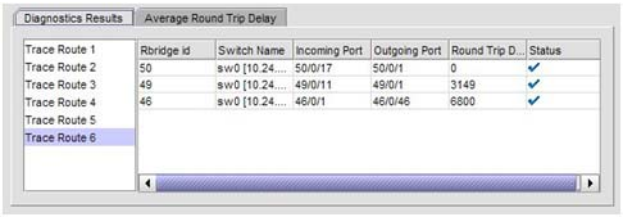


FIGURE 168 Ethernet Fabrics Traceroute for *Ethernet_Fabric* dialog box — Diagnostics Results tab

The **Diagnostics Results** tab updates dynamically as each traceroute request becomes available. The results list on the left contains a traceroute for each repeated request. The results table details the selected traceroute. Each row represents a hop and the data includes the following information:

- **RBridge ID**: The RBridge ID of the VCS member.
- **Switch Name**: The display name or IP address or display name and IP address of the VCS member (defined by you in the main window).
- **Incoming Port**: The port numbers in the path to the source RBridge from the destination RBridge.
- **Outgoing Port**: The port numbers in the path to the destination RBridge from the source RBridge.
- **Round Trip Delay**: The round trip delay in microseconds.

NOTE
The round trip delay for the starting RBridge (edge) is always 0 microseconds for a successful trace as this represents a self-loop.

- **Status**: Whether the traceroute succeeded or failed.

  NOTE
  A failed status indicates that the destination is not reachable from the outgoing port of this RBridge after the switch initiates the **traceroute** command.

16. To review the average round trip delay for the RBridge across the requests, click the **Average Round Trip Delay** tab.

    The **Average Round Trip Delay** tab displays the round trip data for the RBridge for all repeated requests:

    - **RBridge ID**: The RBridge ID of the VCS member.
    - **Switch Name**: The display name or IP address or display name and IP address of the VCS member (defined by you in the main window).
    - **Average**: The average round trip delay of all traceroute samples in microseconds for each hop.
    - **Traceroute** *number*: The round trip delay in microseconds for each hop.

      NOTE
      The round trip delay for the starting RBridge (edge) is always 0 microseconds for a successful trace as this represents a self-loop.

Exporting diagnostic data

You can export data to a CSV-formatted text file. To export data from the **Ethernet Fabrics Traceroute for** *Ethernet_Fabric* dialog box, complete the following steps.

1. Choose one of the following options:
   - To export diagnostic results, click the **Diagnostics Results** tab.
   - To export the average round trip delay for the RBridge across the requests, click the **Average Round Trip Delay** tab.
2. Right-click anywhere in the table and select **Export Table**.

   The **Save table to a tab delimited file** dialog box displays.
3. Browse to the directory where you want to save the data.

Chapter

Host Management

15

In this chapter

Host management

Extensive management operations are supported on the switches and fabrics of the SAN using the Management application. Adapters and hosts are visible as part of the fabrics managed by the Management application.

The Management application integrates with another manageability application called the Host Connectivity Manager (HCM) to provide complete management of the Host Bus Adapters (HBAs) and Converged Network Adapters (CNAs).

The Management application focuses on operations such as fault management, performance management, and configuration management for multiple adapters and adapter ports and security configuration using Fibre Channel Security Protocol (FC-SP) that is set up on the adapter port and the switch.

HCM supports management for individual adapters (4/8/16 Gbps HBAs), 10 Gbps CNAs, 10 Gbps or 16 Gbps Fabric Adapters, and other devices, such as the host, DCB ports, FCoE ports, and Ethernet ports.

The Management application, in conjunction with HCM, provides end-to-end management capability. For information about configuring, monitoring, and managing individual adapters using the HCM GUI or the Brocade Command Utility (BCU), refer to the *Adapters Administrator's Guide*.

Brocade adapters

The following sections describe the three Brocade adapter types:

- "Host Bus Adapters"
- "Converged Network Adapters"
- "Fabric Adapters"

Host Bus Adapters

Brocade offers five models of Fibre Channel Host Bus Adapters (HBAs). These models provide reliable, high-performance host connectivity for mission-critical SAN environments. The Brocade HBAs are listed in Table 49.

TABLE 49 Brocade Fibre Channel HBA models

Model number	Description	Number of ports
825	Dual-port stand-up HBA with a per-port maximum of 8 Gbps using an 8 Gbps SFP.[1]	2
815	Single-port stand-up HBA with a maximum of 8 Gbps using an 8 Gbps SFP.[1]	1
804[2]	Dual-port mezzanine HBA with a per-port maximum of 8 Gbps. This HBA installs in server blades that install in supported blade system enclosures.	2
425	Dual-port stand-up HBA with a per-port maximum of 4 Gbps using a 4 Gbps SFP.[3]	2
415	Single-port stand-up HBA with a maximum of 4 Gbps using a 4 Gbps SFP.[3]	1

[1] A 4 Gbps SFP installed in Brocade 815 or 825 HBAs allows 4, 2, or 1 Gbps speed only.
[2] Brocade 804 mezzanine cards connect to the embedded switch modules or embedded interconnect modules on the blade system chassis by way of an internal backplane and, therefore, no optical modules (SFP transceivers) are involved. With the exception of no SFP transceivers, the Brocade 804 mezzanine FC HBA card functions the same as the other Brocade HBAs.
[3] An 8 Gbps SFP installed in Brocade 425 or 415 HBAs allows 4 or 2 Gbps speed only.

Using Brocade HBAs, you can connect your server (host system) to devices on the Fibre Channel SAN. The combined high performance and proven reliability of a single-ASIC design makes these HBAs ideal for connecting hosts to SAN fabrics based on Brocade Fabric or M-Enterprise operating systems.

Converged Network Adapters

Table 50 describes available Brocade Converged Network Adapters (CNAs) for PCIe x 8 host bus interfaces, hereafter referred to as Brocade CNAs. These adapters provide reliable, high-performance host connectivity for mission-critical SAN environments.

TABLE 50 Brocade Fibre Channel CNA models

Model number	Port speed	Number of ports	Adapter type
1741M-k[1]	10 Gbps maximum	2	Expansion
1020	10 Gbps maximum	2	Stand-up
1010	10 Gbps maximum	1	Stand-up
1007[2]	10 Gbps maximum	2	Expansion

[1]The Brocade 1741M-k and Brocade 1007 are two-port 10 GbE CNAs that mount on a blade server that installs in a system enclosure. The adapter uses FCoE to converge standard data and storage networking data onto a shared Ethernet link. Ethernet and Fibre Channel communication are routed through the DCB ports on the adapter to the blade system enclosure midplane and onto the installed switch modules installed in the enclosure.

[2]The Brocade 1741M-k and Brocade 1007 CNAs connect to the embedded switch modules or embedded interconnect modules on the blade system chassis by way of an internal backplane and, therefore, no optical modules (SFP transceivers) are involved. With the exception of no SFP transceivers, the Brocade 1741M-k and Brocade 1007 CNAs function the same as the other Brocade CNAs.

For information on installing the Brocade CNAs on a blade server, refer to the *Brocade Adapters Installation and Reference Guide*.

Brocade CNAs combine the functions of a Host Bus Adapter (HBA) and Network Interface Card (NIC) on one PCIe x 8 card. The CNAs appear as NICs and Fibre Channel adapters to the host. These CNAs fully support FCoE protocols and allow Fibre Channel traffic to converge onto 10 Gbps Data Center Bridging (DCB) networks. FCoE and 10 Gbps DCB operations are simultaneous.

The combined high performance and proven reliability of a single-ASIC design makes these CNAs ideal for connecting host systems on Ethernet networks to SAN fabrics based on Brocade Fabric or M-Enterprise operating systems.

Fabric Adapters

Table 51 describes the available Brocade 1860 Fabric Adapter model. The Brocade 1860 provides dual mode support for the port. You can configure the port mode as a 16 Gbps Fibre Channel (FC) HBA and a 10 Gbps CNA mode using the Brocade Command Utility (BCU).

TABLE 51 Brocade Fabric Adapter models

Model number	Port speed	Number of ports
1860-1 860-2	16 Gbps FC HBA and 10 Gbps CNA or NIC	1 or 2
1867	16 Gbps FC mezzanine card	2

AnyIO™ technology

Although the Brocade 1860 Fabric Adapter can be shipped in a variety of small form-factor pluggable (SFP) transceiver configurations, you can change port function to the following modes using Brocade AnyIO™ technology, provided the correct SFP transceiver is installed for the port:

- HBA or Fibre Channel mode — This mode utilizes the Brocade Fibre Channel storage driver. An 8 or 16 Gbps Fibre Channel SFP transceiver can be installed for the port. The port provides Host Bus Adapter (HBA) functions on a single port so that you can connect your host system to devices on the Fibre Channel SAN. Ports with 8 Gbps SFP transceivers configured in HBA mode can operate at 2, 4, or 8 Gbps. Ports with 16 Gbps SFP transceivers configured in HBA mode can operate at 2, 4, 8, or 16 Gbps.

  Fabric Adapter ports set in HBA mode appear as “FC” ports when discovered in HCM. They appear as “FC HBA” to the operating system.

- Ethernet or NIC mode — This mode utilizes the Brocade network driver. A 10 GbE SFP+ transceiver must be installed for the port. This mode supports basic Ethernet, Data Center Bridging (DCB), and other protocols that operate over DCB to provide functions on a single port that are traditionally provided by an Ethernet Network Interface Card (NIC). Ports configured in this mode can operate at up to 10 Gbps. Fabric Adapters that ship from the factory with 10 GbE SFP transceivers installed or no SFP transceivers installed are configured for Ethernet mode by default.

  Fabric Adapter ports set in NIC mode appear as Ethernet ports when discovered in HCM. These ports appear as “10 GbE NIC” to the operating system.

- CNA mode — This mode provides all functions of Ethernet or NIC mode, plus adds support for FCoE features by utilizing the Brocade FCoE storage driver. A 10 GbE SFP+ transceiver must be installed for the port. Ports configured in CNA mode connect to an FCoE switch. The port provides all traditional CNA functions for allowing Fibre Channel traffic to converge onto 10 Gbps DCB networks. The ports appear as Network Interface Cards (NICs) and Fibre Channel adapters to the host. FCoE and 10 GbE operations run simultaneously.

  Fabric Adapter ports set in CNA mode appear as FCoE ports when discovered in HCM. These ports appear as “10 GbE NIC” to the operating system.

HCM software

The Host Connectivity Manager (HCM) is a management software application for configuring, monitoring, and troubleshooting Brocade HBAs and CNAs in a SAN environment. For instructions about how to install the HCM software, refer to the *Adapters Installation and Reference Manual.*

You can manage the software on the host or remotely from another host. The communication between the management console and the agent is managed using JSON-RPC over HTTPS or CIM-XML over HTTPS.

NOTE
All HCM, utility, SMI-S Provider, boot software, and driver installation packages, as well as the Driver Update Disk (DUD), are described in the *Adapters Installation and Reference Manual*.

HCM features

Common HBA and CNA management software features include the following:

- Discovery using the agent software running on the servers attached to the SAN, which enables you to contact the devices in your SAN.
- Configuration management, which enables you to configure local and remote systems. With HCM, you can configure the following items:
  - Brocade 4 Gbps and 8 Gbps HBAs
  - HBA ports (including logical ports, base ports, remote ports, and virtual ports) associated with the local host
  - Brocade 10 Gbps single-port and 10 Gbps dual-port CNAs
  - Brocade 16 Gbps FC adapters
  - DCB ports (CNA only)
  - FCoE ports (CNA only)
  - Ethernet ports (CNA only)
- Diagnostics, which enables you to test the adapters and the devices to which they are connected:
  - Link status of each adapter and its attached devices
  - Loopback test, which is external to the adapter, to evaluate the ports (transmit and receive transceivers) and the error rate on the adapter
  - Read/write buffer test, which tests the link between the adapter and its devices
  - FC protocol tests, including echo, ping, and traceroute
  - Ethernet loopback test (CNA only)
  - Diagnostic Port (D-Port) test
- Monitoring, which provides statistics for the SAN components.
- Security, which enables you to specify a Challenge Handshake Authentication Protocol (CHAP) secret and configure authentication parameters.
- Event notifications, which provide asynchronous notification of various conditions and problems through a user-defined event filter.

Host adapter discovery

The Management application enables you to discover individual hosts, import a group of hosts from a CSV file, or import host names from discovered fabrics. The maximum number of host discovery requests that can be accepted is 1000. Host discovery requires HCM Agent 2.0 or later.

ESXi host adapter discovery requires the Brocade HBA CIM provider to be installed on the ESXi host.

NOTE
Pure Fabric discovery alone shows adapters behind Access Gateway and all adapter ports as virtual. When you discover an adapter and ports using host discovery, the adapter and all its ports are shown as physical.

Instructions for discovering hosts are detailed in Chapter 3, “Discovery”.

VM Manager

A vCenter server can be discovered by adding a VM Manager to the Management application. Refer to Chapter 3, “Discovery” for information about discovering VM Managers.

Adding a VM Manager

1. Click **Add** on the **Discover VM Managers** dialog box.

   The **Add VM Manager** dialog box displays, as shown in Figure 169.

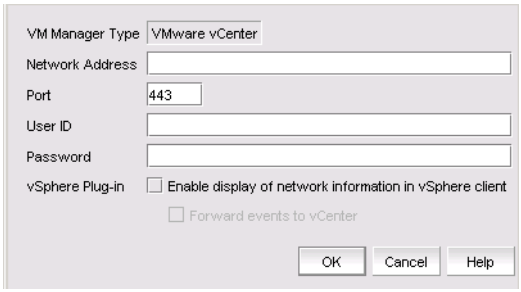


FIGURE 169 Add VM Manager dialog box

2. Enter the IP address or host name of the VM Manager (VMM) into the **Network Address** field. The maximum number of supported characters is 256.
3. Enter the VMM server port number into the **Port** field. The valid port number range is from 0 through 65536. The default port number is 443.
4. Enter the user ID into the **User ID** field to identify the user of the VMM. The maximum number of supported characters is 64.
5. Enter the password into the **Password** field. The maximum number of supported characters is 64.
6. Click **OK**.

The VMM discovery process begins. When complete, the vCenter server and all ESX and ESXi hosts managed by that vCenter display in the Host product tree.

Editing a VM Manager

The fields in the **Edit VM Manager** dialog box are identical to the fields in the **Add VM Manager** dialog box except for the **Network Address** field, which you cannot edit.

1. Click **Edit** on the **Discover VM Managers** dialog box.

   The **Edit VM Manager** dialog box displays.

2. Enter the VMM server port number into the **Port** field. The valid port number range is from 0 through 65536.
3. Enter the user ID into the **User ID** field to identify the user of the VMM. The maximum number of supported characters is 64.
4. Enter the password into the **Password** field. The maximum number of supported characters is 64.
5. Click **OK**.

   The VMM discovery process begins. When complete, the vCenter server and all ESX and ESXi hosts managed by that vCenter display in the Host product tree.

Deleting a VM Manager

You cannot delete an ESX host. Hosts can only be excluded or included. If you select a host from the **Discovered VM Managers** list in the **Discover VM Managers** dialog box and click **Delete**, the host displays in the **Previously Discovered Addresses** list.

HCM and Management application support on ESXi systems

Through the Brocade Adapters ESXi Management feature, ESXi systems support HCM and the Management application when CIM Provider is installed on these systems.

For installation and other information on CIM Provider, refer to the following publications:

- *CIM Provider for Brocade Adapters Developer's Guide*
- *CIM Provider for Brocade Adapters Installation Guide*

ESXi CIM listener ports

The Management application server uses two CIM indication listener ports to listen for CIM indications.

- HCM Proxy Service CIM Indication Listener Port — This port is used to listen for CIM indications from ESXi hosts managed through HCM instances launched by the Management application. You can learn the value of these ports through the **Port Status** dialog box.
- Fault Management CIM Indication Listener Port — This port is used to listen for CIM indications from ESXi hosts managed through the Management application's host adapter discovery.

The two ports described above are part of the range of ports reserved for use by the Management application server, configurable during installation from the Server Configuration wizard. Refer to the *Installation and Migration Guide* for server configuration instructions.

Adding host adapter credentials for ESXi

CIM-based discovery is available for ESXi versions 4.1 and later. The CIM server transport does not support operating systems other than ESXi.

NOTE
CIM server credentials are optional. If you do not provide credentials, basic authentication on the CIM server is disabled and the Management application attempts discovery without authentication.

The Protocol, Port, User ID, and Password fields on the **Add Host Adapters** dialog box are persisted when changing from HCM agent to CIM Server (ESXi only).

1. Select **Discover > Host Adapters**.

   The **Host Adapters** dialog box displays.

2. Click **Add**.

   The **Add Host Adapters** dialog box, shown in Figure 170, displays.

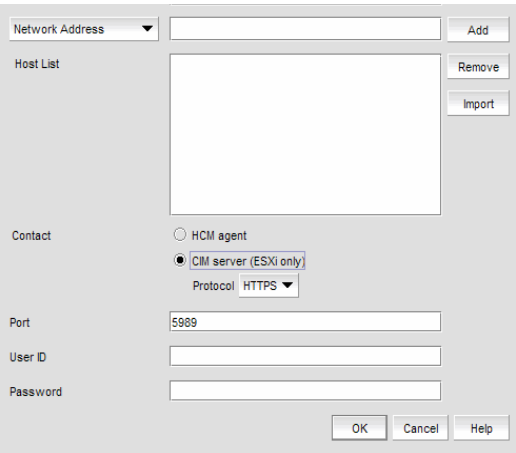


FIGURE 170 Add Host Adapters dialog box

3. Select **CIM server (ESXi only)** as the **Contact** option.
4. (*Optional*) Select **HTTP** or **HTTPS** from the **Protocol** list. HTTPS is the default.
5. Click **OK**.

Adapter software

The **Adapter Software** dialog box allows you to perform the following tasks:

- Select and import a driver file or delete existing drivers from the driver repository
- Update the driver to the hosts

NOTE
For Linux and Solaris systems, you cannot upgrade to driver file version 3.0.3.0. You must upgrade to version 3.0.3.1 or later.

The ability to update drivers to the hosts is available for hosts that are disovered through the Host Connectivity Manager (HCM) agent with driver version 2.3.0.0 or later. Driver updates cannot be performed for ESXi hosts, which are discovered using the CIM Server. Use the VMware vSphere Update Manager to update the drivers on ESXi hosts.

To update the drivers to selected hosts, complete the following steps.

1. Select **Host > Adapter Software** from the **Configure** menu.

   The **Adapter Software** dialog box, **Driver** tab, shown in Figure 171, displays.

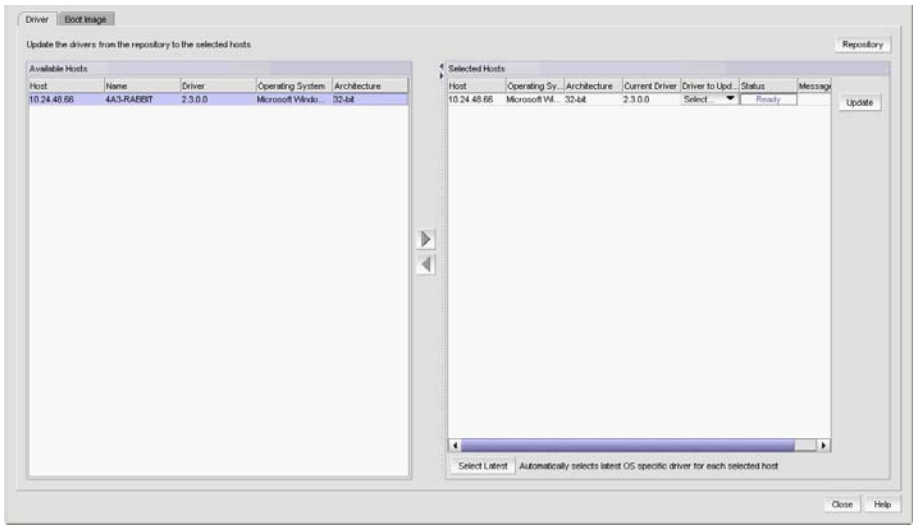


FIGURE 171 Adapter Software dialog box, Driver tab

2. Select one or more hosts from the **Available Hosts** list and click the right arrow button to move the selected hosts to the **Selected Hosts** list.

   The **Available Host** list displays the following information for hosts that are discovered through the HCM agent with driver version 2.3.0.0 or later:

   - Hosts — The IP address of the host.

- Name — The name of the host. The first three digits indicate the host's operating system; for example, WIN or LIN.
- Operating System — The host operating system; for example, Microsoft Windows or Red Hat Linux.
- Driver Version — The host's current driver version.
- Architecture — The host's architecture; for example, 32-bit or 64-bit.

3. Select one or more hosts from the **Selected Hosts** list. You can select mutliple hosts, but if the selected host count is greater than 20, a batch of 20 hosts is initiated for the driver update first and the remaining hosts are queued.

   The **Selected Hosts** list displays the following information for hosts that have been selected for the driver update:

   - Host — The IP address of the host.
   - Operating System — The host operating system; for example, Microsoft Windows or Red Hat Linux.
   - Driver to Update — Select the driver to update from the list.
   - Status — The ready status of the selected host.
   - Architecture — The host's architecture; for example, 32-bit or 64-bit.
   - Current Driver Version — The host's current driver version.
   - Message — Additional information pertaining to the selected host.

4. Select the host's corresponding driver to update from the **Driver to Update** list. Once the driver has been selected for each host, click **Update** .

   Alternatively, you can select one or more hosts from the **Selected Hosts** list and click **Select Latest** to automatically select the latest operating system-specific driver for each selected host. If you want to import a driver from another location, follow the instructions in "Driver repository" on page 460.

Driver repository

You can access the **Driver Repository** dialog box from the **Adapter Software** dialog box. Initially, the repository is empty. You must import files into the repository. Imported driver files are then displayed in the **Available Driver Files** list in the **Driver Repository** dialog box.

Importing a driver into the repository

To import drivers into the Management application, perform the following tasks.

1. From the **Adapter Software** dialog box, click the **Repository** button.

   The **Driver Repository** dialog box, shown in Figure 172, displays.

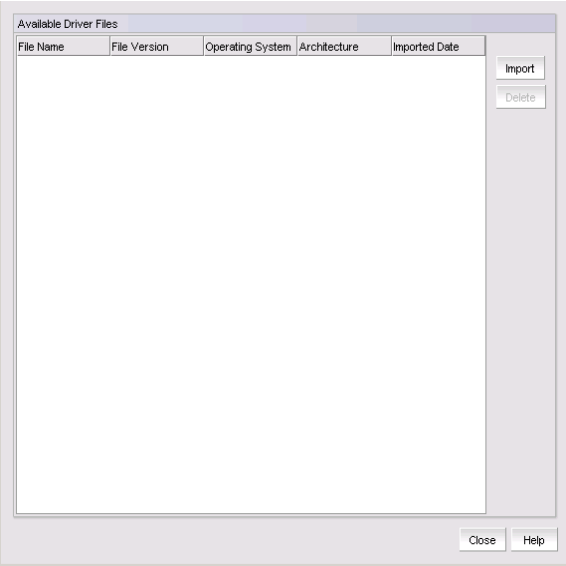


FIGURE 172 Driver Repository dialog box

2. Click **Import** on the **Driver Repository** dialog box.

   The **Import Driver Repository** dialog box displays.

3. Locate the driver file using one of the following methods:
   - Search for the file you want from the **Look In** list.
   - Enter the name of the image file you want to import in the **File Name** field.
4. Click **Open**.

   After the import completes, you see a message that the driver imported successfully.

5. Click **OK**.

Deleting a driver file from the repository

1. Select one or more driver files from the **Available Driver Files** list on the **Driver Repository** dialog box.
2. Click **Delete**.

   The driver file is removed from the **Driver Repository** dialog box.

NOTE
Windows drivers (.exe files) cannot be imported into the server repository when the Management application server is running on Linux or Solaris platforms.

Boot image repository

The boot code image stored in the adapter's flash memory contains the instructions that enable the server to locate the boot disk in SAN. The boot code image contains the basic input/output system (BIOS), extensible firmware interface (EFI), and open firmware which enable the adapters to be compatible with any system platform.

Importing a boot image into the repository

Boot images are required for adapters that are shipped without a boot image or when it is necessary to overwrite images on adapters that contain older or corrupted boot image versions.

1. From the Management application menu bar, select **Configure > Host > Adapter Software**.
2. Click the **Boot Image** tab.

   The **Boot Image Management** dialog box, shown in Figure 173, displays.

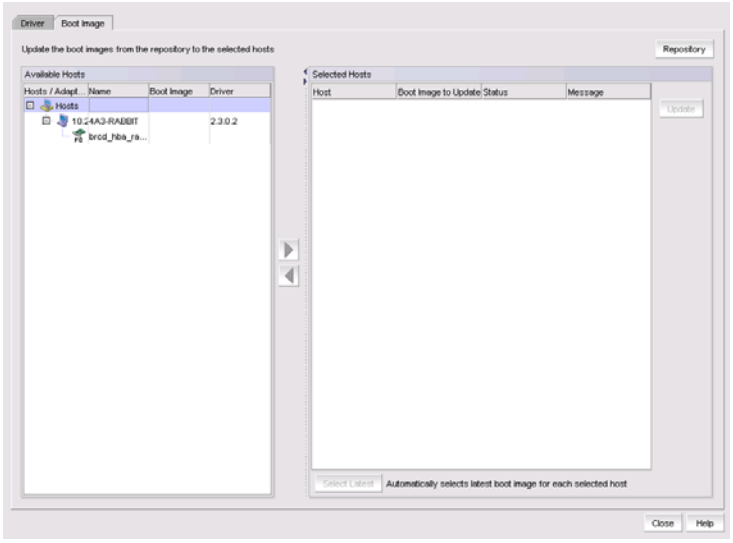


FIGURE 173 Boot Image Management dialog box

3. From the **Boot Image Management** dialog box, click the **Repository** button.

   The **Boot Image Repository** dialog box, shown in Figure 174, displays.

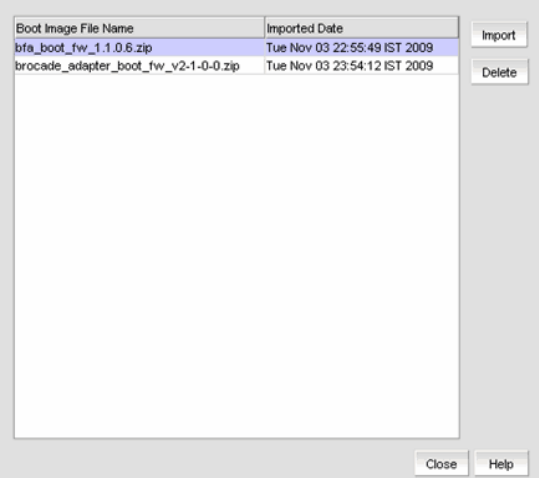


FIGURE 174 Boot Image Repository dialog box

4. Click **Import** on the **Boot Image Repository** dialog box.
5. The **Import Boot Image** dialog box displays.
6. Locate the boot image file using one of the following methods:
   - Search for the file you want from the **Look In** list. Boot image files version 2.0.0.0 and 2.1.0.0 are .zip files and other boot image files are .tar files.
   - Enter the name of the image file you want to import in the **File Name** field.
7. Click **Open**.

   After the import completes, you see a message that the boot image imported successfully.

NOTE
The boot image file is imported to *Install_Server_Home*/data/*adapter_software*/adapter_boot_images.

8. Click **OK**.

Downloading a boot image to a selected host

To download boot images to a selected host, perform the following tasks.

1. Select one or more hosts from the **Available Hosts** list on the **Boot Image Management** dialog box, and click the right arrow button to move the selected hosts to the **Selected Hosts** list.

   You can select up to 50 hosts. The first 20 hosts execute the download concurrently. If you select more than 20 hosts, they will be queued and will start when the previous download completes.

NOTE
The boot image version must be 2.0.0.0 or later.

2. Click **Select Latest** to automatically select the latest boot image for the selected hosts.

3. From the **Boot Image Management** dialog box, click the **Update** button to download a boot image to one or more selected hosts.

   One of the following download status messages displays in the **Status** column of the **Selected Hosts** list:

   - Ready
   - Queued
   - In progress
   - Failed — If the download failed, the failure reason displays in the **Message** column of the **Selected Hosts** list; for example, failed to connect to HCM agent, a checksum error occurred, or the file is invalid.
   - Finished

4. Alternatively, you can click the **Select Latest** button to automatically select the latest boot image for the selected hosts.

Deleting a boot image from the repository

1. Select one or more boot images from the **Boot Image File Name** list on the **Boot Image Repository** dialog box.
2. Click **Delete**.

   The boot image is removed from the boot image repository.

Backing up boot image files

You can back up the boot image files from the repository using the **Options** dialog box. Refer to "Backup support" on page 479 for instructions.

Bulk port configuration

Use the **Adapter Host Port Configuration** dialog box to create and assign port-level configurations to either a single or multiple adapter ports at a time. You can save up to 50 port-level configurations.

The Management application supports the following default port configurations, which you can select and assign to one port or multiple ports. You cannot edit the default configurations, but you can delete them.

- Default Port — The port property. The default value is Enabled.
- Default FDFS — The Frame Data Field Size property. The default value is 2048.
- Default QoS — The Quality of Service property. The default value is Enabled.
- Default TRL — The Target Rate Limiting property. The default value is Enabled.

Configuring host adapter ports

To create, edit, duplicate, or delete port configurations, complete the following steps.

Select **Host > Adapter Ports** from the **Configure** menu.

The **Configure Host Adapter Ports** dialog box, shown in Figure 175, displays.

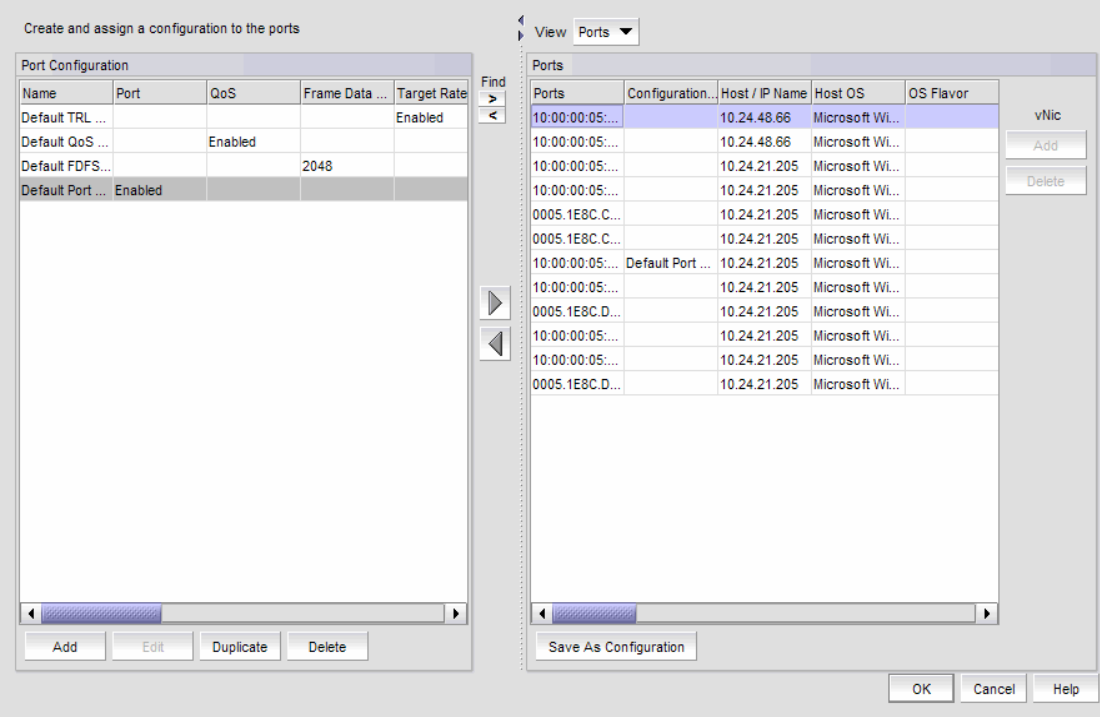


FIGURE 175 Configure Host Adapter Ports dialog box

Adding a port configuration

The **Add Port Configuration** dialog box allows you to create a maximum of 50 customized port configurations which you can then select and assign to ports.

1. Click **Add** on the **Configure Host Adapter Ports** dialog box.

   The **Add Port Configuration** dialog box, shown in Figure 176, displays.

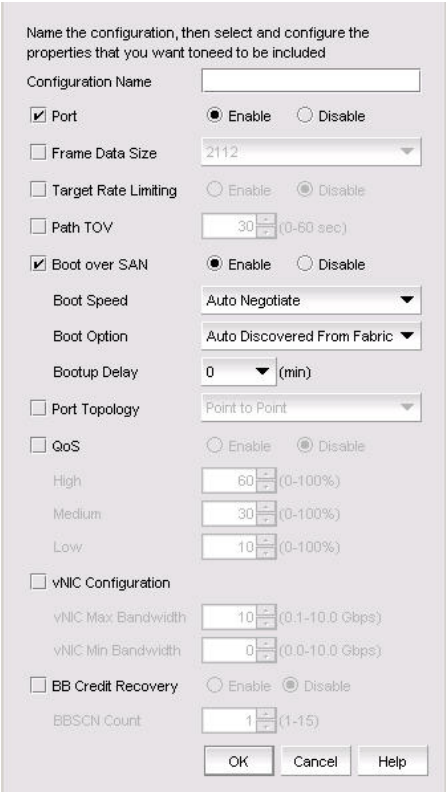


FIGURE 176 Add Port Configuration dialog box

2. Enter a name for the port configuration in the **Configuration Name** field. A maximum of 128 alphanumeric characters is supported.
3. Configure at least one of the following port properties:
   - **Port** — Enable or disable the port. Enable is the default.
   - **Frame Data Size** — Select the frame data size, in bytes, of the port. Options include Auto, 512, 1024, 2112, and 2048; the default value is 2112. Select auto to set the frame data field size automatically. Buffer credits determine the maximum amount of frame data. If the number of buffer credits is not large enough to handle the link distance and speed, performance can be severely limited.
   - **Target Rate Limiting** — Enable the Target Rate Limiting feature to minimize congestion at the adapter port. Limiting the data rate to slower targets ensures that there is no buffer-to-buffer credit back-pressure between the switch due to a slow-draining target.

     NOTE
     NOTE: Target Rate Limiting and **QoS** cannot be enabled at the same time.

   - **Path TOV** — Enter a path timeout value (TOV) to either force an immediate failover (by setting the TOV to 0) or to specify a delay in seconds (1 through 60 seconds). The default value is 30 seconds.
   - **Boot over SAN** — The Boot over SAN feature allows you to target remote boot devices (LUNs on SAN storage arrays) from which to boot the host system. Configure the following boot parameters:

Boot Speed — Set the port speed. Possible values are Auto Negotiate (to auto-negotiate the speed) and 1, 2, 4, 8, and 16 Gbps and unknown speeds.

Boot Option — From the list, select one of the following:

- **Auto Discovered From Fabric** — Enables Boot over SAN using boot LUN information stored in the fabric. This is the default setting.
- **First Visible LUN** — Enables Boot over SAN from the first discovered LUN in the SAN.

Bootup Delay — Enter a bootup delay value. Valid values are 0, 1, 2, 5, and 10 minutes and the default value is 0 minutes. The Bootup Delay feature allows you to configure the delay to device discovery, offsetting the disk spinup delay time when servers and storage devices are powered on simultaneously.

- **Port Topology** — Specify the topology type. The supported topology mode is point-to-point (p2p) or loop. You can set the toplogy to loop only if QoS and Target Rate Limiting are disabled.
- **QoS** — Enable the Quality of Service (QoS) feature to assign traffic priority (high, medium, or low) for a given source and destination traffic flow. By default, all flows are marked as medium.

NOTE
NOTE: QoS and Target Rate Limiting cannot be enabled at the same time.

QoS Percentage — The QoS priority flow value extends QoS support by allowing the user to configure custom bandwidth values for High, Medium, and Low QoS priorities. The QoS % value represents the bandwidth in percentage for each of the priorities (high, medium, and low) and the three values must equal 100 percent.

The default priority flow settings of the switch are 60 (high), 30 (medium), and 10 (low). If QoS is disabled and enabled again without providing the high, medium, and low bandwidth values, the default values are applied.

- **vNIC Configuration** — Enables you to configure a single physical CNA Ethernet port into multiple virtual Network Interface Cards (vNICs).
  - Enter the maximum allowable output bandwidth in increments of 100 Mbps in the vNIC Max Bandwidth (Mbps) box. The maximum bandwidth is 10 Gbps and this is the default.
  - Enter the minimum allowable output bandwidth in the Min Bandwidth (Mbps) box. The minimum bandwidth is 0 Mbps. A zero value of minimum bandwidth (the default) implies that no bandwidth is guaranteed for that vNIC.
- **BB Credit Recovery** — Enables you to enable or disable buffer-to-buffer (BB) credits, which are a flow control mechanism that represent the availability of resources at the receiving port. Supported state change notification (BB_SCN) values are from 1 through 15 and the default is 1.

4. Click **OK**.

   The **Adapter Port Configuration Status** dialog box displays.

5. Click **Start**.

   The adapter port configuration is applied to the ports.

6. Click **Close** after the configuration is complete (indicated by “Completed” in the **Progress** list).

Editing a port configuration

The **Edit Port Configuration** dialog box allows you to modify port configuration parameters that were configured using the **Add Port Configuration** dialog box.

1. Click **Edit** on the **Configure Host Adapter Ports** dialog box.

   The **Edit Port Configuration** dialog box displays.

2. Modify the parameters that are described in "Adding a port configuration" on page 465.

3. Click **OK** to save the changes.

Duplicating a port configuration

1. Click **Duplicate** on the **Configure Host Adapter Ports** dialog box.

   The **Duplicate Port Configuration** dialog box displays. The default name of the configuration file is **source_name** copy1.

2. Change the name of the configuration and click **OK** to save the changes.

Deleting a port configuration

1. Select a configuration from the **Port Configuration** list in the **Configure Host Adapter Ports** dialog box.

2. Click the **Delete** button.

   The port configuration is removed from the list.

Adapter port WWN virtualization

Adapter port world wide name (WWN) virtualization enables the adapter port to use a switch-assigned WWN rather than the physical port WWN for communication, allowing you to preprovision the server with the following configuration tasks:

- Create the zones with the Fabric Assigned WWN (FAWWN) before the servers and devices are connected to the switches, before they are exposed to the SAN network.
- Create LUN mapping and LUN masking without the devices present in the network.
- Preconfigure boot LUN zoning. You can configure Solaris ports or Linux ports on the switch, enabling the server to boot automatically with the predefined boot LUNs.

NOTE
Fabric Assigned WWN (FAWWN) is not supported for base switches or FICON-enabled switches.

Configuring FAWWNs on switch ports

The **Configure Fabric Assigned WWNs** dialog box, shown in Figure 177, enables you to perform the following tasks:

- Enable and disable the Fabric Assigned WWN feature status on a switch or Access Gateway port.

- Set the type value to *auto* or *user-defined*. When the **User** button is clicked, the WWN is cleared from the table and editing is enabled.
- Delete the Fabric Assigned WWN from the **Fabric Assigned WWN - Configuration** list.

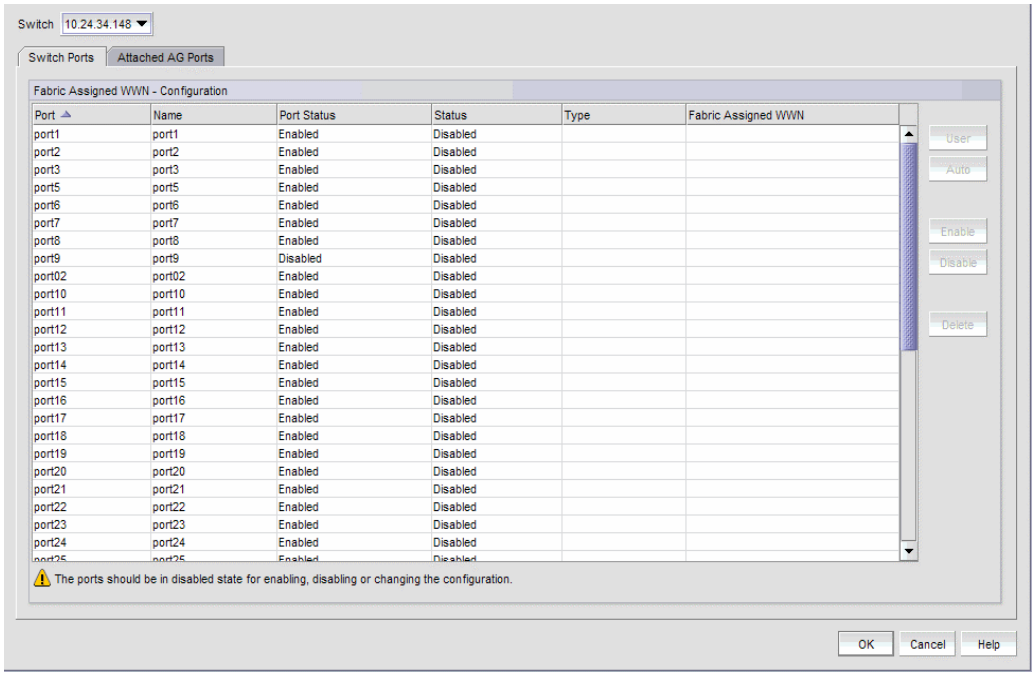


FIGURE 177 Configure Fabric Assigned WWNs dialog box

Enabling the FAWWN feature on a switch or AG ports

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select **Fabric Assigned WWN**.

   The **Configure Fabric Assigned WWNs** dialog box displays.
2. Select a switch port from the **Fabric Assigned WWN - Configuration** list.
3. Click the **Enable** button.

   The selected switch's port status is enabled.
4. Click **OK**.

   The **Fabric Assigned WWN Confirmation and Status** dialog box displays.
5. Click **Start** to save the changes to the switch.
6. Click **Close** on the **Fabric Assigned WWN Configuration and Status** dialog box.

Disabling the FAWWN feature on a switch or AG ports

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select **Fabric Assigned WWN**.

The **Configure Fabric Assigned WWNs** dialog box displays.

2. Select a switch port from the **Fabric Assigned WWN - Configuration** list.
3. Click the **Disable** button.

   The selected switch's FAWWN feature status is disabled.
4. Click **OK**.

Auto-assigning a FAWWN to a switch or AG port

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select **Fabric Assigned WWN**.

   The **Configure Fabric Assigned WWNs** dialog box displays.
2. Select a switch port or AG port from the **Fabric Assigned WWN - Configuration** list.
3. Click the **User** button.

   The system sets the type to User and the Fabric Assigned WWN parameters are now editable.
4. Enter a valid WWN on the selected switch.
5. Click **OK**.

Manually assigning a FAWWN to a switch or AG port

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select **Fabric Assigned WWN**.

   The **Configure Fabric Assigned WWNs** dialog box displays.
2. Select a switch port or AG port from the **Fabric Assigned WWN - Configuration** list.
3. Click the **Auto** button.

   If the switch port does not have an Auto FAWWN map type and the FAWWN feature is not yet enabled on the port, a To Be Generated message displays.
4. Click **OK**.

Modifying a FAWWN on a switch or AG port

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select **Fabric Assigned WWN**.

   The **Configure Fabric Assigned WWNs** dialog box displays.
2. Select a switch port or AG port from the **Fabric Assigned WWN - Configuration** list.
3. Click the **User** button.

   The Fabric Assigned WWNs parameters are now editable.

Deleting a FAWWN from a switch or AG port

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select **Fabric Assigned WWN**.

   The **Configure Fabric Assigned WWNs** dialog box displays.

2. Select a switch port or AG port from the **Fabric Assigned WWN - Configuration** list.
3. Click the **Delete** button.

   The Fabric Assigned WWN row is deleted from the **Fabric Assigned WWN - Configuration** list for the selected switch port or AG port.

FAWWNs on attached AG ports

The **Configure Fabric Assigned Assigned WWNs** dialog box, shown in Figure 178, enables you to configure the Fabric Assigned WWN feature on a selected attached Access Gateway (AG) port.

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select Fabric Assigned WWN.

   The **Configure Fabric Assigned WWNs** dialog box displays.

2. Click the **Attached AG Ports** tab.

   The **Configure Fabric Assigned WWNs** dialog box — **Attached AG Ports** tab displays.

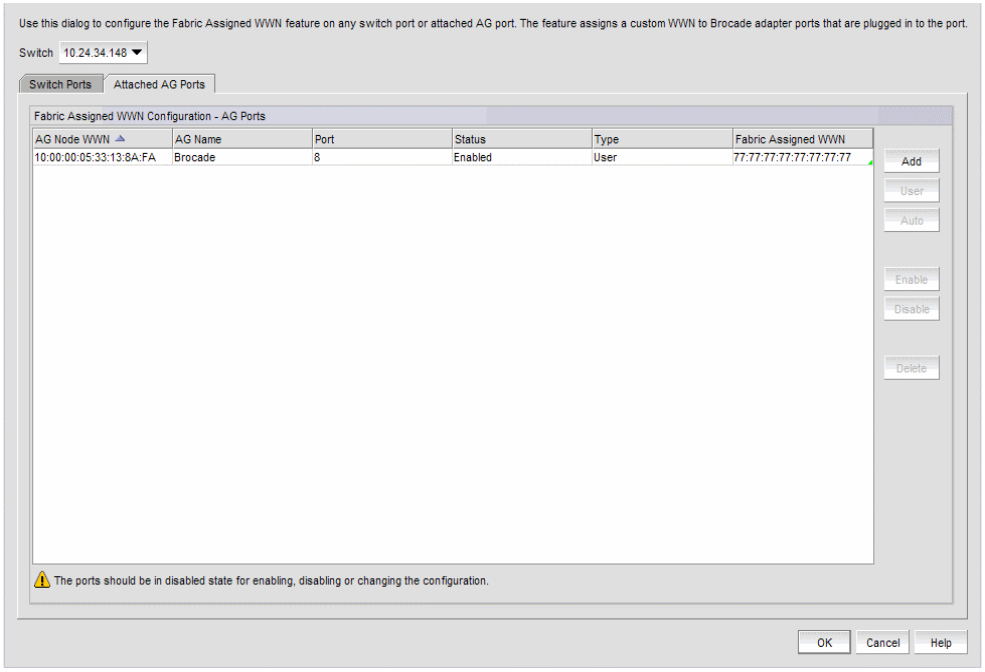


FIGURE 178 Configure Fabric Assigned WWNs dialog box--Attached AG Ports tab

Adding AG port FAWWNs

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select **Fabric Assigned WWN**.

   The **Configure Fabric Assigned WWNs** dialog box displays.
2. Click the **Attached AG Ports** tab.
3. Select a row in the **Fabric Assigned WWN Configuration - AG Ports** list.
4. Click **Add**.

   The **Add AG Fabric Assigned WWN Configuration** dialog box displays.
5. Enter a valid world wide name (WWN), with or without colons, for the Access Gateway node. Optionally, you can select an existing AG Node WWN from the list. The **AG Node WWN** box includes all discovered AG Node WWNs that are connected to the selected switch.
6. Enter a port or a port range using numbers or a hyphen (-). For example, you can enter a range as 1-6 or you can separate values with a comma; for example: 1, 2, 5, 7-10, 20.
7. Click the **Enable** button to enable the FAWWN.
8. Set the FAWWN type to one of the following map types:
   - Auto — If the switch port does not have an Auto FAWWN map type and the FAWWN feature is not yet enabled on the port, a <To Be Generated> message displays.
   - User defined — If this option is selected, you must enter a valid world wide name, with or without colons. The User defined text box cannot be empty.
9. Click **OK** to add the rows for this configuration to the **Fabric Assigned WWN Configuration - AG Ports** list.

Deleting AG port FAWWNs

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select **Fabric Assigned WWN**.

   The **Configure Fabric Assigned WWNs** dialog box displays.
2. Click the **Attached AG Ports** tab.
3. Select an online AG FAWWN row and click the **Delete** button.

   The AG FAWWN row is cleared from the **Fabric Assigned WWN Configuration - AG Ports** list.

Moving an AG port FAWWN across switches

The AG port FAWWN can be online or offline when moved across switches.

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select **Fabric Assigned WWN**.

The **Configure Fabric Assigned WWNs** dialog box displays.

2. Click the **Attached AG Ports** tab.
3. Right-click the WWN row you want to move, select the **Copy Row** option, and paste the contents into a text editor.
4. Select an online AG FAWWN row and click the **Delete** button.
5. Select a switch from the **Switch** list and click **Add** to launch the **Add AG Fabric Assigned WWN Configuration** dialog box.
6. Using the information you copied to the text editor, configure the AG port FAWWN information to be moved to the selected switch.
7. Click **OK**.

   The specified AG FAWWN row is added to the new switch.

Role-based access control

The Management application enables you to create resource groups and assign users to the selected role within that group. This enables you to assign users to a role within the resource group.

The Management application provides one preconfigured resource group (All Fabrics). When you create a resource group, all available roles are automatically assigned to the resource group. Once the resource group is available, you can assign a user to a role within the resource group.

Host adapter management privileges

You can launch the Host Connectivity Manager (HCM) if you have read and write permissions to the Host Adapter Management privilege. Other HBA-related operations are controlled by the following privileges:

- The HBA technical support launch point is controlled by the Technical Support Data Collection privilege.
- The Fibre Channel Security Protocol (FC-SP) launch point is controlled by the Security privilege. Read-write (RW) and read-only (RO) permissions are required.
- The HBA performance monitoring launch point is controlled by the Performance privilege.

Host adapter administrator privileges

The Host Adapter Administrator role has the following privileges:

- Add and delete properties
- Discovery setup
- Host management
- Performance
- Properties edit
- Security
- Servers
- View management

- Port Mapping
- Virtual Network Management

Instructions for managing resource groups and users using roles and privileges are detailed in "User accounts,""Roles," and "Areas of responsibility," in Chapter 6, "User Account Management".

Host performance management

Real-time performance enables you to collect data from managed HBA and CNA ports. You can use real-time performance to configure the following options:

- Select the polling rate from 20 seconds up to 1 minute.
- Select up to 32 ports total from a maximum of 10 devices for graphing performance.
- Choose to display the same Y-axis range for both the Tx MBps and Rx MBps measure types for easier comparison of graphs.

NOTE
In the **Port Picker** dialog box, the Brocade 1860 Fabric Adapter in AnyIO mode displays in both categories (HBA port measures and CNA port measures). The ports are properly filtered to display only the CNA or HBA port based on the selection.

Table 52 lists the counters that are supported for the FC ports and for the HBA and CNA ports.

TABLE 52 Counters

FC port measures	HBA port measures	CNA port measures
Tx % utilization	Tx % utilization	Tx % utilization
Rx % utilization	Rx % utilization	Rx % utilization
Tx MBps	Tx MBps	Tx MBps
Rx MBps	Rx MBps	Rx MBps
CRC errors	CRC errors	
Signal losses	Signal losses	
Sync losses	Sync losses	
Link failures	Link failures	
Sequence errors	Primitive sequence protocol errors	
Invalid transmissions		
Rx link resets		
Tx link resets		
	NOS count	
	Error frames	
	Dropped frames	
	Undersized frames	
	Oversized frames	
	Bad EOF frames	

TABLE 52 Counters (Continued)

FC port measures	HBA port measures	CNA port measures
	Invalid ordered sets	
	Non-frame coding error	
		Received paused frames
		Transmitted paused frames
		Received FCoE pause frames
		Transmitted FCoE pause frames
		Received FCS error frames
		Transmitted FCS error frames
		Received alignment error frames
		Received length error frames
		Received code error frames

Instructions for generating real-time performance data are detailed in "Generating a real-time performance graph" on page 976.

Host security authentication

Fibre Channel Security Protocol (FC-SP) is a mechanism used to secure communication between two switches or between a switch and a device such as an HBA port.

You can use either the Management application or the HCM GUI to display the authentication settings and status. When you enable FC-SP authentication using the Management application, you can also set the authentication settings on the attached 8 Gbps 8-FC port.

NOTE
FC-SP is only available for Brocade HBAs that are managed using the HCM agent and CIM Server. FC-SP is not available for virtual ports or unmanaged HBA ports. The user must have the Security privilege to use this feature. FC-SP is not supported for hosts connected to Access Gateway mode-enabled devices.

Configuring security authentication using the Management application

Access the **Fibre Channel Security Protocol Configuration** dialog box by selecting an adapter port from the device tree. Select the appropriate device based on how you want to configure security authentication.

1. Select **Configure > Element Manager > HCM**.

   The Host Connectivity Manager (HCM) launches.

2. From HCM, select **Configure > Authentication**.

   The **Fibre Channel Security Protocol Configuration** dialog box, shown in Figure 179, displays.

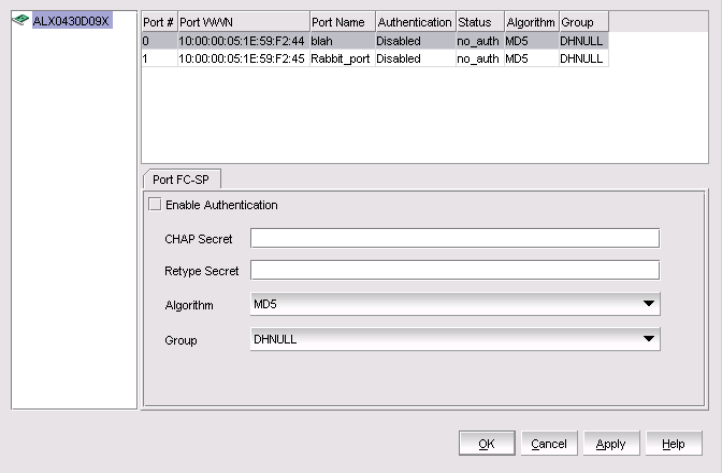


FIGURE 179 Fibre Channel Security Protocol Configuration dialog box

3. Configure the following parameters on the **Fibre Channel Security Protocol Configuration** dialog box:

   a. Select the **Enable Authentication** check box to enable the authentication policy.

      If authentication is enabled, the port attempts to negotiate with the switch. If the switch does not participate in the authentication process, the port skips the authentication process.

   b. In the **Algorithm** list, select one of the following options:

      - **MD5** - A hashing algorithm that verifies a message's integrity using Message Digest version 5. MD5 produces a 128-bit digest and is the required authentication mechanism for LDAP v3 servers.
      - **SHA1** - A secure hashing algorithm that computes a 160-bit message digest for a data file that is provided as input.
      - **MD5SHA1** - Similar to the MD5 hashing algorithm, but used for DH-CHAP authentication.
      - **SHA1MD5** - Similar to the SHA1 hashing algorithm, but used for DH-CHAP authentication.

   c. Enter a secret in the **CHAP Secret** field. Enter the secret again in the **Retype Secret** field.

      The length of the secret must be from 8 through 41 characters in length. The **Secret** field cannot be blank.

   d. From the **Group** list, select **DHNULL** as the DH-group type value.

4. Click **OK** to save the changes and close the dialog box.

   FC-SP settings are also applied to the attached switch.

supportSave on adapters

Host management features support capturing support information for managed Brocade adapters, which are discovered in the Management application. You can trigger supportSave for multiple adapters at the same time.

supportSave cannot be used to collect support information for ESXi hosts managed by a CIM Server. Refer to the *Brocade Adapters Administrator's Guide* for information about supportSave on ESXi hosts.

NOTE
You cannot schedule host supportSave information.

Instructions for scheduling and capturing technical support files are detailed in Chapter 39, "Technical Support".

Host fault management

Fault management enables you to monitor your SAN using the following methods:

- Monitors logs for specified conditions and sends a notification or runs a script when the specified condition is met.
- Creates event-based policies, which contain an event trigger and action.
- Configures e-mail event notifications.
- Receives and forwards Syslog messages from Fabric OS switches and Brocade HBAs, managed using the Host Connectivity Manager (HCM).
- Through the Brocade Adapters ESXi Management feature, ESXi systems support the HCM and the Management application when the CIM provider is installed on these systems.

NOTE
The host name of the ESXi host being discovered through CIM discovery in the Management application should be configured such that it resolves to the same IP address used for discovering that ESXi host in the Management application.

Adapter events

You can configure triggers and actions for the following event types:

- Product Audit Event — Occurs when a target product is audited.
- Product Status Event — Occurs when a device or connection changes to up or down.
- Product Threshold Alert Event — Notifies you when a threshold alert has been reached.

Filtering event notifications

The Management application provides notification of many different types of SAN events. If a user wants to receive notification of certain events, you can filter the events specifically for that user.

NOTE
The e-mail filter in the Management application is overridden by the firmware e-mail filter. When the firmware determines that certain events do not receive e-mail notification, an e-mail notification is not sent for those events even when the event type is added to the **Selected Events** table in the **Define Filter** dialog box. Refer to for more information.

To configure an e-mail event, use the instructions in .

Syslog forwarding

NOTE
Syslog messages are only available on Fabric OS devices and HBAs (managed using the HCM Agent). CIM events are only logged in the master log and the forwarding of CIM events is not supported.

Syslog forwarding is the process by which you can configure the Management application to send Syslog messages to other computers. Switches only send the Syslog information through port 514; therefore, if port 514 is being used by another application, you must configure the Management application to listen on a different port. Then you must configure another Syslog server to listen for Syslog messages and forward the messages to the Syslog listening port of the Management application. Brocade HBAs only send the Syslog information through port 514; therefore, if port 514 is being used by another application, the Management application cannot send Syslog messages to another computer.

Syslog messages are persisted in the database. You can view the Syslog messages from the Management application. However, the Management application does not convert the Syslog messages into event objects except for the audit Syslog messages.

For more information about Syslog forwarding, refer to "Syslog forwarding" on page 1163.

Backup support

The Management application helps you to protect your data by backing it up automatically. The data can then be restored, as necessary.

Configuring backup to a hard drive

NOTE
Configuring backup to a hard drive requires a hard drive. The drive should not be the same physical drive on which your operating system or the Management application is installed.

To configure the backup function to a hard drive, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Server Backup** in the **Category** list.

   The currently defined directory displays in the **Output Directory** field.

3. Select the **Enable Backup** check box, if necessary.

4. Choose one or more of the following options:

   - Select the **Include Adapter Boot Image** check box to back up boot image files from the boot image repository.
   - Select the **Include FTP Root directory** check box.

     If you select the FTP Root directory, the FTP Root sub-directories, Technical Support, and Trace Dump are selected automatically and you cannot clear the sub-directory selections. If you do not select the FTP Root directory, the sub-directories can be selected individually.

5. Enter the time (using a 24-hour clock) you want the backup process to begin in the **Next Backup Start Time Hours** and **Minutes** fields.

6. Select an interval from the **Backup Interval** list to set how often backup occurs.

7. Browse to the hard drive and directory to which you want to back up your data.

8. Click **Apply** or **OK**.

   The application verifies that the backup device exists and that the server can write to it.

   If the device does not exist or is not writable, an error message displays that states you have entered an invalid device. Click **OK** to go back to the **Options** dialog box and fix the error.

   Backup occurs, if needed, at the interval you specified.

Enabling backup

Backup is enabled by default. However, if it has been disabled, complete the following steps to enable the function.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Server Backup** in the **Category** list.
3. Select the **Enable Backup** check box.
4. Click **Apply** or **OK**.

Disabling backup

Backup is enabled by default. If you want to stop the backup process, you must disable backup. To disable the backup function, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Server Backup** in the **Category** list.
3. Clear the **Enable Backup** check box.
4. Click **Apply** or **OK**.

Chapter

16

Fibre Channel over Ethernet

In this chapter

FCoE overview

Fibre Channel over Ethernet (FCoE) leverages Ethernet enhancements, called Data Center Bridging (DCB), to transport encapsulated Fibre Channel frames over Ethernet. Ethernet is the physical layer over which the encapsulated Fibre Channel frames are transported.

One of the barriers to using Ethernet as the basis for a converged network has been the limited bandwidth that Ethernet has historically provided. However, with 10 Gbps Ethernet, the available bandwidth offers the potential to consolidate all the traffic types over the same link.

Unlike Fibre Channel, Ethernet is not a peer-to-peer protocol. The mechanism used to discover new ports, MAC address assignments, and Fibre Channel logins and logouts is called the FCoE Initialization Protocol (FIP).

DCBX protocol

Data Center Bridging Exchange (DCBX) protocol allows enhanced Ethernet devices to convey and configure their DCB capabilities and ensures a consistent configuration across the network. DCBX protocol is used between DCB devices, such as a converged network adapter (CNA) and an FCoE switch, to exchange configuration with directly connected peers.

NOTE
When DCBX protocol is used, any other Link Layer Discovery Protocol (LLDP) implementation must be disabled on the host systems.

Enhanced Ethernet features

Data Center Bridging (DCB) is a set of IEEE 802 standard Ethernet enhancements that enable Fibre Channel convergence with Ethernet. The two basic requirements in a lossless Ethernet environment are Enhanced Transmission Selection (ETS) and priority-based flow control. These capabilities allow the Fibre Channel frames to run directly over 10 Gbps Ethernet segments without adversely affecting performance.

Enhanced Transmission Selection

Enhanced Transmission Selection (ETS) allows lower priority traffic classes to use available bandwidth that is not being used by higher priority traffic classes and maximizes the use of available bandwidth.

ETS allows configuration of bandwidth per priority group.

Priority group ID (PG ID) usage is defined as follows:

- PG ID 0, 7 are used when the priority group is limited for its bandwidth use.
- PG ID 8, 14 are reserved.
- PG ID 15.0 through 15.7 are used for priorities that are not limited for their bandwidth use.

The configured priority group percentage refers to the maximum percentage of available link bandwidth after PG ID 15.0 to 15.7 is serviced, assuming all priority groups are fully subscribed. If one of the priority groups does not consume its allocated bandwidth, then any unused portion is available for use by other priority groups.

Priority-based flow control

Priority-based flow control (PFC) allows the network to selectively pause different classes of traffic and create lossless lanes for Fibre Channel, while retaining packet drop congestion management for IP traffic. A high-level pause example follows:

- During periods of heavy congestion, the receive buffers reach high threshold and generate a pause.
- The pause tells transmission (Tx) queues to stop transmitting.
- After the receive (Rx) buffers reach low threshold, a zero pause is generated.
- The zero pause signals the Tx queues to resume transmitting.

Ethernet jumbo frames

The basic assumption underlying FCoE is that TCP/IP is not required in a local data center network and the necessary functions can be provided with Enhanced Ethernet. The purpose of an "enhanced" Ethernet is to provide reliable, lossless transport for the encapsulated Fibre Channel traffic. Enhanced Ethernet provides support for jumbo Ethernet frames and in-order frame delivery.

The Fabric OS FCoE 10 Gbps converged network adapter supports jumbo packets of up to 9 KB, compared to the original 1,518-byte maximum transmission unit (MTU) for Ethernet. The frame size increase allows the same amount of data to be transferred with less effort.

FCoE protocols supported

The Fabric OS FCoE converged network adapter supports two layers of protocols: Ethernet link layer and FCoE layer.

Ethernet link layer protocols supported

The following protocols support the Ethernet link layer:

- 802.1q (VLAN)
- 802.1Qaz (Enhanced Transmission Selection)
- 802.1Qbb (priority-based flow control)
- 802.3ad (link aggregation)
- 802.3ae (10 Gb Ethernet)
- 802.1p (priority encoding)
- IEEE 1149.1 (JTAG) for manufacturing debug and diagnostics
- IPv4 specification (RFC 793/768)
- IPv6 specification (RFC 2460)
- TCP/UDP specification (RFC 793/768)
- ARP specification (RFC 826)
- RSS with support for IPV4TCP, IPV4, IPV6TCP, IPV6 hash types
- HDS (Header-data split)

FCoE protocols

The following protocols support Fibre Channel over Ethernet:

- FIP (FC-BB5-compliant):
  - Support for FIP Discovery protocol for dynamic FCF discovery and FCoE link management
  - Support for FPMA and SPMA type FIP fabric login
- Support for Initiator mode only (FCP-3-compliant in Initiator mode)
- SCSI protection information support
- IP-over-FC
- NPIV support

FCoE licensing

The FCoE license enables Fibre Channel over Ethernet (FCoE) functionality on the following supported DCB switches:

- Network OS 10 GbE 24-port 8 GbE 8 FC port switch
- Network OS VDX 6710, 6720, and 6730 switches
- Network OS VDX 6740 and 6740T switches
- Network OS VDX 8770-series switches
- Network OS VDX 2730 10 GbE connection blade for the Fujitsu PRIMERGY BX900 and BX400 Blade Servers

Without the FCoE license, the DCB switches are pure Layer 2 Ethernet switches and do not allow FCoE bridging capabilities.

NOTE
The VCS license includes the FCoE Base license. With the VCS license, the virtual FCoE ports are displayed for Network OS switches in VCS mode.

Saving running configurations

The **Save Running to Startup** dialog box lists discovered DCB switches with Fabric OS version 6.3x firmware or later. You can select available switches and move them to the **Selected Switches** list. Upon startup, the DCB switch configuration is copied to the selected switches.

NOTE
The **Save Running to Startup** dialog box launches if there is at least one DCB switch discovered. If no DCB switches exist, a warning message displays.

Copying switch configurations to selected switches

1. To access the **Save Running to Startup** dialog box, select **Configure > Configuration > Save Running to Startup**.

   The **Save Running to Startup** dialog box displays, as shown in Figure 180.

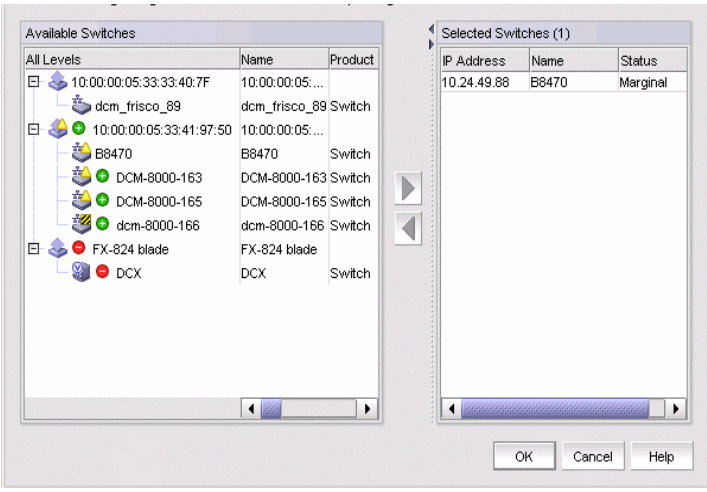


FIGURE 180 Save Running to Startup dialog box

2. Highlight a discovered DCB switch from the **Available Switches** list, and click the right arrow button to move the switch to the **Selected Switches** list.
3. Highlight the selected switch and click **OK** to start the configuration.

   The running configuration is saved to the selected switch, effective on the next system startup. If you restore the DCB switch using the **Restore Switch Configuration** dialog box, you are prompted to select one of two restoration methods:

   - As the running configuration and reboot

     ATTENTION
     Rebooting a switch connected to a fabric will stop all traffic to and from the switch. All ports on the switch will become inactive until the switch comes back online.

   - As the startup configuration (no reboot)

   For instructions on how to restore a saved switch configuration, refer to the section "Restoring a switch configuration for a selected device" in the "Device Configuration" chapter.

DCB configuration management

Depending on the platform, the DCB switch has one of the configurations shown in Table 53.

TABLE 53 DCB configurations

Device type	Configuration possibilities
IBM blade server	• 14 internal 10-Gbps ports for IBM BladeCenter H (BCH) chassis type • 12 internal 10-Gbps ports IBM BladeCenter HT (BCHT) chassis type • 8 external 10-Gbps DCB ports • 8 8-Gbps FC ports
Dell embedded switch module	• 16 10-Gbps internal ports • 8 10-Gbps external ports • 4 8-Gbps FC ports
Fabric OS DCB switch	• 8 16-Gbps FC ports • 24 10-Gbps Ethernet ports
Fabric OS FCOE10-24 blade	24 10-Gbps Ethernet ports
Network OS VDX switches	• Network OS VDX 2730 10 Gbps connection blade • Network OS VDX 6710 switch • Network OS VDX 6720-24 switch • Network OS VDX 6720-60 switch • Network OS VDX 6730-32 switch • Network OS VDX 6730-76 switch • Network OS VDX 6740 switch • Network OS VDX 6740T switch • Network OS VDX 8770-4 switch • Network OS VDX 8770-8 switch

You must configure DCB interfaces and ports differently than you configure Fibre Channel ports to effectively use the converged network features.

For example, priority-based flow control (PFC) and Enhanced Transmission Selection (ETS) are the two QoS policy enhancements you must configure to create a lossless Ethernet. You then use DCBX protocol on DCB-enabled devices to exchange configuration information.

The DCB ports of FOS DCB devices are categorized into two types:

- External ports - The eight external ports are the same as the original 10 Gbps Ethernet DCB ports. The default name in the device tree is ExT <slot>/<port>.
- Internal ports - The default name for the 12 or 14 internal ports is InT <slot>/<port>. 802.1x, LAG configuration, and Spanning Tree Protocol (STP) are not supported on internal ports.

Switch policies

You can configure and enable a number of DCB policies on a switch, port, or link aggregation group (LAG).

The following switch policy configurations apply to all ports in a LAG:

- DCB map and Traffic Class map
- Link Layer Discovery Protocol (LLDP)

The switch policies are described in the following sections.

DCB map and Traffic Class map

With DCB, Fibre Channel uses a buffer management system based on buffer-to-buffer credits, with corresponding confirmation by the R-RDY frame. The flow control standard used for DCB is based on “pause” frames. Coupled with an appropriate input buffer, lossless transport of frames is possible.

Priority-based flow control (PFC) deals with the prioritization of frames. This standard IEEE 802.1Q allows application-specific bandwidth reservations in DCB. When you create a DCB map, you specify the precedence (priority) and then you map the priority groups with the Class of Service (CoS) and apply bandwidth percentages.

Refer to “QoS configuration” on page 501 for instructions on how to create DCB maps and Traffic Class maps.

LLDP profiles

Data Center Bridging Exchange (DCBX) protocol enables Enhanced Ethernet devices to discover whether a peer device supports particular features, such as Priority-based Flow Control (PFC) or Class of Service (CoS). In a Data Center Bridging (DCB) environment, LLDP is enhanced with DCBX protocol to further share or change the configured DCB enhancements.

Refer to “LLDP-DCBX configuration” on page 514 for instructions on how to configure LLDP for FCoE.

802.1x policy

802.1x is a standard authentication protocol that defines a client-server-based access control and authentication protocol. 802.1x restricts unknown or unauthorized clients from connecting to a LAN through publicly accessible ports.

Refer to “802.1x authentication” on page 517 for information on setting 802.1x parameters.

DCB configuration

To launch the **DCB Configuration** dialog box, select **Configure > DCB** from the menu bar.

The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

NOTE
For FOS DCB devices, the **Protocol Down Reason** column, shown in Figure 181, displays the values only for the external ports of embedded platforms but not for the internal ports.

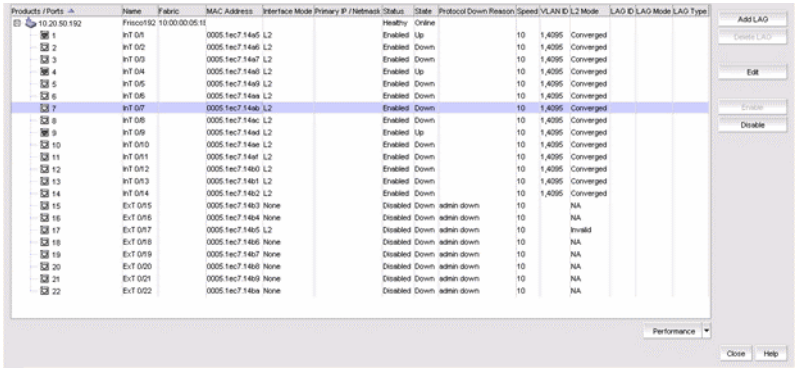


FIGURE 181 DCB Configuration dialog box

Minimum DCB configuration for FCoE traffic

You must complete the following procedures to create the basic configuration of DCB for FCoE traffic.

NOTE
This section is applicable for Fabric OS versions 6.3.0, 6.3.1, 6.3.2, 6.4.1, and 6.4.2. This section is not applicable for Fabric OS versions 6.3.1_dcb, 6.3.1_cee, 6.4.1_fcoe, and 7.0.x.

In release 12.1 of the Management application, you cannot perform DCB configuration on Network OS VDX switches. You can only view Network OS switch configuration in the Management application DCB dialog. Refer to "Network OS switches in VCS mode" on page 524 for more information.

NOTE
Editable operations from the Management application on Network OS products are not supported for this release. You must use the command line interface to configure or modify parameter on Network OS products. For more information, refer to the *Network OS Command Reference*.

Beginning with Network OS 4.0, VCS mode encompasses two mode types:

- Fabric cluster mode—The data path for nodes is distributed, but the configuration path is not distributed. Each node keeps its configuration database independently.
- Logical chassis cluster mode—Both the data and configuration paths are distributed. The entire cluster can be configured from the principal node. Logical chassis mode requires Network OS 4.0 or later.

For more information about fabric cluster mode and logical chassis cluster mode, refer to the *Network OS Administrator's Guide* and the *Network OS Command Reference*, versions 4.0 or later.

The term *VCS mode* refers to *both* fabric cluster mode and logical chassis cluster mode unless otherwise indicated.

NOTE
In the Management application, a logical chassis cluster is shown without all its members; a fabric cluster is shown with all its members.

Creating a DCB map to carry the LAN and SAN traffic

To create a DCB map to carry the LAN and SAN traffic, complete the following steps.

NOTE
This procedure is applicable for Fabric OS versions earlier than Fabric OS 7.0. For Fabric OS versions 7.0 and later, you can only edit the default DCB map.

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays.

2. Select the switch to edit from the **Products/Ports** list and click **Edit**.

   The **Edit Switch** dialog box displays.

3. Click the **QoS** tab.

   The **Edit Switch** dialog box - **QoS** tab displays, as shown in Figure 182.

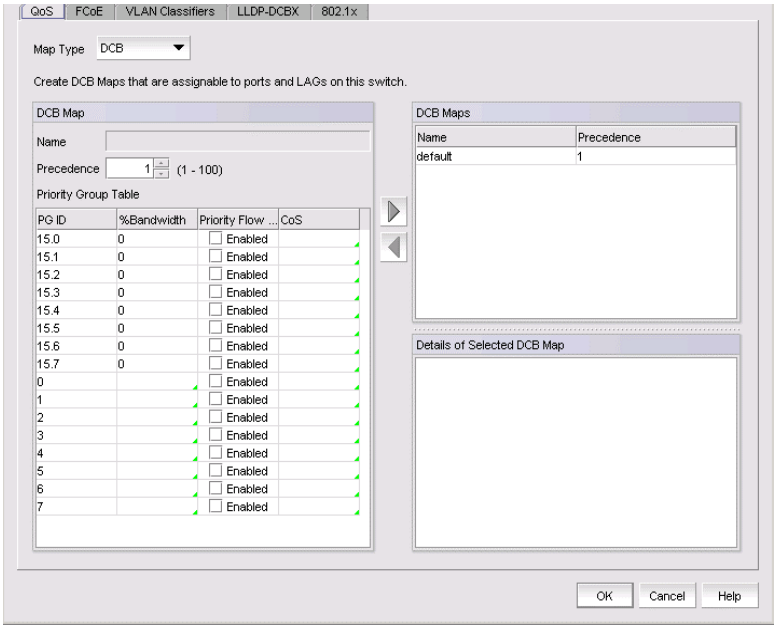


FIGURE 182 Edit Switch dialog box - QoS tab

4. Select **DCB** from the **Map Type** list.
5. Configure the following DCB Map parameters in the **DCB Map** area:

- **Name** - Enter a name to identify the DCB map.
- **Precedence** - Enter a value from 1 through 100. This number determines the map's priority.
- **Priority Flow Control** check box - Check to enable priority-based flow control on individual priority groups.
- **CoS** - Click the CoS cell to launch the **Edit CoS** dialog box, where you can select and assign one or more priorities (PG ID 15.0 through 15.7).

  All of the eight CoS values (0-7) must be used in a DCB map. Duplicate CoS values in two or more priority groups are not allowed.

  NOTE
  You can only edit CoS fields that are displayed with a green tick mark.

  % Bandwidth (optional) - While in the **Edit CoS** dialog box, enter a bandwidth value for PG IDs 15.0 through 15.7. You must map each CoS to at least one of the PG IDs.

  Note the following points:

  - You cannot define a bandwidth percentage for strict priorities (PG ID 15.0-15.7). The total bandwidth percentage for PG ID 15.0 through 15.7 must equal 0.
  - If you set a CoS value to one or more of the PG IDs 0-7, you must also enter a non-zero bandwidth percentage. The total bandwidth percentage must equal 100.
  - For PG IDs 0-7 that do not have an assigned CoS value or PFC enabled, the bandwidth percentage must be 0.

6. Click the right arrow button to add the map to the **DCB Maps** list.

   If a DCB map exists with the same name, a validation dialog box launches and you are asked if you want to overwrite the map.

7. Click **OK**.
8. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.

Configuring LLDP

To configure LLDP, complete the following steps.

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays.

2. Select the switch to edit from the **Product/Ports** list and click **Edit**.

   The **Edit Switch** dialog box displays.

3. Click the **LLDP-DCBX** tab.

   The **Edit Switch** dialog box - **LLDP-DCBX** tab displays, as shown in Figure 183.

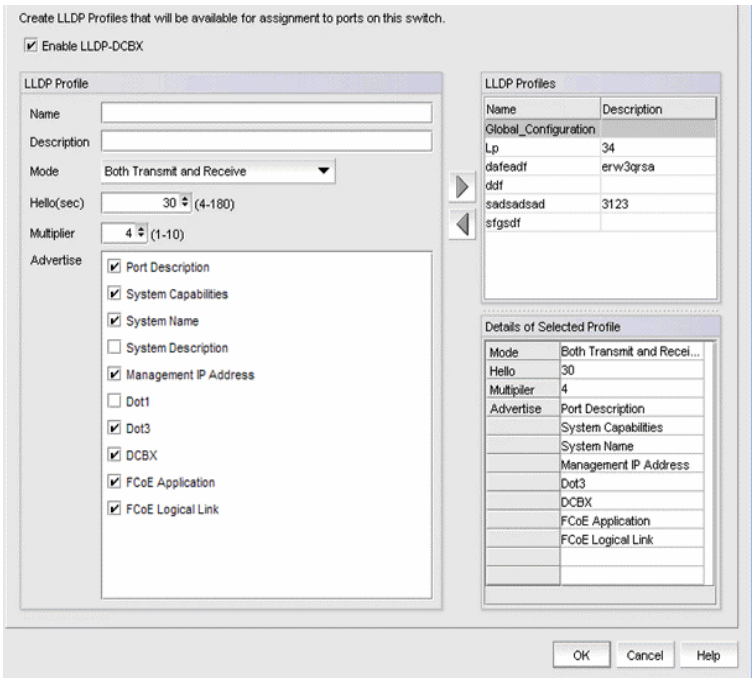


FIGURE 183 Edit Switch dialog box - LLDP-DCBX tab

4. Select the **Global Configuration** LLDP profile in the **LLDP Profiles** list.
5. Click the left arrow button to edit.
6. Select the **FCoE Application** and **FCoE Logical Link** check boxes in the **Advertise** list to advertise them on the network.
7. Click **OK** after changing the attributes of the current deployment.

   The **Deployment Status** dialog box displays.
8. Click **Start** on the **Deployment Status** dialog box to save the changes to the switch.
9. Click **Close** to close the **Deployment Status** dialog box.

Configuring the DCB interface with the DCB map and global LLDP profile

To configure the DCB interface, complete the following steps.

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays.
2. Select the Te port connected to the CNA from the **Product/Ports** list and click **Edit**..

   The **Edit Port** dialog box displays, as shown in Figure 186.
3. Select the **Port** tab, if necessary, and select the **Enable** check box.
4. Select **L2** from the **Interface Mode** list.
5. Select **Converged** (for a Brocade CNA) or **Access** (for a QLogic CNA) from the **L2 Mode** list.
6. Click the **QoS** tab and select the **Assign a map** check box.
7. Select **DCB** from the **Map Type** list.

8. Select the DCB map you created in "Creating a DCB map to carry the LAN and SAN traffic" on page 489 from the **Available DCB Maps** list.
9. Click the **LLDP-DCBX** tab and select the **Enable LLDP-DCBX on Te** *Port Number* check box.
10. Select **Assign the Global Configuration**.
11. Click **OK**.

    The **Deploy to Ports** dialog box displays.
12. Click **OK** after changing the attributes of the current deployment.

    The **Deployment Status** dialog box displays.
13. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected ports.
14. Click **Close** to close the **Deployment Status** dialog box.

Creating the FCoE VLAN to carry FCoE traffic

NOTE
You can complete this procedure using the Management application on embedded platforms such as the Fabric OS converged 10 GbE switch module for the IBM BladeCenter or the Dell M8428-k switch. You must use Web Tools to complete this procedure for the Fabric OS Fabric OS switch or the FCOE10-24 port blade.

To create the FCoE VLAN, complete the following steps. This procedure is applicable for Fabric OS versions earlier than Fabric OS 7.0.

1. Select the Fabric OS FCoE switch in the device tree.
2. Select **Configure > Element Manager > Admin**.

   The Web Tools application displays. You can also launch Web Tools by clicking the **Element Manager** button on the **DCB Configuration** dialog box.
3. Click the **DCB** tab.
4. Click the **VLAN** tab.
5. Click **Add**.

   The **VLAN Configuration** dialog box displays.
6. Enter the VLAN identifier in the **VLAN ID** field.
7. Click **OK** on the **VLAN Configuration** dialog box.
8. Select the VLAN you created and click **Edit** to convert the VLAN to FCoE VLAN.
9. Select the **FCoE** check box.
10. Select the DCB interface to carry the FCoE traffic from the **Selection List** and click **Add** to add it to the **Selected List**.
11. Click **OK** on the **VLAN Configuration** dialog box to save your changes.
12. Close the Web Tools application.

Creating and activating VLAN classifiers on the DCB interface

NOTE
You can complete this procedure using the Management application for Fabric OS versions 7.0 and later. For Fabric OS versions earlier than Fabric OS 7.0, you must use the CLI.

To create and activate the VLAN classifiers on the DCB interface, complete the following steps.

1. Log in to the switch and enter global configuration mode.

```
switch:<userid>>cmsh
switch#configure terminal
```

2. Create and apply VLAN classifiers to the DCB interface to classify Ethernet frames on an untagged interface to VLAN.

```
switch(config)#vlan classifier rule 1 proto fip encap ethv2
switch(config)#vlan classifier rule 2 proto fcoe encap ethv2
switch(config)#vlan classifier group 1 add rule 1
switch(config)#vlan classifier group 1 add rule 2
```

3. Apply the VLAN classifier group to the DCB interface.

```
switch(conf-if-te-0/7)#vlan classifier activate group 1 vlan 1002
```

4. Save the running-config file to the startup-config file.

```
switch#copy running-config startup-config
```

Adding a LAG

Link aggregation, based on the IEEE 802.3ad protocol, is a mechanism to bundle several physical ports together to form a single logical channel or trunk. The collection of ports is called a link aggregation group (LAG).

NOTE
An internal port cannot be part of a LAG. You can create LAGs with external ports only.

- The **Add LAG** button on the **DCB Configuration** dialog box is enabled when a single DCB switch or ports of a single DCB switch are selected.
- The **Add LAG** button is disabled when multiple switches are selected, ports from different switches are selected, or LAGs are selected.
- The **Edit LAG** button is enabled when a single LAG, port, or switch is selected.

Creating a LAG is not supported for Network OS products. You must use the command line interface to configure a LAG for Network OS products. Refer to the *Network OS Command Reference* for more information.

NOTE
When LLDP-DCBX is disabled on the switch, a yellow banner displays on the **DCB Configuration** dialog box, indicating that LLDP-DCBX is not only disabled on the switch, but is also disabled for all ports and LAGs on the switch.

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select the DCB switch or one or more DCB ports from the **Products/Ports** list to add to a link aggregation group (LAG).
3. Click **Add LAG** or **Edit LAG**.

   The **Add LAG** or **Edit LAG** dialog box displays, as shown in Figure 184.

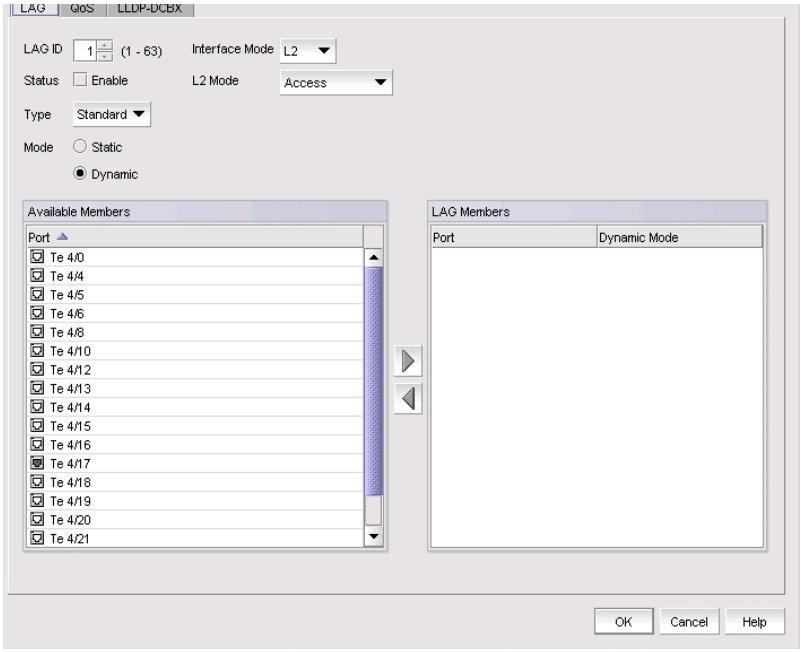


FIGURE 184 Add LAG dialog box

4. Configure the following LAG parameters:

NOTE
Ports with 802.1x authentication or ports that are enabled in L2 mode or L3 mode are not supported in a LAG.

- **LAG ID** - Enter the LAG identifier, using a value from 1 through 63. Duplicate LAG IDs are not allowed.
- **Status** - Click the **Enable** check box to enable the LAG. You must enable the LAG to use the DCB functionality.
- **Interface Mode** - Select **None** or **L2**. Ports that are in L2 mode cannot be added to a LAG. The L3 interface mode option is displayed in the **Edit LAG** dialog box only.
- **L2 Mode** - Select **Access** or **Trunk**:
  - Access mode allows only one VLAN and allows only untagged frames.
  - Trunk mode allows more than one VLAN association and allows tagged frames.
- **IP/Netmask** - The netmask is used to divide an IP address into subnets. It specifies which portion of the IP address represents the network and which portion represents the host, and can only be configured if the interface mode is L3.
  - **Primary** - The primary IP address assigned to a 10 Gbps DCB/FC switch module.
  - **Secondary** - The secondary IP address is optional. Secondary IP addresses are helpful when the interface port is part of multiple subnets.

5. Select at least one available DCB port from the **Available Members** list and click the right arrow button to move it to the **LAG Members** list.

   The DCB ports are now part of the link aggregation group.

6. Continue to configure the following LAG parameters. These parameters are always enabled.

   - **Type** - Sets the limit on the size of the LAG. The type values include Standard, where the LAG is limited to 16 ports, and Brocade LAG, where the LAG is limited to 4 ports. The default is Standard.

     For Network OS devices, you can add a maximum of 8 ports to the LAG.

     NOTE
     You cannot create Fabric OS-type LAGs from different anvil chips. If you do, an error message displays. Only the first port is considered as part of the LAG.

   - **Mode** - Sets all ports added to the LAG members list in either Static or Dynamic mode. The default is Dynamic, Active, but LAG members can be Active or Passive if the LAG member is Dynamic.

7. When you have finished configuring the policies, click **OK**.

   The **Deploy to LAGs** dialog box displays.

8. Click **OK** after changing the attributes of the current deployment.

   The **Deployment Status** dialog box launches.

9. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected LAG or LAGs.

10. Click **Close** to close the **Deployment Status** dialog box.

Editing a DCB switch

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select the DCB switch from the **Products/Ports** list.

3. Click **Edit**.

   The **Edit Switch** dialog box displays (Figure 185).

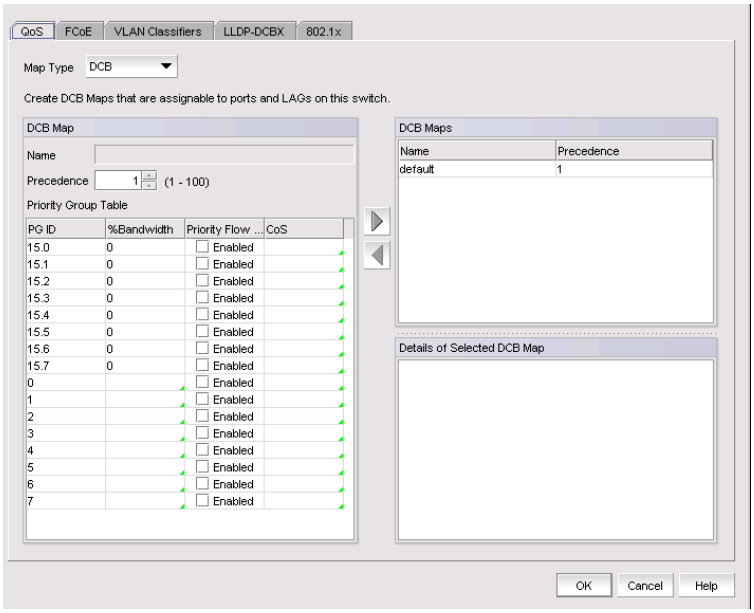


FIGURE 185 **Edit Switch dialog box**

4. Configure the policies for the **Edit Switch** dialog box tabs, which are described in the following sections:
   - "QoS configuration" on page 501
   - "FCoE provisioning" on page 508
   - "VLAN classifier configuration" on page 510
   - "LLDP-DCBX configuration" on page 514
   - "802.1x authentication" on page 517
5. When you have finished configuring the policies, apply the settings to the switch.

NOTE
Clicking **Cancel** when there are pending changes launches a pop-up dialog box.

6. Click **OK**.

   The **Deploy to Products** dialog box displays.
7. Click **OK** after changing the attributes of the current deployment.

   The **Deployment Status** dialog box launches.
8. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected devices.
9. Click **Close** to close the **Deployment Status** dialog box.

Editing a DCB port

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a DCB port from the **Products/Ports** list.
3. Click **Edit**.

   The **Edit Port** dialog box displays, as shown in Figure 186.

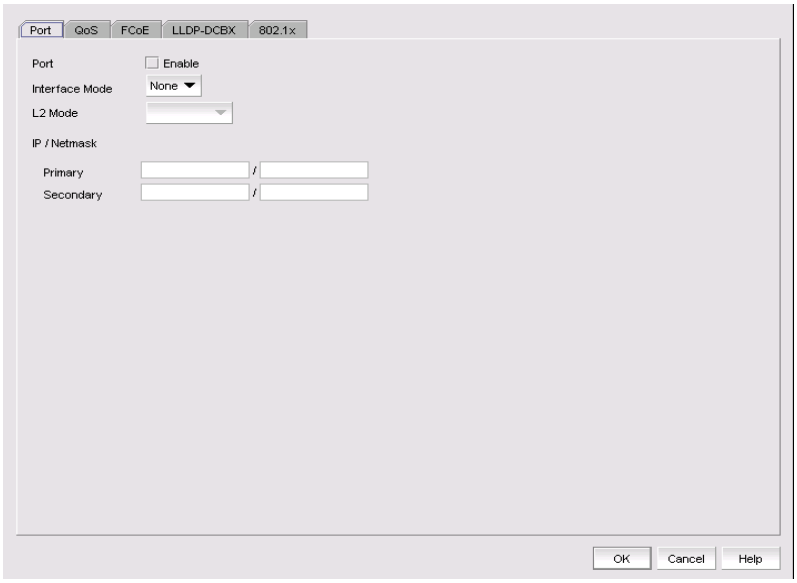


FIGURE 186 Edit Port dialog box

4. Modify the following DCB port parameters as required:

   - **Interface Mode** - Select **None** or **L2**. For external ports, the L3 interface mode displays in addition to **None** or **L2**. If you select **L3** as the interface mode, the **IP/Netmask** field is enabled and you can then assign the primary and secondary IP addresses.
     - L2 mode is enabled if you select L2 as the interface mode. If a DCB port is enabled on the 10 Gbps DCB/FC switch module, the L2 mode is disabled.
     - L3 mode appears only for the external ports of embedded platforms.

     NOTE
     You can change the interface mode from **L2** to **None** only if the port is assigned to the default VLAN 1.

   - **IP/Netmask** - The netmask is used to divide an IP address into subnets. It specifies which portion of the IP address represents the network and which portion represents the host, and can only be configured if the interface mode is L3.
     - **Primary** - The primary IP address assigned to a 10 Gbps DCB/FC switch module.
     - **Secondary** - The secondary IP address is optional. Secondary IP addresses are helpful when the interface port is part of multiple subnets.

5. When you have finished configuring the policies, apply the settings to the DCB port.

NOTE
Clicking **Cancel** when there are pending changes launches a pop-up dialog box.

6. Click **OK** when you have finished modifying the DCB port parameters.

   The **Deploy to Ports** dialog box displays.

7. Click **OK** after changing the attributes of the current deployment.

   The **Deployment Status** dialog box launches.

8. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected port or ports.

9. Click **Close** to close the **Deployment Status** dialog box.

Editing a LAG

Use the following procedure to change members and policies in a link aggregation group (LAG).

NOTE
Editing a LAG is not supported for Network OS products. You must use the command line interface to configure a LAG for Network OS products. Refer to the *Network OS Command Reference* for more information.

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select the link aggregation group (LAG) from the **Products/Ports** list.

3. Click **Edit**.

   The **Edit LAG** dialog box displays, as shown in Figure 187.

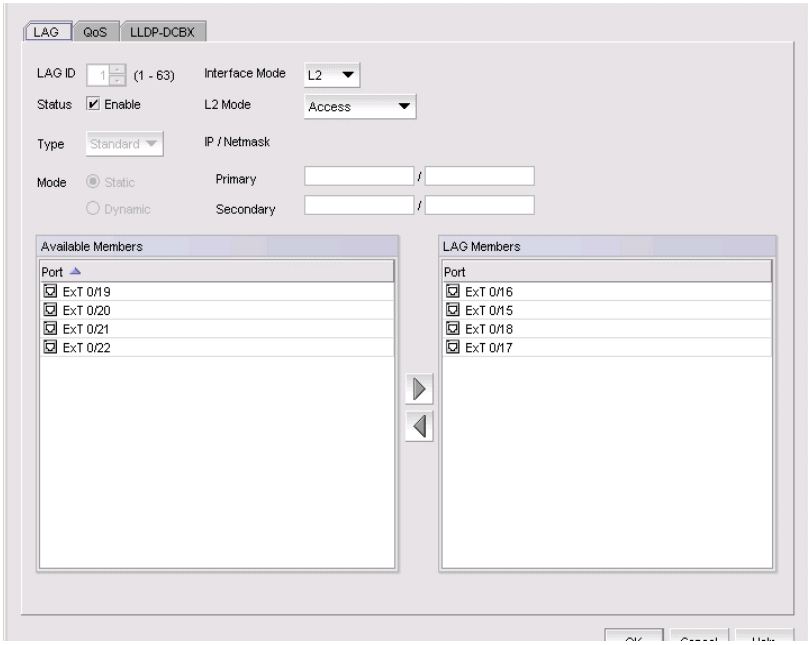


FIGURE 187 Edit LAG dialog box

4. Configure the following LAG parameters, as required:

NOTE
Ports with 802.1x authentication or ports that are enabled in L2 mode or L3 mode are not supported in a LAG.

- **LAG ID** - The LAG identifier, which is not an editable field.
- **Status** - Click the **Enable** check box to enable the LAG. You must enable the LAG to use the DCB functionality.
- **Interface Mode** - Select **None** or **L2**. For external ports, the L3 interface mode displays, in addition to **None** or **L2**. If you select **L3** as the interface mode, the **IP/Netmask** field is enabled and you can then assign the primary and secondary IP addresses.
  - A port must be in non-L2 mode if you are adding the port as a member of a LAG.
  - You cannot change the interface mode from **L2** to **None** if the LAG is assigned to a VLAN.
- **L2 Mode** - Select **Access** or **Trunk.**
  - Access mode allows only one VLAN and allows only untagged frames.
  - Trunk mode allows more than one VLAN association and allows tagged frames.
- **IP/Netmask** - The netmask is used to divide an IP address into subnets. It specifies which portion of the IP address represents the network and which portion represents the host, and can only be configured if the interface mode is L3. Primary and secondary IP address fields are applicable only to the external ports and the interface mode must be L3 to enable these fields.
  - **Primary** - Enter the primary IP address assigned to an L3 port.
  - **Secondary** - Enter the secondary IP address (optional). Multiple (secondary) IP addresses help when the interface and port are part of multiple subnets.

5. Continue to configure the following LAG parameters. These parameters are disabled until you add a DCB port to the **LAG Members** list.
   - **Mode -** The ports that are LAG members are in either Static or Dynamic mode. You cannot change the mode on existing members of a LAG.

     If the mode is set as **Dynamic**, you can change the dynamic mode type (to Active or Passive) only for newly-added ports, not for existing port members of a LAG.
   - **Type** - The type value options are **Standard**, where the LAG is limited to 16 ports, and **Brocade**, where the LAG is limited to four ports. The default is **Standard**. The type is set when you add a LAG; you cannot edit the type using the **Edit LAG** dialog box.
6. Click **OK**.

   The **Deploy to LAGs** dialog box displays.
7. Click **OK** after changing the attributes of the current deployment.

   The **Deployment Status** dialog box displays.
8. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected LAG or LAGs.

   NOTE
   If the primary or secondary IP address already exists on another interface, an error message displays in the **Status** area.
9. Click **Close** to close the **Deployment Status** dialog box.

Enabling a DCB port or LAG

If you select multiple switches or multiple ports and LAGs from two or more switches, both the **Enable** button and the **Disable** button are disabled.

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.
2. Select one or more DCB ports or LAGs (which can span multiple switches) that you want to enable.

   NOTE
   All selected LAGs must be in the same state (enabled or disabled); otherwise, both the **Enable** and **Disable** buttons are disabled.
3. Click **Enable**.

   The **Confirmation and Status** dialog box launches with the selected ports or LAGs.

4. Click **Start** on the **Confirmation and Status** dialog box to save the changes to the selected ports or LAGs.

   The selected DCB ports or LAGs are enabled in the **DCB Configuration** dialog box.

5. Click **Close** to close the **Confirmation and Status** dialog box.

Deleting a LAG

You can only delete a link aggregation group (LAG) that is selected from a single switch. If you select multiple switches or multiple ports from two or more switches, the **Delete** button is disabled.

NOTE
Deleting a LAG is not supported for Network OS products. You must use the command line interface to delete a LAG for Network OS products. Refer to the *Network OS Command Reference* for more information.

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select one or more LAGs (that can span multiple switches) that you want to delete from the **Products/Ports** list.

3. Click **Delete**.

   The **Confirmation and Status** dialog box launches with the selected LAGs.

4. Click **Start** on the **Confirmation and Status** dialog box to save the changes to the DCB switches.

   The selected LAGs are deleted in the **DCB Configuration** dialog box.

5. Click **Close** to close the **Confirmation and Status** dialog box.

QoS configuration

QoS configuration involves configuring packet classification, mapping the priority and traffic class, controlling congestion, and scheduling. The configuration of these QoS entities consists of DCB Map and Traffic Class Map configuration.

In a Data Center Bridging (DCB) configuration, Enhanced Transmission Selection (ETS) and priority-based flow control (PFC) are configured by utilizing a priority table, a priority group table, and a priority traffic table. The Traffic Class map is the mapping of user priority to traffic class.

Priority-based flow control

Priority-based flow control (PFC) is an enhancement to the existing pause mechanism in Ethernet. PFC creates eight separate virtual links on the physical link and allows any of these links to be paused and restarted independently, enabling the network to create a no-drop Class of Service (CoS) for an individual virtual link.

Table 54 shows examples of how priority grouping might be allocated in a 15-priority group scenario.

TABLE 54 Priority grouping allocated in a 15-priority group example

Priority group ID	Bandwidth (%)	Priority flow control
0	55	on
1	25	on
2	0	off
3	0	off
4	5	off
5	0	off
6	15	on
7	0	off
15.0-15.7	Strict priority No bandwidth % configuration allowed	on

Creating a DCB map

The procedure in this section applies only for Fabric OS versions earlier than Fabric OS 7.0.

When you create a DCB map, each of the Class of Service (CoS) options (0-7) must be mapped to at least one of the Priority Group IDs (0-7) and the total bandwidth percentage must equal 100. All QoS, DCB map, and Traffic Class map configurations apply to all ports in a LAG.

There can be, at the most, 16 entries in the Priority Group table. Eight of the entries are Strict Priority entries with a Priority Group ID (15.0-15.7) and eight are user-definable entries with a Priority Group ID of 0-7. Refer to Table 54 for an example of priority group configuration.

NOTE
The 10 Gbps DCB/FC switch module can have only one DCB map.

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch, and click **Edit**.

3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays, as shown in Figure 188.

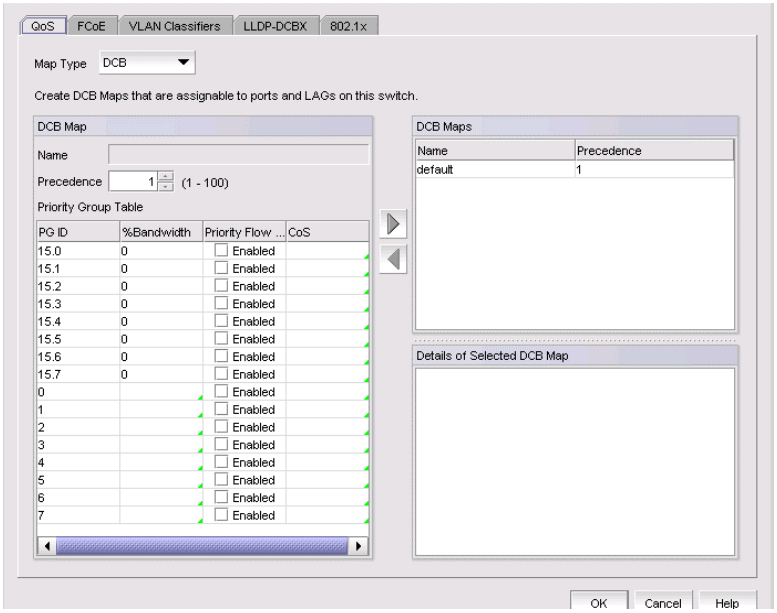


FIGURE 188 QoS, Create DCB Map dialog box

4. Select **DCB** from the **Map Type** list.
5. Configure the following DCB map parameters in the **DCB Map** area:
   - **Name** - Enter a name to identify the DCB map.

     NOTE
     Only one DCB map (the default) is supported on Fabric OS version 6.3.1_dcb and version 7.0.0 and later.

   - **Precedence** - Enter a value from 1 through 100. This number determines the map's priority.
   - **Priority Flow Control** check box - Check to enable priority-based flow control on individual priority groups.
   - **CoS** - Click the CoS cell to launch the **Edit CoS** dialog box, where you can select and assign one or more priorities (PG ID 15.0 through 15.7).

     All of the eight CoS values (0-7) must be used in a DCB map, separated with a comma and a space. Duplicate CoS values in two or more priority groups are not allowed.

     NOTE
     You can only edit CoS fields that are displayed with a green tick mark.

     % Bandwidth *(optional)* - While in the **Edit CoS** dialog box, enter a bandwidth value for priority group (PG) IDs 15.0 through 15.7. You must map each CoS to at least one of the PG IDs.

     Note the following points:

     - You cannot define a bandwidth percentage for strict priorities (PG ID 15.0-15.7). The total bandwidth percentage for PG ID 15.0 through 15.7 must equal 0.

- If you set a CoS value to one or more of the PG IDs 0-7, you must also enter a non-zero bandwidth percentage. The total bandwidth percentage must equal 100.
- For PG IDs 0-7 that do not have an assigned CoS value or PFC enabled, the bandwidth percentage must be 0.

6. Click the right arrow button to add the map to the **DCB Maps** list.

   If a DCB map exists with the same name, a validation dialog box launches and you are asked if you want to overwrite the map.

7. Click **OK**.
8. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.

Editing a DCB map

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.

4. Select a DCB map from the **DCB Maps** list and click the left arrow button to load its values in the left pane. The fields are now editable.
5. Keep the same DCB map name and modify the following values, as required. Refer to Table 54 for an example of priority group configuration.
   - **Name** - Enter a name to identify the DCB map.
   - **Precedence** - Enter a value from 1 through 100. This number determines the map's priority.
   - **% Bandwidth** - Enter a bandwidth value for priority group IDs 0-7. The total of all priority groups must equal 100 percent.
   - **Priority Flow Control** check box - Check to enable priority flow control on individual priority groups.
   - **CoS** - Click the CoS cell to launch the **Edit CoS** dialog box, where you can select and assign one or more priorities (PG ID 15.0 through 15.7).
6. Click the right arrow button to re-add the map to the **DCB Maps** list.

   If the DCB map already exists, an overwrite message displays.

7. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.

Deleting a DCB map

You cannot delete the DCB map of a 10 Gbps DCB/FC switch module. To delete the DCB map of an 8 Gbps DCB switch, complete the following steps.

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.

4. Select one or more DCB maps.
5. Click the left arrow button.

   The selected DCB map row is removed from the list.

6. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.

   NOTE
   With Fabric OS version 7.0 and later, there is only one DCB map (default), that you cannot delete.

7. Click **OK** after changing the attributes of the current deployment.

   The **Deployment Status** dialog box displays.

8. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected devices.
9. Click **Close** to close the **Deployment Status** dialog box.

Assigning a DCB map to a port or link aggregation group

The **Edit Port** dialog box - **QoS** tab allows you to assign DCB maps to ports and LAGs on a selected switch.

NOTE
QoS maps are created using the **Edit Switch** dialog box, accessible from the **DCB Configuration** dialog box.

A port can have either a DCB map or a Traffic Class map assigned to it, but it cannot have both.

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a port or LAG, and click **Edit**.
3. Click the **QoS** tab on the **Edit Port** or **Edit LAG** dialog box.

   The **QoS** dialog box displays.

4. Click the **Assign a map to** <*device_name*> check box to assign the selected port to a DCB map.

   If you do not select this check box, all QoS edit features are disabled.

5. Select **DCB Map** in the **Map Type** list.
6. Select a DCB map in the **Available DCB Maps** list.

If no DCB maps were created on the switch, the **Available DCB Maps** list is empty. Otherwise, the following DCB map details display:

- **PG - ID** — Lists the priority group ID (15.0 through 15.7 and 0 through 7).
- **% Bandwidth** — Lists the bandwidth value for priority group IDs 0-7. The total of all priority groups must equal 100 percent.
- **Priority Flow** checkbox — Check to enable priority-based flow control on individual priority groups.
- **CoS** — Lists the Class of Service (CoS) value that corresponds to the priority group ID rows. The CoS value must be mapped to at least one of the priority group IDs (0-7).

7. When you have finished the configuration, click **OK** to launch the **Deploy to Ports/LAGs** dialog box.

Creating a Traffic Class map

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.

4. Select **Traffic Class** from the **Map Type** list.
5. Name the Traffic Class map.
6. Click the Traffic Class cell in a CoS row and directly enter a value from 0-7. You can leave the cell empty to indicate zero (0).
7. Click the right arrow button to add the map to the **Traffic Class Maps** list.

   If the name of the Traffic Class map already exists, an overwrite warning message displays. Click **Yes** to overwrite the existing Traffic Class map.

8. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.

Editing a Traffic Class map

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.

4. Select a Traffic Class map from the **Traffic Class Maps** list and click the left arrow button to load its values in the left pane. The fields are now editable.

If the name of the Traffic Class map already exists, an overwrite warning message displays. Click **Yes** to overwrite the existing Traffic Class map.

5. Keep the same Traffic Class map name and modify the values, as required.
6. Click the right arrow button to re-add the map to the **Traffic Class Maps** list.
7. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.

Deleting a Traffic Class map

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.
2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.
4. Select a Traffic Class map that you want to delete from the **Traffic Class Maps** list.
5. Click the left arrow button.

   The selected Traffic Class map row is removed from the list.
6. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.
7. Click **OK** after changing the attributes of the current deployment.

   The **Deployment Status** dialog box displays.
8. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected devices.

Assigning a Traffic Class map to a port or link aggregation group

You can assign a Traffic Class map to a port or ports under the LAG; however, a port does not require a Traffic Class map be assigned to it. A port can have either a DCB map or a Traffic Class map assigned to it, but it cannot have both.

NOTE
You cannot configure QoS or LLDP-DCBX on a LAG.

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.
2. Select a port or LAG, and click **Edit**.
3. Click the **QoS** tab on the **Edit Port** or **Edit LAG** dialog box.

   The **QoS** dialog box displays.
4. Click the **Assign a map** check box.

5. Select **Traffic Class** in the **Map Type** list.
6. Select a Traffic Class map in the **Traffic Class Map** list.
7. When you have finished the configuration, click **OK** to launch the **Deploy to Ports/LAGs** dialog box. Refer to "Switch, port, and LAG deployment" on page 520 for more information.

FCoE provisioning

The Management application supports FCoE provisioning only on Fabric OS version 6.3.1_dcb.

The command line interface (CLI) supports FCoE provisioning for the following versions of Fabric OS:

- Fabric OS 6.3.1_cee
- Fabric OS 6.3.1_del
- Fabric OS 6.4.1_fcoe
- Fabric OS 7.0.x

Refer to the *Fabric OS Command Reference* for CLI procedures.

FCoE provisioning simplifies the number of steps required to configure a DCB port to carry the FCoE traffic. The FCoE map contains the default DCB map and the VLAN ID. You can change the default VLAN ID using the **FCoE** tab of the **Edit Switch** dialog box, shown in Figure 185.

NOTE
For FOS DCB switches, the default DCB map associated with the default FCoE map can be edited on the switch from the **Edit Switch** dialog box - **QoS** tab.

Changing the VLAN ID on the default FCoE map

You can change the VLAN ID on the default FCoE map only when no ports or LAGs are participating as members of the switch. You must first manually remove the FCoE map option for each of the port members before you change the VLAN ID on the switch.

NOTE
You can complete this procedure using the Management application on embedded platforms such as the Fabric OS converged 10 GbE switch module for the IBM BladeCenter or the Dell M8428-k switch. You cannot perform this task on the Fabric OS Fabric OS switch or the FCOE10-24 port blade.

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch and click **Edit**.
3. Click the **FCoE** tab on the **Edit Switch** dialog box.

   The **Edit Switch** dialog box, **FCoE** tab displays the following FCoE map parameters:

   NOTE
   The **FCoE** tab does not display for the Fabric OS Fabric OS switch or the FCOE10-24 port blade.

- **Name** — The name of the FCoE map that will be available for assignment to ports on this switch. This is a read-only field.
- **VLAN ID** — Enter an FCoE VLAN identifier to associate with the FCoE map. The values range from 2 through 3583, and 1002 is the default.
- **DCB Map** — The DCB map that is associated with the FCoE map. This is a read-only field.

4. Accept the default VLAN ID of 1002, or change the value. The valid VLAN ID range is from 2 through 3583.
5. Click the right arrow button to move the FCoE map parameters into the **FCoE Maps** list.
6. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.
7. Click **OK** after changing the attributes of the current deployment.

   The **Deployment Status** dialog box displays.
8. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected devices.

Enabling or disabling the FCoE map on the port

You must first manually disable an FCoE map-enabled port if you want to edit the VLAN ID of the FCoE map. Refer to "Changing the VLAN ID on the default FCoE map" on page 508 for information on editing the VLAN ID using the **Edit Switch** dialog box, **FCoE** tab.

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.
2. Select a port and click **Edit**.
3. Click the **FCoE** tab on the **Edit Port** dialog box.

   The **Edit Port** dialog box, **FCoE** tab displays the following parameters:

   - **FCoE Map** field — Displays the name of the FCoE map (read-only).
   - **VLAN ID** list — The FCoE VLAN identifier associated with the FCoE map. The values range from 2 through 3583, and 1002 is the default.
   - **DCB Map** — Displays the name of the DCB map (read-only).
   - Details of selected DCB Map list:
     - **PG - ID** — Lists the priority group ID (15.0 through 15.7 and 0 through 7)
     - **% Bandwidth** — Lists the bandwidth value for priority group IDs 0-7. The total of all priority groups must equal 100 percent.
     - **Priority Flow** check box — Check to enable priority-based flow control on individual priority groups.
     - **CoS** — Lists the Class of Service (CoS) value that corresponds to the priority group ID rows. The CoS value must be mapped to at least one of the priority group IDs (0-7).
4. If enabled, click the **Enable FCoE** check box to disable the port's membership on the FCoE map.

5. When you have finished the configuration, click **OK** to launch the **Deploy to Ports** dialog box.
6. Click **OK** after changing the attributes of the current deployment.

   The **Deployment Status** dialog box displays.
7. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected devices.

VLAN classifier configuration

The Management application supports VLAN classifier management only on Fabric OS 6.3.1_dcb and Fabric OS 7.0.0.

VLAN classifier rules are used to define specific rules for classifying untagged packets to selected VLANs based on protocol and MAC addresses. The classified frames are then tagged with a VLAN ID.

VLAN classifier rules can be categorized into the following areas:

- 802.1Q protocol-based classifier rules
- MAC address-based classifier rules

VLAN classifiers are created on a per-switch basis.

NOTE
The **VLAN Classifiers** tab on the **Edit Switch** dialog box displays only on switches with Fabric OS versions 7.0.0 and later.

Adding a VLAN classifier rule

The **Edit Switch** dialog box, **VLAN Classifiers** tab allows you to create rules and group them into VLAN classifiers, which can then be applied to access port and LAG VLAN members and converged port VLAN members.

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.
2. Select a switch and click **Edit**.
3. Click the **VLAN Classifiers** tab on the **Edit Switch** dialog box.

   The **Edit Switch** dialog box, **VLAN Classifiers** tab displays, as shown in Figure 189. The **Available Rules** list contains the following information:

   - **Rule ID** — The rule identifier. Valid rule ID values are from 1 through 256.
   - **Rule Type** — Valid rule types are **MAC** (MAC address-based rule) and Proto (802.1Q protocol-based rule).
   - **Encapsulation** — The encapsulation type (Ethv2, nosnaplic, or snaplic). The **Encapsulation** column only displays a value when Proto is the rule type.

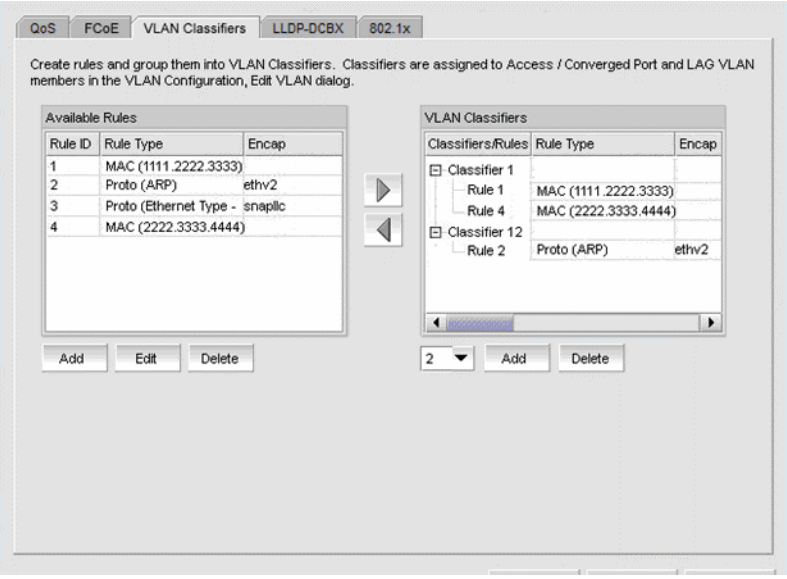


FIGURE 189 Edit Switch dialog box, VLAN Classifiers tab

4. Click the **Add** button under the **Available Rules** list.

   The **Add Rules** dialog box displays, as shown in Figure 190.

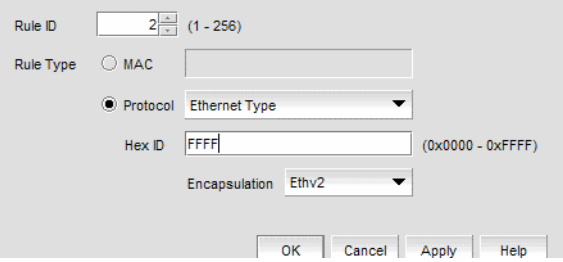


FIGURE 190 Add Rules dialog box

   The **Rule ID** field is pre-populated with the next available rule ID number.

5. Keep the rule ID number as it is, or change the number using a value from 1 through 256.
6. Select a rule type. Valid rule types are **MAC** (MAC address-based rule) and Proto (802.1Q protocol-based rule).
7. If **Ethernet Type** is selected as the protocol rule type, enter any valid four-digit hexadecimal value within the allowed range of 0x0000 through 0xFFFF. For the other Proto options, the hex ID value is hard-coded as follows:
   - ARP — 0x0808
   - IP — 0x8881
   - IPv6 — 0x86DD
8. Select an encapsulation type from the list. Options include Ethv2, nosnapllc, and snapllc. The **Encapsulation** list only accepts a value when **Protocol** is selected as the rule type.

9. Click **OK** to add the rule to the **Available Rules** list on the **VLAN Classifiers** tab of the **Edit Switch** dialog box and close the **Add Rules** dialog box.

NOTE
Clicking **Apply** also adds the rule to the **Available Rules** list on the **VLAN Classifiers** tab of the **Edit Switch** dialog box, and in addition, the **Add Rules** dialog box remains open and clears all entries for you to define the next rule.

10. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.

Editing a VLAN classifier rule

1. From the **VLAN Classifiers** tab of the **Edit Switch** dialog box, select a row in the **Available Rules** list and click **Edit**.

   The **Edit Rules** dialog box displays with the fields pre-populated with the rule details. The **Rule ID** field is disabled.

2. Select a rule type. Valid rule types are **MAC** (MAC address-based rule) and Proto (802.1q protocol-based rule).
3. If Ethernet is selected as the protocol-based rule type, enter any valid four-digit hexadecimal value within the allowed range of 0x0000 through 0xFFFF. For the other Proto options, the hex ID value is hard-coded as follows:
   - ARP — 0x0808
   - IP — 0x8881
   - IPv6 — 0x86DD
4. Select an encapsulation type from the list. Options include Ethv2, nosnapllc, and snapllc. The **Encapsulation** list only accepts a value when Protocol is selected as the rule type.
5. Click **OK** to add the edited rule to the **Available Rules** list on the **VLAN Classifiers** tab of the **Edit Switch** dialog box and close the **Edit Rules** dialog box.
6. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.

Deleting a VLAN classifier rule

1. From the **VLAN Classifiers** tab of the **Edit Switch** dialog box, select a row in the **Available Rules** list and click **Delete**.

   A message displays if the rules are participating in VLAN classifier groups that are currently associated with VLAN port or LAG members.

2. Click **Yes** to remove the selected rule row from the list.
3. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.

Creating a VLAN classifier group

You can assign existing rules to a selected VLAN classifier and form a VLAN classifier group. If no rules are available, you can add rules to a selected switch using the **Add Rules** dialog box.

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch and click **Edit**.
3. Click the **VLAN Classifiers** tab on the **Edit Switch** dialog box.

   The **Edit Switch** dialog box, **VLAN Classifiers** tab displays.

4. Select a classifier ID from the **VLAN Classifier** list. Values range from 1 through 16.
5. Click the **Add** button under the **VLAN Classifie**r list.

   The classifier with the selected ID is displayed in the **VLAN Classifier** list.

6. Select the classifier from the **VLAN Classifier** list and then select the rules you want to add under this classifier from the **VLAN Classifier Rules** list.
   - If no rules are available, the following error message displays: “No rules are available on this switch. Choose **Add** under the **Available Rules** list to add rules to this switch.”
   - If no classifier group IDs are available, the list is disabled.
7. Click the right arrow button.

   The selected rules are assigned to the selected VLAN classifier ID in the **VLAN Classifier** list.

8. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.

Deleting a VLAN classifier group

1. Click the **VLAN Classifiers** tab on the **Edit Switch** dialog box.

   The **Edit Switch** dialog box, **VLAN Classifiers** tab displays.

2. Select a classifier from the **VLAN Classifiers** list.
3. Click **Delete**.

   The VLAN classifier group is deleted.

4. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.

LLDP-DCBX configuration

Link Layer Discovery Protocol (LLDP) provides a solution for the configuration issues caused by increasing numbers and types of network devices in a LAN environment, because, with LLDP, you can statically monitor and configure each device on a network.

Data Center Bridging Exchange (DCBX) protocol enables Enhanced Ethernet devices to discover whether a peer device supports particular features, such as Priority-based Flow Control (PFC) or Class of Service (CoS). In a Data Center Bridging (DCB) environment, LLDP is enhanced with DCBX protocol to further share or change the configured DCB enhancements. You must enable the DCBX protocol and configure certain parameters in order to effectively utilize the benefits of a converged network.

Using the **LLDP-DCBX** dialog box, you can create and manage LLDP profiles and assign an LLDP profile to a port or link aggregation group (LAG).

Configuring LLDP for FCoE

To configure LLDP for FCoE, complete the following steps.

NOTE
When a TE port is selected to assign to an LLDP profile, a yellow banner displays with the following error message: "LLDP-DCBX is disabled on this switch. The configuration becomes functional when LLDP-DCBX is enabled on the switch."

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays.

2. Select the switch to edit in the **DCB Ports and LAGs** list and click **Edit**.

   The **Edit Switch** dialog box displays, as shown in Figure 191.

3. Click the **LLDP-DCBX** tab.

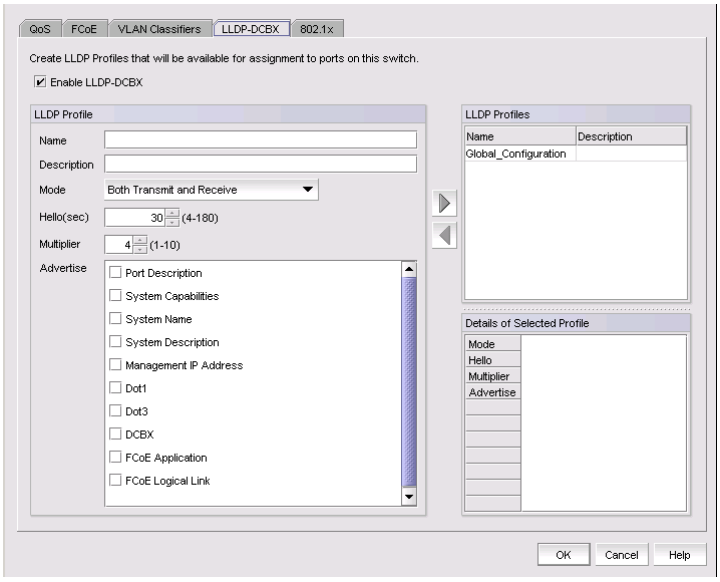


FIGURE 191 Edit Switch dialog box - LLDP-DCBX tab

Adding an LLDP profile

NOTE
When a TE port is selected to assign to an LLDP profile, a yellow banner displays with the following error message: "LLDP-DCBX is disabled on this switch. The configuration becomes functional when LLDP-DCBX is enabled on the switch."

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **LLDP-DCBX** tab on the **Edit Switch** dialog box.

   The **LLDP-DCBX** dialog box displays.

4. Click the **Enable LLDP-DCBX** checkbox.
5. Configure the LLDP Profile parameters:
   - Enter a name for the LLDP profile.

     If the name of the LLDP profile already exists on the switch, an overwrite warning displays.

   - Enter a meaningful description of the LLDP profile.
   - Select a mode from the list: Both Tx (transmitted) or Rx (received), Tx only, or Rx only.
   - Enter a hello interval time (in seconds) for the bridge in the **Hello (secs)** field. The value range is from 4 through 180 and the default value is 30.
   - Enter a multiplier (in seconds). The value range is from 1 through 10 and the default is 4.
   - Check the profile parameters that you want to display as part of the LLDP profile from the **Advertise** list:
     - Port description - The user-configured port description.
     - System name - The user-configured name of the local system.
     - System capabilities - The system capabilities running on the system.
     - System description - The system description containing information about the software running on the system.
     - Management IP address - The management IP address of the local system.
     - Dot *x*
     - DCBX - The DCBX profiles.
     - FCoE application - The FCoE application feature.
     - FCoE logical link - The logical link level for the SAN network.
6. Click the right arrow button to move the newly created profile into the **LLDP Profiles** list.
7. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.

Editing an LLDP profile

1. Select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **LLDP-DCBX** tab on the **Edit Switch** dialog box.

   The **LLDP-DCBX Profile** dialog box displays.

4. Select an LLDP profile in the **LLDP Profile** list.

   NOTE
   You can edit the <Global Configuration> profile. You cannot, however, delete or duplicate global configurations.

5. Click the left arrow to load the LLDP profile's values in the left pane.
6. Modify the values, as described in "Adding an LLDP profile" on page 515. You are not allowed to modify the LLDP profile's name.
7. Click the right arrow to update the LLDP profile parameters.
8. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.

Deleting an LLDP profile

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **LLDP-DCBX** tab on the **Edit Switch** dialog box.
4. Select an existing LLDP profile from the **LLDP Profiles** list in the upper right pane.

   NOTE
   You cannot delete <Global Configurations>. You can, however, edit global configurations. For more information, refer to "Product configuration templates" on page 779.

5. Click the left arrow button.

   The selected LLDP profile is removed from the list.

6. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.
7. Click **OK**.

   The **Deployment Status** dialog box launches.

8. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected devices.
9. Click **Close** to close the **Deployment Status** dialog box.

Assigning an LLDP profile to a port or ports in a LAG

You create LLDP profiles using the **Edit Switch** dialog box, which you access from the **DCB Configuration** dialog box. Global configuration parameters, which is the default selection, are displayed in the Assigned Profile table.

NOTE
A yellow banner displayed on the **LLDP-DCBX** dialog box indicates that LLDP-DCBX is disabled on the switch. The configuration options become functional when LLDP-DCBX is enabled on the switch.

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a port or link aggregation group (LAG), and click **Edit**.
3. Click the **LLDP-DCBX** tab on the **Edit Port** or **Edit LAG** dialog box.

   The **Assign an LLDP profile** dialog box displays.

4. Click **Assign an LLDP profile to <port name>** button to enable the feature.

   NOTE
   Assign the Global Configuration is the default. The **Available Profiles** list is disabled if global configuration is selected. In addition, the **Assign an LLDP profile** button is disabled if no LLDP profiles exist on the switch.

5. Select an LLDP profile from the **Available Profiles** list.
6. When you have finished the configuration, click **OK** to launch the **Deploy to Ports/LAGs** dialog box. Refer to "Switch, port, and LAG deployment" on page 520 for more information.

802.1x authentication

802.1x is a standard authentication protocol that defines a client-server-based access control and authentication protocol. 802.1x restricts unknown or unauthorized clients from connecting to a LAN through publicly accessible ports.

NOTE
802.1x is not supported for internal ports.

A switch must be enabled for 802.1x authentication before you configure its parameters. See "Setting 802.1x parameters for a port" for more information.

Enabling 802.1x authentication

802.1x authentication is enabled or disabled globally on the switch using the **Edit Switch** dialog box.

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch and click **Edit**.
3. Click the 802.1x tab on the **Edit Switch** dialog box.
4. Click the **Enable 802.1x** check box to enable 802.1x authentication, and click **OK**.
5. Configure the 802.1x parameters, which are described in "Setting 802.1x parameters for a port" on page 518.
6. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.

Disabling 802.1x authentication

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch and click **Edit**.
3. Click the 802.1x tab on the **Edit Switch** dialog box.
4. Clear the **Enable 802.1x** check box to disable 802.1x authentication.
5. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.

Setting 802.1x parameters for a port

The 802.1x parameters can be configured whether or not the feature is enabled on the switch. The default parameters are initially populated when 802.1x is enabled, but you can change the default values as required.

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a port and click **Edit**.
3. Click the 802.1x tab on the **Edit Port** dialog box.

   The **Enable 802.1x** dialog box displays, as shown in Figure 192.

4. Click the **Enable 802.1x** check box to enable 802.1x authentication.

   The 802.1x parameters are enabled for editing.

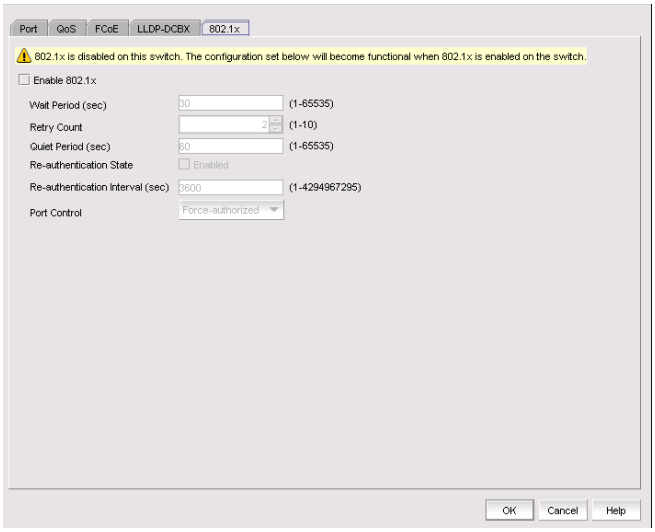


FIGURE 192 802.1x dialog box

5. Configure the following 802.1x parameters:
   - **Wait Period** - The number of seconds the switch waits before sending an EAP request. The value range is 15 to 65535 seconds. The default value is 30.
   - **Retry Count** - The maximum number of times that the switch restarts the authentication process before setting the switch to an unauthorized state. The value range is 1 to 10. The default value is 2.
   - **Quiet Period** - The number of seconds that the switch remains in the quiet state after a failed authentication exchange with the client. The value range is 1 to 65535 seconds. The default value is 60.
   - **Re-authentication State** - Enable or disable the periodic re-authentication of the client. The default is Disable.
   - **Re-authentication Interval** - The number of seconds between re-authentication attempts. The value range is 1 to 4294967295. The default value is 3600 seconds. This feature is not dependent on the re-authentication state being enabled.
   - **Port Control** - Select an authorization mode from the list to configure the ports for authorization. Options include auto, force-authorized, or force-unauthorized and the default value is auto.
6. When you have finished the configuration, click **OK** to launch the **Deploy to Ports** dialog box. Refer to "Switch, port, and LAG deployment" on page 520 for more information.

Switch, port, and LAG deployment

The **Deploy to Products**, **Deploy to Ports**, and **Deploy to LAGs** dialog boxes provide the flexibility to commit DCB configurations either right away or at a scheduled time. These dialog boxes also allow you to commit the switch-level configuration changes to one or more target switches.

NOTE
Deployment from the Management application to a Network OS device is not supported.

Deploying DCB product, port, and LAG configurations

The switch, port, and LAG deployment dialog boxes provide common deployment options, save configuration options, and schedule options. Depending on which product, port, or LAG you select, the **Deploy to Products**, **Deploy to Ports**, or **Deploy to LAGs** dialog box displays upon deployment.

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch, port, or LAG, and click **Edit**.

3. Configure the switch, port, or LAG. When you have finished the configuration, click **OK** to launch the appropriate dialog box. Refer to Figure 193, Figure 194, and Figure 195.

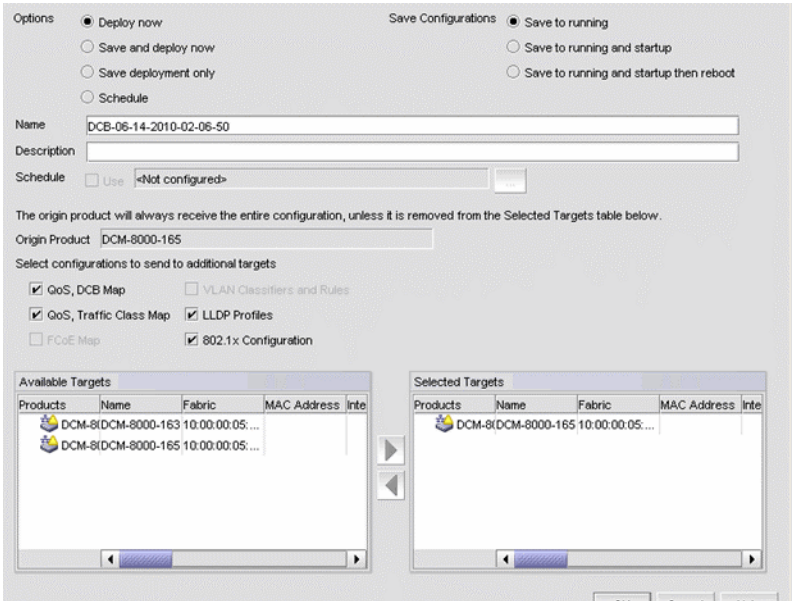


FIGURE 193 Deploy to Products dialog box

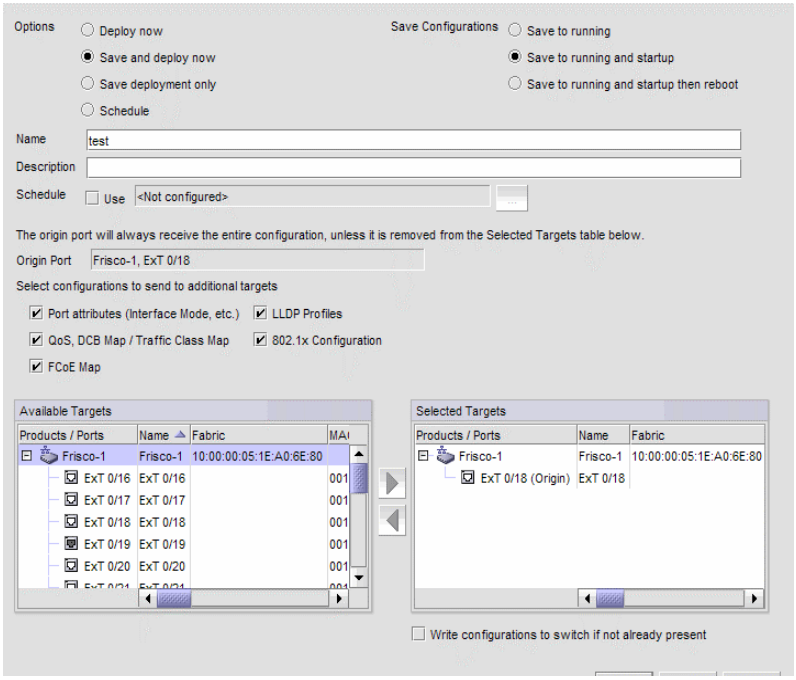


FIGURE 194 Deploy to Ports dialog box

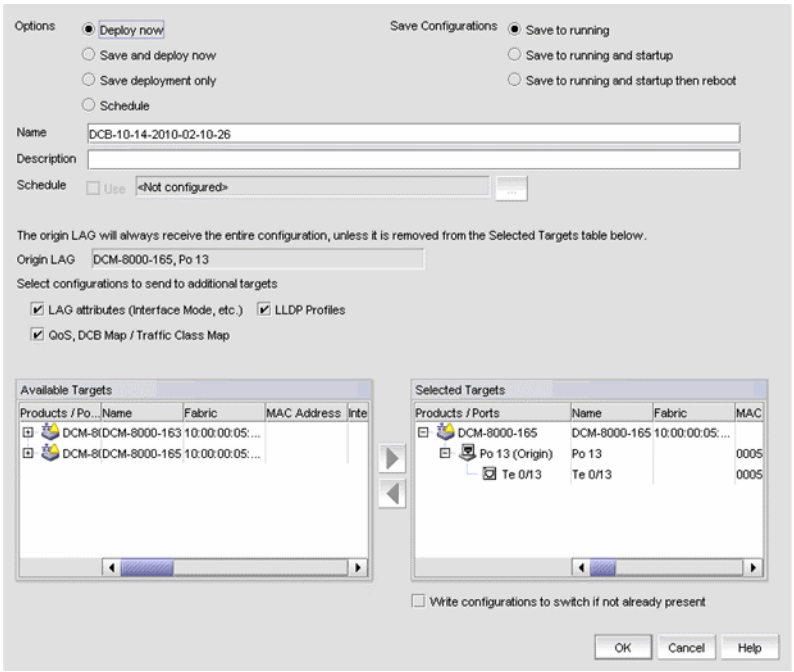


FIGURE 195 Deploy to LAGs dialog box

4. Click one of the following deployment options:
   - Deploy now
   - Save and deploy now
   - Save deployment only
   - Schedule
5. Click one of the following save configuration options:
   - Save to running
   - Save to running and startup
   - Save to running and startup then reboot

   The name for the scheduled product deployment is pre-populated with a "DCB-MM-DD-YYYY-HR-MIN-SS" prefix. This is an editable field.
6. Provide a description for the product/port/LAG deployment.
7. If the **Schedule** option is selected, click the **Use** check box for one-time deployment. One-time deployment is the only option.

   The name of the origin product is a read-only field. The origin product receives the entire configuration, unless it is removed from the **Selected Targets** list.
8. Select one or more of the following configurations, to be deployed on the selected targets.

NOTE
These configurations can be pushed to target DCB switches, FOS version 6.3.1_cee or 6.3.1_del.

For switches:

- QoS, DCB Map
- QoS, Traffic Class Map
- FCoE Map
- VLAN Classifiers and Rules
- LLDP Profiles
- 802.1x Configuration

NOTE
See "Source to target switch Fabric OS version compatibility for deployment" for restrictions.

For ports:

- Port attributes (interface mode, etc.)
- QoS, DCB Map / Traffic Class Map
- FCoE Map
- LLDP Profiles
- 802.1x Configuration

NOTE
On the **Deploy to Ports** dialog box, you can write port configurations to the switch by enabling the check box at the bottom of the dialog box.

For LAGs:

- LAG attributes (Interface Mode, etc.)
- QoS, DCB Map / Traffic Class Map
- LLDP Profiles

9. Click to move the available targets selected for configuration deployment to the **Selected Targets** list.
10. Click **OK**.

    The **Deployment Status** dialog box launches.
11. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected devices.
12. Click **Close** to close the **Deployment Status** dialog box.

Source to target switch Fabric OS version compatibility for deployment

Table 55 lists the restrictions that exist when deploying source switches to target switches.

TABLE 55 Source to target switch Fabric OS version compatibility

Source Fabric OS version and device	Target Fabric OS version supported	Comments
Fabric OS DCB switch and FCOE10-24 DCB blade with Fabric OS version 6.4.2 or earlier.	Allows Fabric OS DCB switch and FCOE10-24 DCB blade with Fabric OS version 6.4.2 or earlier. Excludes Fabric OS Converged 10 Gbe switch module for IBM BladeCenter with Fabric OS 6.3.1_cee, Fabric OS 6.4.1_fcoe, and Fabric OS 6.3.1_dcb.	You cannot copy legacy configurations to Fabric OS version 7.0 switches, because these switches support FCoE maps and can have only one default DCB map. Legacy Fabric OS switches, however, can have more than one default map.
Fabric OS FCOE10-24 DCB blade with Fabric OS 6.4.1_fcoe	Allows FCOE10-24 DCB blade with Fabric OS 6.4.1_fcoe or Fabric OS 7.0.0. Allows Fabric OS Converged 10 Gbe switch module for IBM BladeCenter with Fabric OS 6.3.1_cee or Fabric OS 6.3.1_dcb. Excludes Fabric OS DCB switch and FCOE10-24 DCB blade with Fabric OS 6.4.2 or earlier.	Both the source and the target support only one default DCB map. You can copy QoS, LLDP, and 802.1x configurations from the source to the target.
Fabric OS DCB switch FCOE10-24 DCB blade with Fabric OS 7.0.	Allows Fabric OS DCB switch and FCOE10-24 DCB blade with Fabric OS 7.0.0. Excludes all others.	VLAN classifiers are supported, but the FCoE map is not supported on Fabric OS 7.0.0.

TABLE 55 Source to target switch Fabric OS version compatibility (Continued)

Source Fabric OS version and device	Target Fabric OS version supported	Comments
Fabric OS Converged 10 GbE switch module for IBM BladeCenter with Fabric OS 6.3.1_cee and 6.3.1_dcb	Allows Fabric OS Converged 10 Gbe switch module for IBM BladeCenter with Fabric OS 6.3.1_cee, Fabric OS 6.3.1_dcb. Allows Dell M8428-k switch with Fabric OS 6.3.1_dell, Fabric OS 6.3.1_dcb.	Both source and target switches must support the FCoE map and VLAN classifiers.
Dell M8428-k switch with Fabric OS 6.3.1_dell and 6.3.1_dcb	Allows Fabric OS Converged 10 Gbe switch module for IBM BladeCenter with Fabric OS 6.3.1_cee, Fabric OS 6.3.1_dcb. Allows Dell M8428-k switch with Fabric OS 6.3.1_dell, Fabric OS 6.3.1_dcb.	Both source and target switches must support the FCoE map and VLAN classifiers.

Network OS switches in VCS mode

For a Network OS switch in VCS mode or standalone mode, you can use the management application to perform the following tasks:

- View Network OS switches, ports, LAGs, and vLAGs and their basic configuration details and detailed DCB configurations.
- Enable and disable ports, LAGs, and vLAGs.
- View real-time performance graphs.
- View historical graphs and reports.
- View profiled port, LAG, and vLAG configurations.
- View the list of virtual FCoE ports.
- Enable, disable, and view Connected End Device details for the listed virtual FCoE ports.
- Launch the VLAN Manager.
- Launch the Access Control List (ACL) Manager.

NOTE
Network OS switches in standalone mode do not support FCoE login group management or virtual FCoE port management.

NOTE
Network OS switches in VCS mode do not support FCoE login group management.

Supported VCS platforms

The following switches are supported in a virtual fabric switching environment:

- VDX 2730 10 GbE connection blade for the Fujitsu PRIMERGY BX900 and BX400 Blade Servers
- VDX 6710
- VDX 6720-24
- VDX 6720-60
- VDX 6730-32
- VDX 6730-76
- VDX 6740
- VDX 6740T
- VDX 8770-4
- VDX 8770-8

Viewing switches in VCS mode

1. Launch the DCB Configuration dialog box using one of the following methods:
   - Select **Configure > DCB** from the menu bar.
   - Right-click the DCB switch from the device tree, and select **Configure > DCB**.
   - Right-click the DCB switch from the topology map and select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.
2. Select a Network OS switch in the **DCB Products/Ports** table and click **View**.

   The **View Switch** dialog box displays, allowing you to view the Network OS switch parameters.
3. Click one of the following tabs and refer to the appropriate corresponding table for a description of the feature parameters.
   - **QoS** — Refer to "Viewing QoS parameters on the Network OS switch" on page 526.
   - **FCoE** — Refer to "Viewing FCoE parameters on the Network OS switch" on page 526.
   - **VLAN Classifiers** — Refer to "Viewing VLAN classifiers and rules parameters on the Network OS switch" on page 527.
   - **LLDP-DCBX** — Refer to "Viewing LLDP-DCBX parameters on the Network OS switch" on page 527.
   - **802.1x** — "Viewing the 802.1x parameter on the Network OS switch" on page 528.

Viewing QoS parameters on the Network OS switch

Table 56 describes the parameters that displays on the **View Switch** dialog box - **QoS** tab.

NOTE
Network OS switches in VCS mode support only the DCB map. Network OS switches in standalone mode supports both the DCB and Traffic Class maps.

TABLE 56 QoS configuration parameters on VCS switch

Map Type	Displays the map type: DCB or Traffic Class for a Standalone Network OS switch or DCB for Network OS switches in VCS mode.
DCB Maps list	Displays the following map information: • Name — The name of the map. • Precedence — The precedence number that determines the map's priority. Valid values are from 1 through 100. • Fabric Remap Priority — The fabric remap priority of the port. Valid values are CoS 0 through CoS 6, and the default is CoS 0. • Lossless Remap Priority — The FCoE lossless remap priority of the port. Valid values are CoS 0 through CoS 6, and the default is CoS 0.
DCB Map Parameters	Displays the following map parameters: • PG ID — Lists the priority group ID (15.0 to 15.7 and 0 to 7). • % Bandwidth — Lists the bandwidth value for priority group IDs 0-7. The total of all priority groups must equal 100%. • Priority Flow — Check to enable priority flow control on individual priority groups. • CoS — Lists the Class of Service (CoS) value that corresponds to the Priority Group ID rows. The CoS value must be mapped to at least one of the Priority Group IDs (0-7).

Viewing FCoE parameters on the Network OS switch

Table 57 describes the parameters that displays on the **View Switch** dialog box - **FCoE** tab.

TABLE 57 FCoE configuration parameters on VCS switch

Field/Component	Description
FCoE Map **Note:** The default FCoE map contains both the default Fabric map and the default DCB map.	Displays the following information about the FCoE map: • Fabric Map — The name of the Fabric map. The default Fabric map consists of virtual fabric and FCoE VLAN-related information. • DCB Map — The name of the DCB map.
Fabric Map	Displays the following information about the Fabric map: • VLAN ID — The FCoE VLAN identifier associated with the Fabric map. • FCMAP — The unique MAC address prefix an FCoE Forwarder (FCF) uses to identify FCoE traffic on a particular FCoE VLAN. • Fabric ID — The Fabric identifier. • Priority — The FCoE priority forwarding class to queue mapping. • FIP Advertisement Interval — Displays the frequency, in seconds, at which FIP advertisements are set. • FIP Keep Alive Timeout — Displays whether the Keep Alive Timeout feature is enabled. The feature represents the amount of time (in seconds) to keep keep-alive connections active.

Viewing VLAN classifiers and rules parameters on the Network OS switch

Table 58 describes the parameters that display on the **View Switch** dialog box - **VLAN Classifiers** tab.

TABLE 58 VLAN classifiers and rules configuration parameters on VCS switch

Field/Component	Description
Available Rules	Displays the following Available Rules information: • Rule ID — The rule identifier. Valid rule ID values are from 1 through 256. • Rule Type — Valid rule types are MAC (MAC address-based rule) and Proto (802.1Q protocol-based rule). • Encapsulation — The encapsulation type (ethv2/nosnaplic/snaplic). Encapsulation only displays a value when Proto is selected as the rule type.
VLAN Classifiers	Displays the following VLAN Classifier information: • Classifiers/Rules — A tree that displays the classifier nodes and rules. • Rule Type — Valid rule types are MAC (MAC address-based rule) and Proto (802.1Q protocol-based rule). • Encapsulation — The encapsulation type (ethv2/nosnaplic/snaplic). Encapsulation only displays a value when Proto is selected as the rule type.

Viewing LLDP-DCBX parameters on the Network OS switch

Table 59 describes the LLDP profiles table (in global configuration) and the LLDP profiles.

TABLE 59 LLDP-DCBX configuration parameters on VCS switch

Field/Component	Description
LLDP Profiles list	Lists the currently available LLDP profiles, the profile parameters (name and description) and whether the profiles are enabled or disabled.
LLDP Profile Parameters	Displays the following details of the selected LLDP profile: • Mode — The Transmit and Received mode. Options include Both Transmit and Received, Transmit Only, or Receive Only. • iSCSI Priority — The CoS priority value for iSCSI traffic. The value range is from COS 0 through COS 7 and the default value is COS 4. • Hello — The hello interval time (in seconds) for the bridge. The value range is from 4 through 180 and the default value is 30. • Multiplier — The multiplier (in seconds). The value range is from 2 through 10 and the default is 4. • Advertise — The following profiles that are configured to advertise. - Port Description - System Capabilities - System Name - System Description - Management IP Address - Dot 1 - Dot 3 - DCBX - FCoE Application - FCoE Logical Link - iSCSI Application

Viewing the 802.1x parameter on the Network OS switch

Table 60 describes the parameter that displays on the **View Switch** dialog box - **QoS** tab.

TABLE 60 802.1x configuration parameter on VCS switch

Field/Component	Description
802.1x	Displays the enabled or disabled status of the 802.1x configuration on the Network OS switch.

Viewing ports in VCS mode

1. Launch the DCB Configuration dialog box using one of the following methods:
   - Select **Configure > DCB** from the menu bar.
   - Right-click the DCB switch from the device tree, and select **Configure > DCB**.
   - Right-click the DCB switch from the topology map and select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.
2. Select a Network OS switch port in the **DCB Products/Ports** table and click **View**.

   The **View Port** dialog box displays, allowing you to view the Network OS switch port parameters.
3. Click one of the following tabs and refer to the appropriate corresponding table for a description of the feature parameters.
   - **Port** — "Viewing port parameters on the Network OS switch port" on page 528
   - **QoS** — Refer to "Viewing QoS parameters on the Network OS switch port" on page 529.
   - **FCoE** — Refer to "Viewing FCoE parameters on the Network OS switch port" on page 530.
   - **LLDP-DCBX** — Refer to "Viewing LLDP-DCBX parameters on the Network OS switch port" on page 531.
   - **802.1x** — "Viewing the 802.1x parameter on the Network OS switch port" on page 531.

Viewing port parameters on the Network OS switch port

Table 61 describes the parameters that displays on the **View Port** dialog box — **Port** tab.

TABLE 61 Port parameters on the Network OS switch port

Field/Component	Description
Port	The status of the port (enabled or disabled).
Profile	The port's profiled status (enabled or disabled). When enabled, the Interface Mode, L2 Mode, and Default CoS are configured by way of port profiles.
Interface Mode	The port's configured operating mode. Options include L2 (Layer 2) and None. <profile> is displayed if the port is profiled.
L2 Mode	The L2 mode. Supported L2 modes for a port are Access, Trunk, and Converged. <profile> is displayed if the port is profiled.
Default CoS	The default Cost of Service (CoS) assigned to the port. The value range is from COS 0 through COS 7 and the default value is COS 0. <profile> is displayed if the port is profiled.

TABLE 61 Port parameters on the Network OS switch port (Continued)

Field/Component	Description
MTU	The maximum transmission unit (MTU) in bytes. The value range is from 1522 through 9216 and the default value is 2500.
iSCSI Priority	The CoS priority value for iSCSI traffic. The value range is from COS 0 through COS 7 and the default value is COS 4.

Viewing QoS parameters on the Network OS switch port

Table 62 (DCB) and Table 63 (non-DCB) describe the parameters that displays on the **View Port** dialog box - **QoS** tab.

NOTE
Network OS switches with VCS enabled supports only the DCB map. Network OS switches in standalone mode supports both the DCB and Traffic Class maps.

QoS-DCB

TABLE 62 QoS (DCB) parameters on the Network OS switch port.

Field/Component	Description
Mode	The QoS mode (DCB).
Fabric Remap Priority	The fabric remap priority of the port. Valid values are CoS 0 through CoS 6, and the default is CoS 0.
DCB Map	The DCB map that is associated with the FCoE Map. This is a read-only field.
Lossless Remap Priority	The FCoE lossless remap priority of the port. Valid values are CoS 0 through CoS 6, and the default is CoS 0.
Precedence	This number determines the map's priority. Valid values are from 1 through 100.
DCB Map Parameters	• PG ID — Lists the priority group ID (15.0 to 15.7 and 0 to 7). • % Bandwidth — Lists the bandwidth value for priority group IDs 0-7. The total of all priority groups must equal 100%. • Priority Flow Control — When enabled, enables priority flow control on individual priority groups. • CoS — Lists the Class of Service (CoS) value that corresponds to the Priority Group ID rows. The CoS value must be mapped to at least one of the Priority Group IDs (0-7).

QoS - Non-DCB

TABLE 63 QoS (non-DCB) parameters on the Network OS switch port

Field/Component	Description
Mode	The mode of Quality of Service (QoS) assigned to the port (non-DCB).
Trust **NOTE:** Applicable only for standalone Network OS devices.	Indicates whether the Ethernet trust of the port is enabled or disabled.
Flow Control	The Ethernet priority flow control mode of the port. The default flow control mode is Off. Possible modes are as follows: • Off • 802.3x pause • Tx On or Off • Rx On or Off • Priority Flow Control. For this mode, the Tx and Rx values for each CoS display in the table.
Maps	Displays details about the following DCB maps: • CoS to CoS — Displays the details of the CoS to CoS map assigned to the port. • Traffic Class — Displays the details of the Traffic Class map assigned to the port.

Viewing FCoE parameters on the Network OS switch port

Table 64 describes the parameters that displays on the **View Port** dialog box - **FCoE** tab.

TABLE 64 FCoE parameters on the Network OS switch port

Field/Component	Description
FCoE	If the port was FCoE-enabled, then the FCoE field is Enabled. If the FCoE map is not assigned to the selected port, the FCoE tab is hidden.
FCoE Map Parameters	Displays the following FCoE map and Fabric map parameters: FCoE Map • Fabric Map — The Fabric map that is associated with the FCoE map. • DCB Map — The DCB map that is associated with the FCoE map. Fabric Map • VLAN ID — Displays the FCoE VLAN identifier that associates the VLAN with the FCoE map. The values range from 2 through 3583, and 1002 is the default. • FCMAP — The unique MAC address prefix an FCoE Forwarder (FCF) uses to identify FCoE traffic on a particular FCoE VLAN. • Fabric ID — The Fabric identifier. The default value is 128. • Priority — The FCoE priority forwarding class to queue mapping. The default priority value is 3. • FIP Advertisement Interval — Displays the frequency, in seconds, at which FIP advertisements are set. The default interval value is 8000. • FIP Keep Alive Timeout — Displays whether the Keep Alive Timeout feature is enabled. The feature represents the amount of time (in seconds) to keep keep-alive connections active. The default value is Enabled.

Viewing LLDP-DCBX parameters on the Network OS switch port

Table 65 describes the LLDP profiles table (in global configuration) and the LLDP profiles.

TABLE 65 LLDP-DCBX parameters on the Network OS switch port

Field/Component	Description
LLDP-DCBX	Indicates whether LLDP-DCBX feature is enabled or disabled.
LLDP Profile Parameters	Displays the following LLDP profile parameters: • Name — The name of the LLDP profile. • Description — A description of the LLDP profile. • Mode — The Transmit and Received mode. Options include Both Transmit and Received, Transmit Only, or Receive Only. • iSCSI Priority — The CoS priority value for iSCSI traffic. The value range is from COS 0 through COS 7 and the default value is COS 4. • Hello — The hello interval time (in seconds) for the bridge. The value range is from 4 through 180 and the default value is 30. • Multiplier — The multiplier (in seconds). The value range is from 2 through 10 and the default is 4. • Advertise — The profiles that are configured to advertise. The profile options are as follows: - Port Description - System Capabilities - System Name - System Description - Management IP Address - Dot 1 - Dot 3 - DCBX - FCoE Application - FCoE Logical Link - iSCSI Application

Viewing the 802.1x parameter on the Network OS switch port

Table 66 describes the parameter that displays on the **View Port** dialog box - **QoS** tab.

TABLE 66 802.1x parameter on the Network OS switch port

Field/Component	Description
802.1x	Indicates whether 802.1x is enabled or disabled. The 802.1x fields are hidden if 802.1x authentication is disabled on the port.
Wait Period (sec)	The number of seconds the switch waits before sending an EAP request. The value range is 15 to 65535 seconds. The default value is 30.
Retry Count	The maximum number of times that the switch restarts the authentication process before setting the switch to an unauthorized state. The value range is 1 to 10. The default value is 2.
Quiet Period (sec)	The number of seconds that the switch remains in the quiet state after a failed authentication exchange with the client. The value range is 1 to 65535 seconds. The default value is 60.
Re-authentication State	Whether the periodic re-authentication of the client is enabled or disabled. The default is Disable.

TABLE 66 802.1x parameter on the Network OS switch port (Continued)

Field/Component	Description
Re-authentication Interval (sec)	The number of seconds between re-authentication attempts. The value range is 1 to 4294967295. The default value is 3600 seconds. This feature is not dependent on the re-authentication state being enabled.
Port Control	The authorization mode to configure the ports for authorization. Options include Auto, Force-authorized, or Force-unauthorized. The default value is Auto.

Viewing LAGs in VCS mode

1. Launch the DCB Configuration dialog box using one of the following methods:
   - Select **Configure > DCB** from the menu bar.
   - Right-click the DCB switch from the device tree, and select **Configure > DCB**.
   - Right-click the DCB switch from the topology map and select **Configure > DCB**.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.
2. Select a Network OS switch LAG in the **DCB Products/Ports** table and click **View**.

   The **View LAG** dialog box displays, allowing you to view the Network OS switch port parameters.
3. Click one of the following tabs and refer to the appropriate corresponding table for a description of the feature parameters.
   - **LAG** — "Viewing LAG parameters on the Network OS switch LAG" on page 532
   - **QoS** — Refer to "Viewing QoS parameters on the Network OS switch LAG" on page 533.
   - **LLDP-DCBX** — Refer to "Viewing LLDP-DCBX parameters on the Network OS switch LAG" on page 535.
   - **FCoE** — Refer to "Viewing FCoE parameters on the Network OS switch" on page 526.

Viewing LAG parameters on the Network OS switch LAG

Table 67 describes the parameters that displays on the **View LAG** dialog box — **LAG** tab.

TABLE 67 LAG parameters on the Network OS switch LAG

Field/Component	Description
LAG ID	For Network OS switches in VCS mode, the LAG ID range is from 1 through 6144. For Network OS switches in standalone mode, the LAG ID range is from 1 through 64.
Interface Mode	The interface mode, which can be none or layer 2 (L2).
Profile	Indicates whether the LAG profile is enabled or disabled.
L2 Mode	The L2 mode (Access or Trunk): • Access mode allows only one VLAN and allows only untagged frames. • Trunk mode allows more than one VLAN association and allows tagged frames. **NOTE:** <profile> displays if the LAG is profiled.

TABLE 67 LAG parameters on the Network OS switch LAG (Continued)

Field/Component	Description
Status	Indicates whether the LAG is enabled or disabled. You must enable the LAG to use the DCB functionality.
Default CoS	The Cost of Service (CoS) value for incoming untagged frames. Values are 0-7 or <profile> if the port is profiled. The default CoS is 0.
Type	Displays the limit on the size of the LAG. The type values include Standard, where the LAG is limited to 16 ports, and Brocade LAG, where the LAG is limited to 8 ports. The default is Standard.
MTU	The maximum transmission unit (MTU). Valid values are from 1522 through 9216 bytes, and the default is 2500 bytes.
Mode	Displays how the ports are added to the LAG members table in either Static or Dynamic mode. The default is Dynamic, Active, but LAG members can be Active or Passive if the LAG member is Dynamic.
Minimum Links	Displays the minimum number of operationally UP links needed to declare the port channel UP. This field is applicable only for standalone Network OS devices.
LAG Members list	Lists the ports that are members of the LAG.

Viewing QoS parameters on the Network OS switch LAG

Table 68 (DCB) and Table 69 (non-DCB) describe the parameters that displays on the **View LAG** dialog box - **QoS** tab.

NOTE
Network OS switches in VCS mode support only the DCB map. Network OS switches in standalone mode supports both the DCB and Traffic Class maps.

QoS-DCB

TABLE 68 QoS (DCB) parameters on the Network OS switch LAG.

Field/Component	Description
Mode	The QoS mode (DCB).
Fabric Remap Priority	The fabric remap priority of the LAG. Valid values are CoS 0 through CoS 6, and the default is CoS 0.
DCB Map	The DCB map that is associated with the FCoE Map. This is a read-only field.
Lossless Remap Priority	The FCoE lossless remap priority of the LAG. Valid values are CoS 0 through CoS 6, and the default is CoS 0.

TABLE 68 QoS (DCB) parameters on the Network OS switch LAG. (Continued)

Field/Component	Description
Precedence	This number determines the map's priority. Valid values are from 1 through 100.
DCB Map Parameters	• PG ID — Lists the priority group ID (15.0 to 15.7 and 0 to 7). • % Bandwidth — Lists the bandwidth value for priority group IDs 0-7. The total of all priority groups must equal 100%. • Priority Flow Control — When enabled, enables priority flow control on individual priority groups. • CoS — Lists the Class of Service (CoS) value that corresponds to the Priority Group ID rows. The CoS value must be mapped to at least one of the Priority Group IDs (0-7).

QoS - Non-DCB

TABLE 69 QoS (non-DCB) parameters on the Network OS switch LAG

Field/Component	Description
Mode	The mode of Quality of Service (QoS) assigned to the LAG (non-DCB).
Trust NOTE: Applicable only for standalone Network OS devices.	Indicates whether the Ethernet trust of the LAG is enabled or disabled.
Flow Control	The Ethernet priority flow control mode of the LAG. The default flow control mode is Off. Possible modes are as follows: • Off • 802.3x pause • Tx On or Off • Rx On or Off • Priority Flow Control. For this mode, the Tx and Rx values for each CoS display in the table.
Maps	Displays details about the following DCB maps: • CoS to CoS — Displays the details of the CoS to CoS map assigned to the port. • Traffic Class — Displays the details of the Traffic Class map assigned to the port.

Viewing FCoE parameters on the Network OS switch LAG

Table 70 describes the parameters that displays on the **View LAG** dialog box - **FCoE** tab.

NOTE
The Interface mode is None and the L2 mode is empty for the FCoE-provisioned LAG.

TABLE 70 FCoE configuration parameters on VCS switch

Field/Component	Description
FCoE Map **Note:** The default FCoE map contains both the default Fabric map and the default DCB map.	Displays the following information about the FCoE map: • Fabric Map — The name of the Fabric map. The default Fabric map consists of virtual fabric and FCoE VLAN-related information. • DCB Map — The name of the DCB map.
Fabric Map	Displays the following information about the Fabric map: • VLAN ID — The FCoE VLAN identifier associated with the Fabric map. • FCMAP — The unique MAC address prefix an FCoE Forwarder (FCF) uses to identify FCoE traffic on a particular FCoE VLAN. • Fabric ID — The Fabric identifier. • Priority — The FCoE priority forwarding class to queue mapping. • FIP Advertisement Interval — Displays the frequency, in seconds, at which FIP advertisements are set. • FIP Keep Alive Timeout — Displays whether the Keep Alive Timeout feature is enabled. The feature represents the amount of time (in seconds) to keep keep-alive connections active.

Viewing LLDP-DCBX parameters on the Network OS switch LAG

Table 71 describe the parameters that displays on the **View LAG** dialog box - **LLDP-DCBX** tab.

TABLE 71 LLDP-DCBX parameters on the Network OS switch LAG

Field/Component	Description
Enable LLDP-DCBX check box	Indicates whether LLDP-DCBX feature is enabled or disabled and whether the global configuration or a specified LLDP profile has been assigned to the vLAG ports.
LLDP Profile Parameters	Displays the following LLDP profile parameters: • Name — The name of the LLDP profile. • Description — A description of the LLDP profile. • Mode — The Transmit and Received mode. Options include Both Transmit and Received, Transmit Only, or Receive Only. • Hello — The hello interval time (in seconds) for the bridge. The value range is from 4 through 180 and the default value is 30. • Multiplier — The multiplier (in seconds). The value range is from 1 through 10 and the default is 4. • Advertise — The profiles that are configured to advertise. The profile options are as follows: - DCBX - FCoE Application - FCoE Logical Link

DCB performance

Performance monitoring provides details about the quantity of traffic and errors a specific port or device generates on the fabric over a specific time frame. You can also use Performance features to indicate the devices that create the most traffic and to identify the ports that are most congested.

The Performance menu items launch either SAN or IP performance dialog boxes based on which tab you select. Note the following points:

- The DCB configuration dialog box can be launched from either the SAN or IP tab.
- The appropriate IP Performance tab launches depending on whether you selected a port or a switch.

Real-time performance graph

You can monitor a device's performance through a performance graph that displays transmit and receive data. The graphs can be sorted by the column headers. You can create multiple real-time performance graph instances.

Generating a real-time performance graph from the SAN tab

To generate a real-time performance graph for a FOS device, complete the following steps.

1. Click the SAN tab.
2. Select a DCB port from the **DCB Configuration** dialog box, and select **Real Time Graph** from the Performance list.

   A message displays, prompting you to close the **DCB Configuration** dialog box.
3. Click **OK** to close the **DCB Configuration** dialog and open the Performance dialog box.

   The **Real Time Performance Graphs** dialog box displays, as shown in Figure 196.

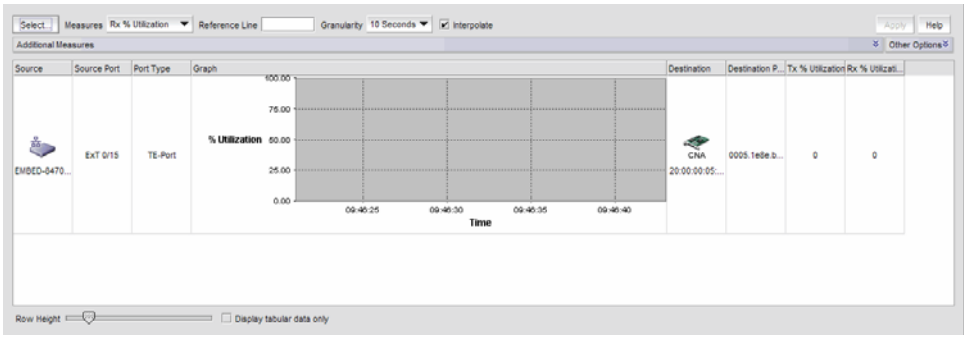


FIGURE 196 Real Time Performance Graphs dialog box - SAN tab

For complete information about Real Time Performance Graphs, refer to "SAN real-time performance data" on page 976.

Generating a real-time performance graph from the IP tab

To generate a real-time performance graph for a Network OS or FOS DCB switch, complete the following steps.

1. Click the IP tab.
2. Select a DCB port from the **DCB Configuration** dialog box, and select **Real Time Graph** from the Performance list.

   A message displays, prompting you to close the **DCB Configuration** dialog box.
3. Click **OK** to close the **DCB Configuration** dialog and open the Performance dialog box.

   The **Real Time Performance Graphs** dialog box displays, as shown in Figure 197.

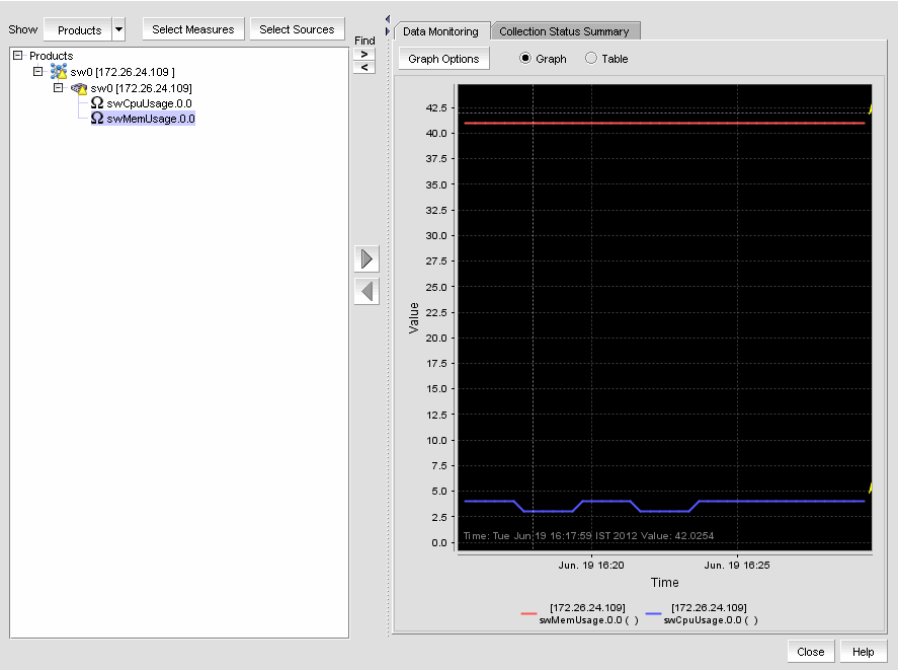


FIGURE 197 Real Time Performance Graphs dialog box - IP tab

For complete information about Real Time Performance Graphs, refer to "SAN real-time performance data" on page 976.

Historical performance graph

The **Historical Performance Graph** dialog box enables you to customize how you want the historical performance information to display.

Generating a historical performance graph

You can generate a historical performance graph by selecting both Network OS and FOS DCB devices from the IP Tab or by selecting only Network OS DCB devices from the IP tab.

1. Select a DCB port from the **DCB Configuration** dialog box, and select **Historical Graph** from the Performance list.

   A message displays, prompting you to close the **DCB Configuration** dialog.

2. Click **OK** to close the **DCB Configuration** dialog and open the Performance dialog box.

   The **Historical Performance Graph** dialog box displays.

For complete information about Real Time Performance Graphs, refer to "SAN real-time performance data" on page 976.

Historical performance report

The **Historical Performance Report** dialog box enables you to customize how you want the historical performance information to display.

Generating a historical performance report

1. Select a DCB port from the **DCB Configuration** dialog box, and select **Historical Report** from the Performance list.

   A message displays, prompting you to close the **DCB Configuration** dialog box.

2. Click **OK** to close the **DCB Configuration** dialog and open the Performance dialog box.

   The **Historical Performance Report** dialog box displays, as shown in Figure 198.

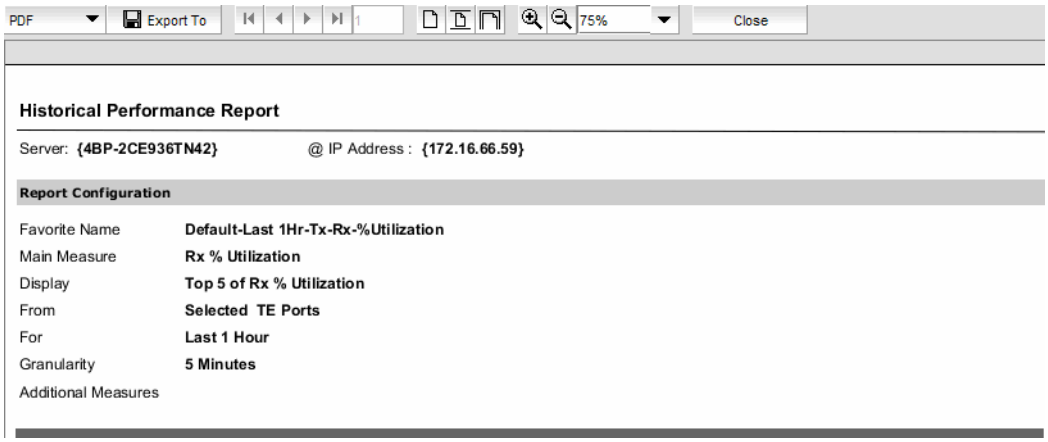


FIGURE 198 Historical Performance Report dialog box

FCoE login groups

The FCoE Configuration dialog box allows you to manage the FCoE login configuration parameters on the DCB switches in all discovered fabrics. FCoE login configuration is created and maintained as a fabric-wide configuration.

With the FCoE license, the **FCoE Configuration** dialog box displays virtual FCoE port information and enables you to manage the virtual port information. The topology displays directly connected converged network adapters (CNAs) and the **Properties** dialog box for the virtual FCoE port details.

Without the FCoE license, the virtual FCoE port displays in the device tree, but you cannot enable, disable, or view virtual FCoE port information.

NOTE
FCoE Login Group is not available for Network OS DCB devices.

1. Select **Configure > FCoE** from the menu bar.

   The **FCoE Configuration** dialog box displays all configured login groups and the following details associated with a selected device, shown in Figure 199.

   - FCoE login — Indicates whether the switch is FCoE enabled or disabled.
   - Group Status — Indicates whether the group is active or conflicted.
   - Member Status — Indicates whether the device associated with the group is active or conflicted.
   - Member WWN — Displays the world wide name (WWN) of the device associated with the group.
   - Type — Displays the model type.

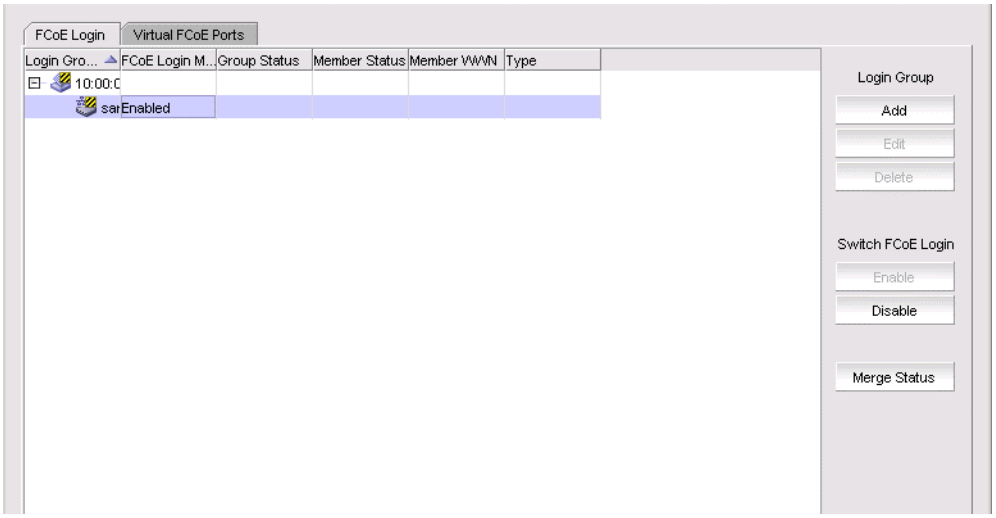


FIGURE 199 FCoE Configuration dialog box

2. Perform one of the following tasks:

   Under Login Group:

   - Click **Add** to launch the Add Login Group dialog box, where you can select an existing switch or enter the WWN of a switch on which the FCoE login group will be created. See "Adding an FCoE login group" on page 540.
   - Click **Edit** to launch the Edit Login Group dialog box, where you can edit the login group parameters. See "Editing an FCoE login group" on page 541.
   - Click **Delete** to remove the login group from the list. See "Deleting one or more FCoE login groups" on page 542.

Adding an FCoE login group

Complete the following steps to add switches to a login group. You can manually add ports by entering the world wide name (WWN) or select available managed CNAs from all discovered hosts. Only directly-connected devices are supported.

1. Select **Configure > FCoE** from the menu bar.

   or

   Right-click the DCB device and select **FCoE**.

2. Click **Add**.

   The **Add Login Group** dialog box displays, as shown in Figure 200.

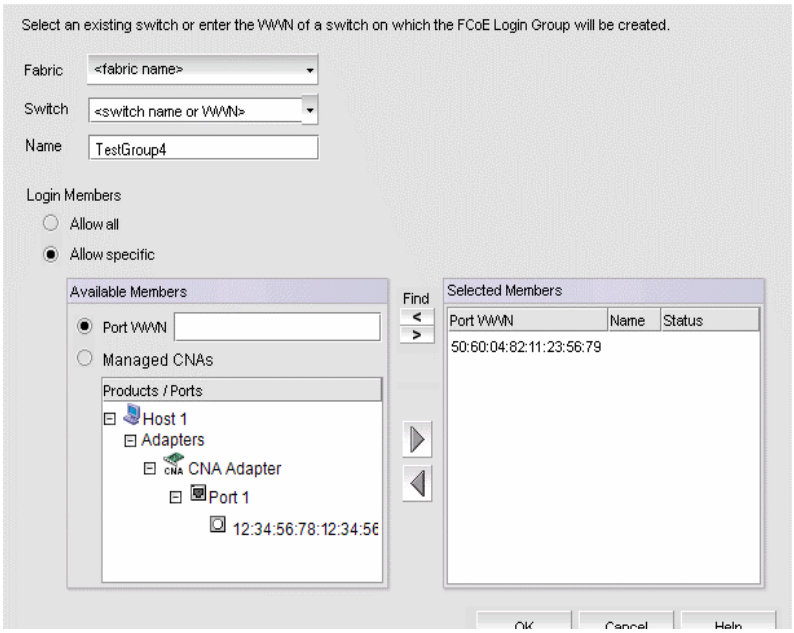


FIGURE 200 Add Login Group dialog box

3. Select an existing switch from the **Switch** list, or enter the WWN of the switch that will be added to the FCoE login group.
4. Select one of the following Login Members options:
   - Allow all — Click to allow all login members into the Available Members list.
   - Allow specific — Click to allow specific login members into the Available Members list. If you select this option, you can add specific login members using the options in the **Available Members** area.
5. Select one of the following Available Member options:
   - Port WWN — Click to enter the world wide name (WWN) of the port to associate with the selected switch. The member port WWN text field allows a maximum of 16 digits.
   - Managed CNAs — Click to show a list of products and ports which can be selected as login group members.
6. Select available members from the **Products/Ports** list and click the right arrow button to move the available members to the **Selected Members** list.

7. Click **OK**.

   The **FCoE Login Group Confirmation and Status** dialog displays.

8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

   On closing the FCoE Login Group Confirmation and Status dialog box, the **FCoE Configuration** Dialog refreshes the data and the latest information is displayed.

- "FCoE login groups"

Editing an FCoE login group

Complete the following steps to edit the name of a login group. You can manually add ports by entering the world wide name (WWN) or select available managed CNAs from all discovered hosts. Only directly-connected devices are supported.

1. Select **Configure > FCoE** from the menu bar.
2. Select a group from the Login Groups list and click **Edit**.

   The **Edit Login Group** dialog box displays, as shown in Figure 186.

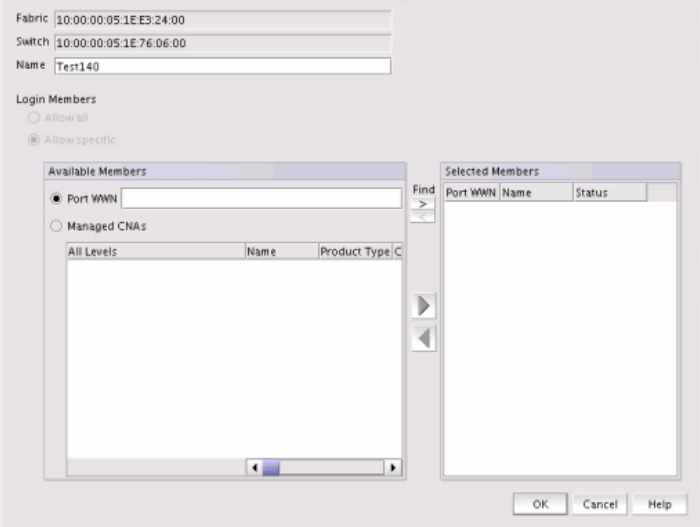


FIGURE 201 Edit Login Group dialog box

NOTE
The **Fabric** field and the **Switch** field are read-only fields.

3. Perform one of the following editing tasks:
   - Rename the login group by entering the new name into the **Name** field. The **Allow All** option must be selected to rename the login group.
   - Select one of the following options to add or remove login members into the **Available Members** list. The **Allow Specific** option must be selected to add or remove login members.
     - Port WWN — Click to enter the world wide name (WWN) of the port to associate with the selected switch. The member port WWN text field allows a maximum of 16 digits.

- Managed CNAs — Click to show a list of products and ports which can be selected as login group members.

4. Select available members from the **Products/Ports** list and click the right arrow button to move the available members to the **Selected Members** list.
5. Click **OK**.

   The **FCoE Login Group Confirmation and Status** dialog displays.
6. Review the changes carefully before you accept them.
7. Click **Start** to apply the changes, or click **Close** to abort the operation.

   On closing the FCoE Login Group Confirmation and Status dialog box, the **FCoE Configuration** Dialog refreshes the data and the latest information is displayed.

Deleting one or more FCoE login groups

1. Select **Configure > FCoE** from the menu bar.

   or

   Right-click the DCB device and select **FCoE**.

   The **FCoE Configuration** dialog box displays.
2. Select a group from the Login Groups list and click **Delete**.

   The **FCoE Login Group Confirmation and Status** dialog displays.
3. Review the changes carefully before you accept them.
4. Click **Start** to apply the changes, or click **Close** to abort the operation.

   The login group is removed from the **Login Group** table.

Disabling the FCoE login management feature on a switch

1. Select **Configure > FCoE** from the menu bar.

   or

   Right-click the DCB device and select **FCoE**.

   The **FCoE Configuration** dialog box displays.
2. Select an FCoE-enabled switch from the Login Groups list and click **Disable**.

   The **FCoE Login Group Confirmation and Status** dialog displays.
3. Review the changes carefully before you accept them.
4. Click **Start** to apply the changes, or click **Close** to abort the operation.

   The FCoE login management feature is disabled and all login groups on the selected switch are deleted.

   The value in the FCoE Login Management State column for the selected switch is **Disabled** and no login groups appear under the switch after the FCoE Configuration dialog box refresh operation.

- "FCoE login groups"

Enabling the FCoE login management feature on a switch

1. Select **Configure > FCoE** from the menu bar.

   or

   Right-click the DCB device and select **FCoE**.

   The **FCoE Configuration** dialog box displays.
2. Select an FCoE-disabled switch from the Login Groups list and click **Enable**.
3. The FCoE Login Group Configuration and Status dialog box displays.
4. Review the changes carefully before you accept them.
5. Click **Start** to apply the changes, or click **Close** to abort the operation.

   The FCoE login management feature is enabled on the selected switch.

   The value in the FCoE Login Management State column is **Enabled** after the **FCoE Configuration** dialog box refresh operation.

Virtual FCoE port configuration

The virtual FCoE port has the following configuration features:

- Displays the virtual FCoE ports on each of the DCB devices, which provides the Ethernet with bridging capability
- One-to-one mapping of FCoE ports with 10 Gbps Ethernet ports
- Option to enable or disable the virtual FCoE ports
- Option to view the end devices connected to a virtual FCoE port

Viewing virtual FCoE ports

Configuration of virtual FCoE ports requires installation of the FCoE license on the switch.

NOTE
For Network OS switches running the Network OS version 3.0 and later, the Management application retrieves all dynamically and statically bonded virtual FCoE ports in the virtual FCoE port pool and displays them. If there are no bonded virtual FCoE ports on any cluster member, then the cluster is not displayed.

The physical port and LAG details are displayed in the **Switch Port** column in the following circumstances:

- There is a dynamic binding between the virtual FCoE port and the physical port or LAG.
- There is a static binding between the virtual FCoE port and the physical port or lag and there are end devices connected to it.

To view the virtual FCoE ports, complete the following steps:

1. Select **Configure > FCoE** from the menu bar.

   or

Right-click the DCB device and select **FCoE**.

The **FCoE Configuration** dialog box displays.

2. Select the **Virtual FCoE Ports** tab.

   The **Virtual FCoE Ports** tab displays, as shown in Figure 202.

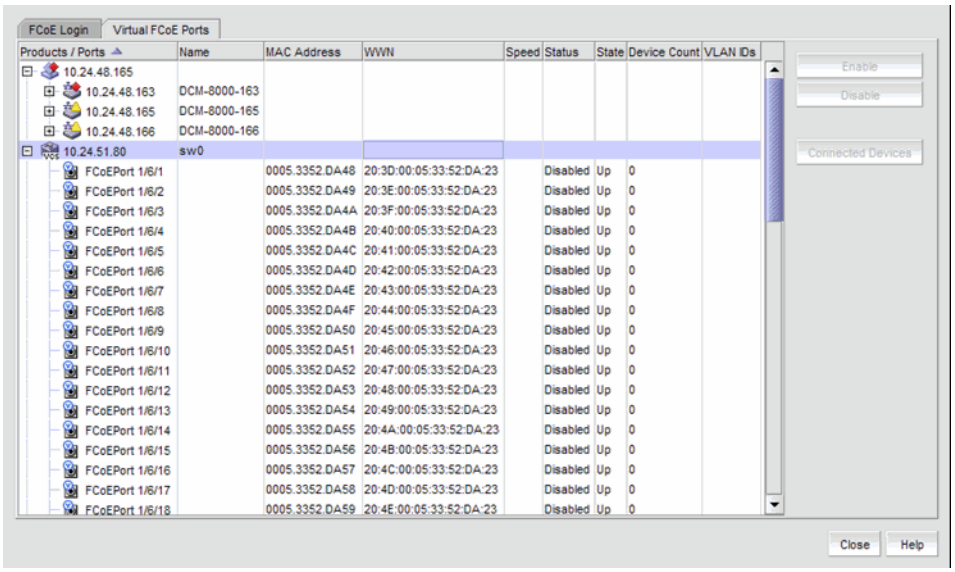


FIGURE 202 **Virtual FCoE Ports dialog box**

3. Select one or more virtual ports from the **Ports** list.
4. Perform one of the following tasks:
   - Click **Enable** to enable a selected virtual FCoE port from the **Virtual FCoE Ports** tab.
   - Click **Disable** to disable a selected virtual FCoE port from the **Virtual FCoE Ports** tab.
   - Click **Connected Devices** to view a list of FCoE virtual ports and to what they are directly connected.
5. Click **Close** to close the dialog box.

Clearing a stale entry

A stale entry is a device that logged in and logged off but, because a port went down after an FLOGI was received, the device failed to receive the message. The entry in the **FCoE Connected Devices** table becomes stale and you must clear it manually.

NOTE
Clearing a stale entry is not supported for Network OS devices.

1. Select a virtual FCoE port from the **FCoE Configuration** dialog box and click **Connected Devices**.

   The **Connected Devices** dialog box displays.

2. Select one or more rows from the **Connected Devices** table and click **Disconnect**.

   The **DCB Confirmation and Status** dialog displays.

The selected connected device should be cleared from the switch cache and from the table. Note, however, that the connected devices might still be active and this operation could potentially stop traffic between the connected devices and the switch.

3. Review the changes carefully before you accept them.
4. Click **Start** to apply the changes, or click **Close** to abort the operation.

   On closing the DCB Confirmation and Status dialog box, the **FCoE Configuration** Dialog refreshes the data and the latest information about the FCoE ports are displayed.

Chapter

17

Telemetry

In this chapter

Telemetry overview

NOTE
Network telemetry is only supported on Ethernet router, Ethernet core router, or Ehternet Backbone router products running 5.4 or later.

Network telemetry enables you to monitor, report, and analyze traffic information and data on your network. The Management application provides three features that enable you to perform Network telemetry:

- ACLs - Collection of permit and deny statements (rules) used to permit or deny incoming frames from passing through an interface. To create an ACL, refer to "Layer 3 access control list policy" on page 580.
- PBR - Collection of ACLs and route maps (rules) that enable you to redirect traffic. To create a policy-based routing policy, refer to "Adding a new policy" on page 550.
- ACL accounting - Counters used to track the number of times an ACL is used to filter traffic. To enable ACL accounting, refer to "Enabling or disabling ACL accounting" on page 558.

Policy-based routing

NOTE
Network telemetry is only supported on Ethernet router, Ethernet core router, or Ehternet Backbone router products running 5.4 or later.

Normally, when a router receives a packet it forwards it based on the destination address in the packet, PBR enables you to forward the packet based on other criteria such as, source or destination network, source or destination address, source or destination port, and protocol.

PBR uses access control lists (Layer 3 ACLs) and route maps (PBR policies) to filter and route IP packets to one or more specified ports.

- ACLs are used to classify the traffic.
- PBR policies are used to set routing attributes and next hop for the traffic. Next hop can be IP (IPv4 or IPv6 formats), Flood VLAN, or Port/LAG.

The Management application creates an IPv4 PBR or IPv6 PBR based on the ACLs defined in the policy.

- If any rule in the policy contains an IPv4 ACL, the Management application creates an IPv4 PBR applies the PBR to the ports.
- If any rule in the policy contains an IPv6 ACL, the Management application creates an IPv6 PBR applies the PBR to the ports.
- If the policy contains an IPv4 ACL and an IPv6 ACL in the same or different rules in the policy, the Management application creates both IPv4 and IPv6 PBRs applies the PBRs to the ports.

Viewing existing PBR policies

1. Select an Ethernet router, Ethernet core router, or Ehternet Backbone routerproduct and select **Configure > Policy Based Routing**.

   The *Product_Name* **PBR Configuration** dialog box displays.

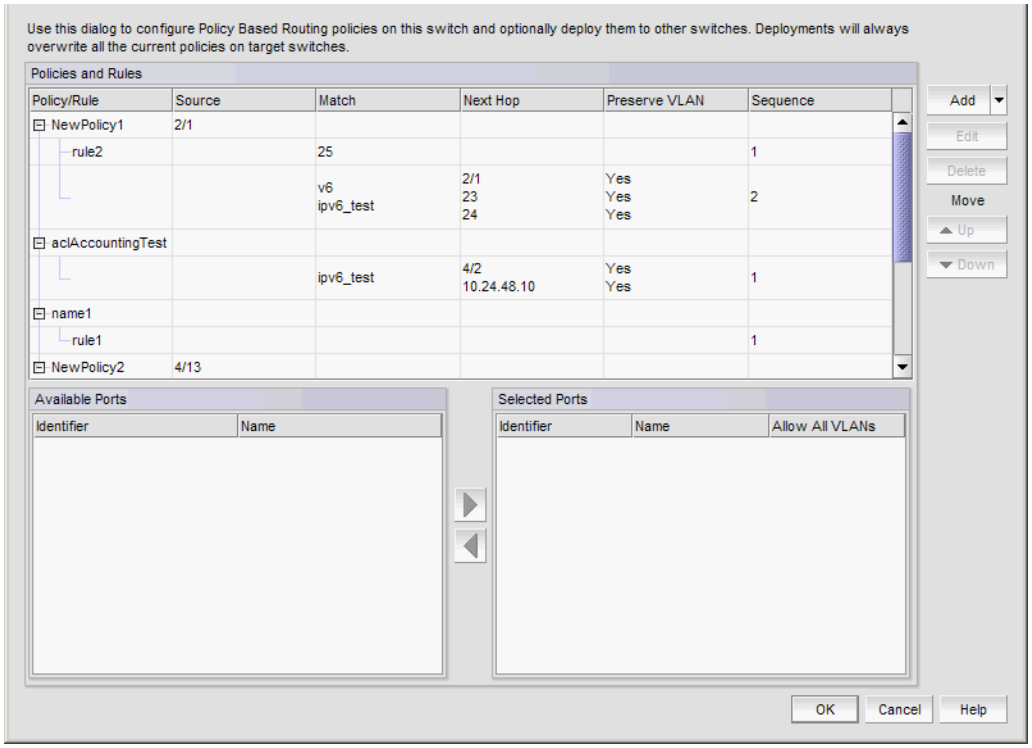


FIGURE 203 *Product_Name* **PBR Configuration dialog box**

- **Policies and Rules** table — All PBR policies defined on the selected product.
  - **Policy/Rule** — PBR policy or rule name.
    The policy name can be up to 80 characters and must be unique on the product. There is no specific limit to the maximum number of defined policies; however, it is limited by the system memory.
    The rule name can be up to 127 characters and must be unique within the policy. There is no specific limit to the number of rules with a single policy; however, PBR only uses the first 64 rules for comparison, then ignores the rest.

- **Source** — Port (one or more) to which this PBR policy is bound. For PBR policies bound to multiple ports, displays all ports separated by commas. For globally applied PBR policies, displays blank.
- **Match** — L3 ACL policy associated with the rule. You can define up to 10 ACL policies (5 IPv4 and 5 IPv6) per rule.
- **Next Hop** — Destination for the packets that pass ACL filter. You can define multiple next hops. PBR selects the first next hop from the next hop list that is up. If the first next hop goes down, PBR uses another next hop if available. If no next hops are available, the product routes the traffic in the normal way.
- **Preserve VLAN** — Whether or not VLAN tags are preserved or not.
- **Sequence** — Sequence number of the rule. The Management application auto-generates the number based on the order in which the policies are listed in the *Product_Name* **PBR Configuration** dialog box. Sequence numbers must be unique within a policy.
  Using the CLI, you can specify a sequence number when you create a rule and the Management application obtains the sequence number when PBR policies are read from the product. For more information, refer to the configuration guide for your product.

- **Add** button list — Select to choose one of the following options:
  - **Add New Policy** — Select to open the **PBR Policy Configuration** dialog box. For more information, refer to "Adding a new policy" on page 550.
  - **Add New Rule** — Select to open the **Add Rule** *Policy_Name* dialog box. For more information, refer to "Adding rules to a policy" on page 550.
  - **From Saved Configurations** — Select to open the **PBR Saved Configurations** dialog box. For more information, refer to "Adding policies from saved configurations" on page 552.
- **Edit** button — Click to edit the policy or rule selected in the **Policy and Rules** table. For more information, refer to "Editing a policy" on page 552 or "Editing a rule" on page 552.
- **Delete** button — Click to deleted the policy or rule selected in the **Policy and Rules** table. For more information, refer to "Deleting a policy or rule" on page 553.
- **Up** button — Click to move a rule up within in the policy.
- **Down** button — Click to move a rule down within in the policy.
- **Available Ports** table — Select a policy in the **Policy and Rules** table to display all ports not currently assigned to any policy. You can only bind one interface to one policy.
  - **Identifier** — Port number in slot/port format.
  - **Name** — Port name.
- Right arrow button — Click to move ports selected in the **Available Ports** table to the **Selected Ports** table.
- Left arrow button — Click to move ports selected in the **Selected Ports** table to the **Available Ports** table.
- **Selected Ports** table — Select a policy in the **Policy and Rules** table to display ports currently assigned to the policy.
  - **Identifier** — Port number in slot/port format.
  - **Name** — Port name.
  - **Allow All VLANs** check box — Checked if enabled (default). Clear is not enabled.

2. Click **Cancel** to close the *Product_Name* **PBR Configuration** dialog box.

Adding a new policy

1. Select an Ethernet router, Ethernet core router, or Ehternet Backbone router product and select **Configure > Policy Based Routing**.

   The *Product_Name* **PBR Configuration** dialog box displays.

2. Select **Add** > **New Policy**.

   The **PBR Policy Configuration** dialog box displays.

3. Enter a name for the new policy and click **OK** on the **PBR Policy Configuration** dialog box.

4. To add one or more rules to the policy, refer to "Adding rules to a policy" on page 550.

5. Click **OK** on the *Product_Name* **PBR Configuration** dialog box.

   The **Deploy to Products - PBR** dialog box displays. To deploy the PBR policy, refer to "Deploying a PBR policy on demand" on page 553, "Saving a PBR policy deployment" on page 554, or "Scheduling a PBR policy deployment" on page 555.

Adding rules to a policy

1. Select an Ethernet router, Ethernet core router, or Ehternet Backbone router product and select **Configure > Policy Based Routing**.

   The *Product_Name* **PBR Configuration** dialog box displays.

2. Select a policy or rule in the **Policies and Rules** table and select **Add** > **New Rule**.

   The **Add Rule** - *Policy_Name* dialog box displays.

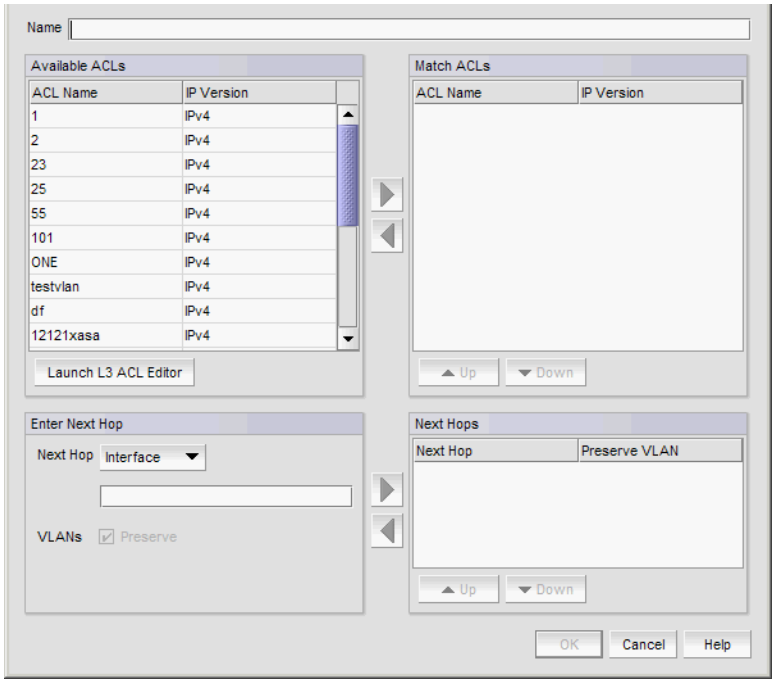


FIGURE 204 Add Rule *Policy_Name* dialog box

3. Enter a name for the rule in the **Name** field.

The rule name can be up to 127 characters and must be unique within the policy.

4. Select one or more ACLs to use in the rule from the **Available ACLs** table.

   Each rule can match up to 10 ACLs (5 IPv4 and 5 IPv6) and can have multiple hops to a destination.

   The **Available ACLs** table displays the available IPv4 and IPv6 ACLs on this product. IPv4 and IPv6 have two separate policy lists. IPv4 PBR rules can only have IPv4 ACLs and IPv4 addresses in the next hop. IPv6 PBR rules can have can have IPv4 and IPv6 ACLs and IPv4 and IPv6 addresses in the next hop.

   The **Available ACLs** table includes the following information:

   - ACL Name — Name of the ACL.
   - IP Version — Whether the ACL is IPv4 or IPv6.

   You can create or edit an ACL by clicking **Launch L3 ACL Editor**. For more information, refer to "Layer 3 access control list policy" on page 580

5. Click the right arrow button to move the selected ACLs to the **Match ACLs** table.

   The **Match ACLs** table identifies which ACL policies this rule uses.

   If you select an ACL that is in an orphan state (ACL deleted, never created, creation scheduled for later date, or creation failed), the PBR configuration is still valid, but is treated as "deny any".

6. Rearrange the order of the ACLs in the **Match ACLs** table by selecting an ACL and using the **Up** or **Down** buttons.

7. Select the packet destination for the ACL filter in the **Enter Next Hop** area by selecting one of the following options from the **Next Hop** list:

   - **Interface** (default) — Port or LAG. Go to step step 8.
   - **IP** (IPv4 or IPv6) — IP address. Go to step step 9.
   - **Flood VLAN** — VLAN identifier. Go to step step 10.

8. Enter the port or LAG interface in slot/port format in the field. Go to step step 12.

9. Enter the IP address in IPv4 or IPv6 format in the field. Go to step step 11.

10. Enter the VLAN identifier in the field. Go to step step 11.

11. Keep the VLAN tag in the packets by selecting the **VLANs Preserve** check box.

12. Validate your entry and move the data to the **Next Hops** table by clicking the right arrow button.

    You can edit an existing hop by selecting the hop from the **Next Hops** table and clicking the left arrow button.

13. Repeat step 7 through step 12 for each hop you want to add to the rule.

14. Rearrange the order of the hops in the **Next Hops** table by selecting a hop and using the **Up** or **Down** buttons.

15. Click **OK** on the **Add Rule** - *Policy_Name* dialog box.

16. Click **OK** on the *Product_Name* **PBR Configuration** dialog box.

    The **Deploy to Products - PBR** dialog box displays. To deploy the PBR policy, refer to "Deploying a PBR policy on demand" on page 553, "Saving a PBR policy deployment" on page 554, or "Scheduling a PBR policy deployment" on page 555.

Adding policies from saved configurations

1. Select an Ethernet router, Ethernet core router, or Ehternet Backbone router product and select **Configure > Policy Based Routing**.

   The *Product_Name* **PBR Configuration** dialog box displays.

2. Select **Add** > **From Saved Configurations**.

   The **PBR Saved Configurations** dialog box displays.

3. Select the configuration you want to add from the list and click **OK**.

4. Click **OK** on the *Product_Name* **PBR Configuration** dialog box.

   The **Deploy to Products - PBR** dialog box displays. To deploy the PBR policy, refer to "Deploying a PBR policy on demand" on page 553, "Saving a PBR policy deployment" on page 554, or "Scheduling a PBR policy deployment" on page 555.

Editing a policy

1. Select an Ethernet router, Ethernet core router, or Ehternet Backbone router product and select **Configure > Policy Based Routing**.

   The *Product_Name* **PBR Configuration** dialog box displays.

2. Select a policy in the **Policy and Rules** table and click **Edit**.

   The **PBR Policy Configuration** dialog box displays.

3. Enter a name for the policy and click **OK**.

4. To add one or more rules to the policy, refer to "Adding rules to a policy" on page 550.

5. To edit a rule in the policy, refer to "Editing a rule" on page 552.

6. To delete a rule in the policy, refer to "Deleting a policy or rule" on page 553.

7. Click **OK** on the *Product_Name* **PBR Configuration** dialog box.

   The **Deploy to Products - PBR** dialog box displays. To deploy the PBR policy, refer to "Deploying a PBR policy on demand" on page 553, "Saving a PBR policy deployment" on page 554, or "Scheduling a PBR policy deployment" on page 555.

Editing a rule

1. Select an Ethernet router, Ethernet core router, or Ehternet Backbone router product and select **Configure > Policy Based Routing**.

   The *Product_Name* **PBR Configuration** dialog box displays.

2. Select a rule in the **Policy and Rules** table and click **Edit**.

   The **Edit Rule** - *Rule_Name* dialog box displays.

3. To edit the rule to the policy, refer to step 4 through step 14 in "Adding rules to a policy" on page 550.

4. Click **OK** on the **Edit Rule** - *Policy_Name* dialog box.

5. Click **OK** on the *Product_Name* **PBR Configuration** dialog box.

The **Deploy to Products - PBR** dialog box displays. To deploy the PBR policy, refer to "Deploying a PBR policy on demand" on page 553, "Saving a PBR policy deployment" on page 554, or "Scheduling a PBR policy deployment" on page 555.

Deleting a policy or rule

1. Select an Ethernet router, Ethernet core router, or Ehternet Backbone router product and select **Configure > Policy Based Routing**.

   The *Product_Name* **PBR Configuration** dialog box displays.

2. Select the policy or rule you want to delete in the **Policy and Rules** table and click **Delete**.

   A confirmation message displays. Click **Yes** to delete the selected rule or the selected policy and all associated rules.

3. Click **OK** on the *Product_Name* **PBR Configuration** dialog box.

   The **Deploy to Products - PBR** dialog box displays. To deploy the PBR policy, refer to "Deploying a PBR policy on demand" on page 553, "Saving a PBR policy deployment" on page 554, or "Scheduling a PBR policy deployment" on page 555.

Deploying a PBR policy on demand

To deploy a PBR policy immediately, complete the following steps.

1. Choose one of the following options:
   - **Deploy now** — Select to deploy the configuration immediately on the product or port without saving the deployment definition.
   - **Save and deploy now** — Select to deploy the configuration immediately on the product or port and save the deployment definition for future deployment.
2. Select one of the following save configuration options:
   - **Save to running** — Select to update the running configuration; however, the deployment is not saved to the product's flash memory.
   - **Save to running and startup** — Select to update the running configuration as well as save the deployment configuration to the product's flash memory. Selecting this option is the equivalent to a write memory command on the product CLI.
   - **Save to running and startup then reboot** — Select to update the running configuration, save the deployment configuration to the product's flash memory, and reboot the product. Selecting this option is the equivalent to entering a write memory and a reload command on the product CLI.
3. Enter a name for the deployment in the **Name** field.
4. Enter a description for the deployment in the **Description** field.
5. Click the **Snapshot Use** check box and click the ellipsis button to select the product monitoring template.

   NOTE
   The **Snapshot Use** check box is only available for IronWare products.

   The **Pre-Post Snapshot Properties** dialog box displays.

6. Select the product monitoring template you want to use from the **CLI Template** list.
7. Select one or more of the following to capture snapshots:
   - Select the **Pre-deployment** check box to capture a snapshot of the product's configuration prior to deployment of the security configuration.
   - Select the **Post-deployment** check box to capture a snapshot of the product's configuration after deployment of the security configuration.

     If you select the **Post-deployment** check box, enter the amount of time (between 1 and 300 seconds) you want the application to wait before capturing the snapshot in the **Delay** field.
8. Select one or more products to which you want to deploy the configuration in the **Available Targets** list and click the right arrow button to move them to the **Selected Targets** list.
9. Click **OK** on the **Deploy to Products - PBR** dialog box.

Saving a PBR policy deployment

To save a PBR policy deployment definition for future deployment, complete the following steps.

1. Select **Save deployment only**.
2. Select one of the following save configuration options:
   - **Save to running** — Select to update the running configuration; however, the deployment is not saved to the product's flash memory.
   - **Save to running and startup** — Select to update the running configuration as well as save the deployment configuration to the product's flash memory. Selecting this option is the equivalent to a write memory command on the product CLI.
   - **Save to running and startup then reboot** — Select to update the running configuration, save the deployment configuration to the product's flash memory, and reboot the product. Selecting this option is the equivalent to entering a write memory and a reload command on the product CLI.
3. Enter a name for the deployment in the **Name** field.
4. Enter a description for the deployment in the **Description** field.
5. Click the **Snapshot Use** check box and click the ellipsis button to select the product monitoring template.

   NOTE
   The **Snapshot Use** check box is only available for IronWare products.

   The **Pre-Post Snapshot Properties** dialog box displays.
6. Select the product monitoring template you want to use from the **CLI Template** list.

7. Select one or more of the following to capture snapshots:
    - Select the **Pre-deployment** check box to capture a snapshot of the product's configuration prior to deployment of the security configuration.
    - Select the **Post-deployment** check box to capture a snapshot of the product's configuration after deployment of the security configuration.

      If you select the **Post-deployment** check box, enter the amount of time (between 1 and 300 seconds) you want the application to wait before capturing the snapshot in the **Delay** field.
8. Select one or more products to which you want to deploy the configuration in the **Available Targets** list and click the right arrow button to move them to the **Selected Targets** list.
9. Click **OK** on the **Deploy to Products - PBR** dialog box.

Scheduling a PBR policy deployment

To schedule a PBR policy deployment, complete the following steps.

1. Select **Schedule**.
2. Select one of the following save configuration options:
    - **Save to running** — Select to update the running configuration; however, the deployment is not saved to the product's flash memory.
    - **Save to running and startup** — Select to update the running configuration as well as save the deployment configuration to the product's flash memory. Selecting this option is the equivalent to a write memory command on the product CLI.
    - **Save to running and startup then reboot** — Select to update the running configuration, save the deployment configuration to the product's flash memory, and reboot the product. Selecting this option is the equivalent to entering a write memory and a reload command on the product CLI.
3. Enter a name for the deployment in the **Name** field.
4. Enter a description for the deployment in the **Description** field.
5. Click the **Schedule Enable** check box and click the ellipsis button to schedule deployment.

   The **Schedule Properties** dialog box displays.
6. Choose one of the following options to configure the frequency at which deployment runs for the schedule:
    - To configure deployment to run only once, refer to "Configuring a one-time deployment schedule" on page 556.
    - To configure hourly deployment, refer to "Configuring an hourly deployment schedule" on page 556.
    - To configure daily deployment, refer to "Configuring a daily deployment schedule" on page 557.
    - To configure weekly deployment, refer to "Configuring a weekly deployment schedule" on page 557.
    - To configure monthly deployment, refer to "Configuring a monthly deployment schedule" on page 557.

7. Click **OK** on the **Schedule Properties** dialog box.
8. Click the **Snapshot Use** check box and click the ellipsis button to select the product monitoring template.

   NOTE
   The **Snapshot Use** check box is only available for IronWare products.

   The **Pre-Post Snapshot Properties** dialog box displays.
9. Select the product monitoring template you want to use from the **CLI Template** list.
10. Select one or more of the following to capture snapshots:
    - Select the **Pre-deployment** check box to capture a snapshot of the product's configuration prior to deployment of the security configuration.
    - Select the **Post-deployment** check box to capture a snapshot of the product's configuration after deployment of the security configuration.

      If you select the **Post-deployment** check box, enter the amount of time (between 1 and 300 seconds) you want the application to wait before capturing the snapshot in the **Delay** field.
11. Select one or more products to which you want to deploy the configuration in the **Available Targets** list and click the right arrow button to move them to the **Selected Targets** list.
12. Click **OK** on the **Deploy to Products - PBR** dialog box.

Configuring a one-time deployment schedule

To configure a one-time schedule, complete the following steps.

1. Select **One Time** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
3. Click the **Date** list to select a date from the calendar.

   To finish configuring the deployment schedule, return to one of the following procedures:

   To finish configuring the deployment schedule, return to step 7 of "Scheduling a PBR policy deployment" on page 555.

Configuring an hourly deployment schedule

To configure an hourly schedule, complete the following steps.

1. Select **Hourly** from the **Frequency** list.
2. Select the minute past the hour you want deployment to run from the **Minutes past the hour** list.

   Where the minute value is from 00 through 59.

   To finish configuring the deployment schedule, return to step 7 of "Scheduling a PBR policy deployment" on page 555.

Configuring a daily deployment schedule

To configure a daily deployment schedule, complete the following steps.

1. Select **Daily** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

   To finish configuring the deployment schedule, return to step 7 of "Scheduling a PBR policy deployment" on page 555.

Configuring a weekly deployment schedule

To configure a weekly schedule, complete the following steps.

1. Select **Weekly** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Select the day you want deployment to run from the **Day of the Week** list.

   To finish configuring the deployment schedule, return to step 7 of "Scheduling a PBR policy deployment" on page 555.

Configuring a monthly deployment schedule

To configure a monthly schedule, complete the following steps.

1. Select **Monthly** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Select the day you want deployment to run from the **Day of the Month** list (1 through 31).

   To finish configuring the deployment schedule, return to step 7 of "Scheduling a PBR policy deployment" on page 555.

ACL Accounting

NOTE
ACL accounting is only supported on Ethernet router, Ethernet core router, or Ehternet Backbone router products running 5.4 or later.

Ethernet router, Ethernet core router, or Ehternet Backbone router products monitor the number of times an ACL is used to filter incoming or outgoing traffic on an interface. When ACL rules are configured, ACL accounting enables you to perform the following functions:

- Diagnostics — Track the number of hits to the ACL rule by the flowing packets going to the destination IP, Flood VLAN, Port, or LAG. This enables you to determine if the configured ACL rules are working correctly.
- Traffic Pattern — Track the number of hit transmit and receive statistics flowing from a particular source to the destination. This enables you to determine if the traffic is as expected or if it needs to be reconfigured.
- On demand statistics collection — Filter data from the product based on a counter (1 second, 1 minute, 5 minutes, and cumulative).
- Multiple port hit statistics — Aggregate statistics for multiple ports based on filtered ports and selected counter.

Enabling or disabling ACL accounting

1. Select an Ethernet router, Ethernet core router, or Ehternet Backbone router product and select **Configure > Security > ACL Accounting.**

   The **ACL Accounting** dialog box displays and obtains the ACL accounting status from product.

   If ACL accounting is enabled, the **Disabled** option is selected.

   If ACL accounting is disabled, the **Enabled** option is selected.

2. Click **OK** on the **ACL Accounting** dialog box.

Resetting ACL counters

NOTE
Counters are automatically cleared when you reboot the product.

Counters, which are stored in the hardware, track of the number of times an ACL filter is used. ACL accounting counters include:

- 1 second — Number of hits during the last second. This counter is updated every second.
- 1 minute — Number of hits during the last minute. This counter is updated every minute.
- 5 minutes — Number of hits during the last five minutes. This counter is updated five minutes.
- Cumulative — Total number of accumulated hits. This counter begins when an ACL is bound to an interface and is updated every minute until it is cleared.

1. Select an Ethernet router, Ethernet core router, or Ehternet Backbone router product and select **Configure > Security > ACL Accounting.**

   The **ACL Accounting** dialog box displays.

2. Select the **Clear all counters on device** check box.
3. Click **OK** on the **ACL Accounting** dialog box.

Viewing ACL counters

Before you can view ACL counters, you must enable ACL accounting on the product (refer to "Enabling or disabling ACL accounting" on page 558).

To view ACL accounting on a product, select an Ethernet router, Ethernet core router, or Ehternet Backbone router product and select **Configure > Security > Layer 2/3 ACL > Product**.

The *Product_Name* - **Layer 2/3 ACL Configuration** dialog box displays. Go to step 4.

OR

To view ACL accounting on a port, complete the following steps.

1. Select an Ethernet router, Ethernet core router, or Ehternet Backbone router product and select **Configure > Security > Layer 2/3 ACL > Port**.

   The **Port Selection** - **Layer 2/3 ACL** dialog box displays.
2. Select a port in the **Available Ports** list and click the right arrow button.
3. Click **OK** on the **Port Selection** - **Layer 2/3 ACL** dialog box.

   The *Product_Name - Port_Number* - **Layer 2/3 ACL Configuration** dialog box displays.
4. Select a duration (1 second, 1 minute, 5 minutes, or Cumulative) from the **Hit Stats Duration** list.
5. Click **Refresh**.

   The last time (client time) the Management application client successfully collected the hit statistics displays in the **Refresh Time** field.

   The number of hits for the ACL displays in the **Hits** column of the **Details of Selected ACL** list.

   (Products level only) Ports that have the selected ACL bound display in the **Assigned Ports** list.
6. Click Cancel on the *Product_Name* - **Layer 2/3 ACL Configuration** dialog box or *Product_Name - Port_Number* - **Layer 2/3 ACL Configuration** dialog box.

Chapter

18

Security Management

In this chapter

Security overview

Security management enables you to filter traffic using Layer 2 and Layer 3 access control lists (ACLs) and Media Access Control (MAC) filters:

- Access control lists enable you to filter traffic based on Layer 2 or Layer 3 information in the packet header of the Ethernet frame.
  - Layer 2, the data link layer, transfers data between the source and destination within the same network.
  - Layer 3, the network layer, transfers data between the source and destination through one or more networks.
- MAC Filters enable you to filter traffic based on the MAC layer header in the Ethernet frame.

Layer 2 access control list management

A Layer 2 access control list (ACL) enables you to filter traffic based on the information in the IP packet header using the MAC address and Ethernet type.

NOTE
Layer 2 ACLs can filter traffic for both Fabric OS and IronWare FCoE devices.

An ACL is a unique collection of permit and deny statements (rules) that apply to frames. You can use ACLs to permit or deny incoming frames from passing through an interface to which you assigned the ACLs. When the interface receives the frame, the device compares the fields in the frame against any ACLs assigned to the interface to verify that the frame has the required permissions to be forwarded. The device compares the frame, sequentially, against each rule in the assigned ACL. If the frame matches the permit rule, the traffic is forwarded; otherwise, the traffic is dropped.

You should configure the ACL on the device before you assign the ACL to an interface. You can create multiple ACLs and save them to the device configuration. However, the ACL does not filter traffic until you assign it to an interface. You can assign an ACL on a physical port, Virtual LAN (VLAN), or Link Aggregation Group (LAG).

For IronWare OS products, you can create a standard ACL. For Fabric OS devices, you can create two types of ACLs:

- Standard ACL — Use to permit and deny traffic based on the source MAC address of incoming frames. You should use standard ACLs when you only need to filter traffic based on the source address.
- Extended ACL — Use to permit and deny traffic based on the source and destination MAC addresses and EtherType, of incoming frames.

IronWare Layer 2 ACL configuration

This section provides procedures for configuring a standard or extended Layer 2 ACL on a device, assigning the Layer 2 ACL to an interface, and clearing Layer 2 ACL assignments from a device.

Creating a Layer 2 ACL configuration (IronWare)

To create a Layer 2 ACL configuration, complete the following steps.

1. Select a device and select **Configure > Security > Layer 2 ACL > Product**.

   The *Device_Name* - **Layer 2 ACL Configuration** dialog box displays.

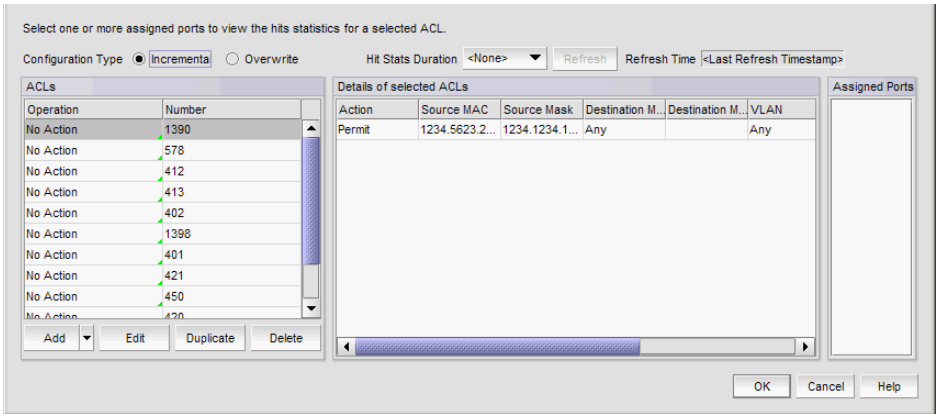


FIGURE 205 *Device_Name* - Layer 2 ACL Configuration dialog box

2. Select **New** from the **Add** list.

   The **Add - Layer 2 ACL Configuration** dialog box displays.

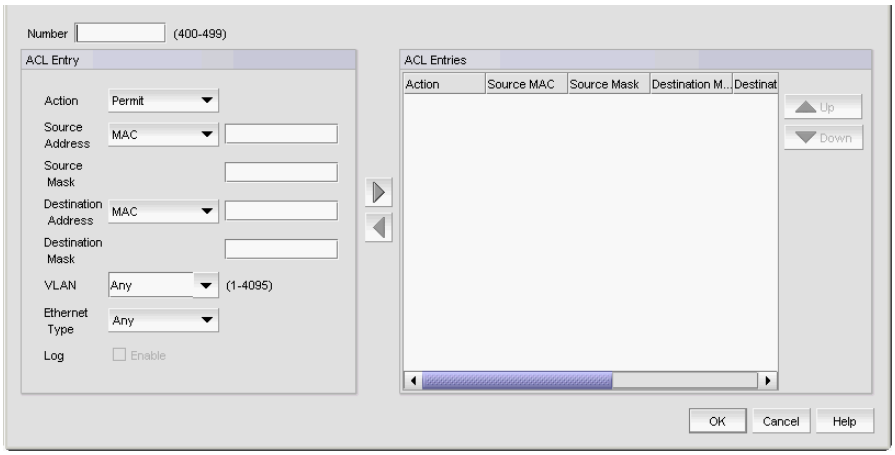


FIGURE 206 Add - Layer 2 ACL Configuration dialog box

3. Enter a number for the ACL in the **Number** field.

   For IronWare 5.4 and later, ACL numbers range from 400 through 1399.

   For IronWare 5.3, ACL numbers range from 400 through 599.

   For IronWare less than 5.3, ACL numbers range from 400 through 499.

4. Select **Permit** or **Deny** from the **Action** list.
5. In the **Source Address** list, select one of the following options:
   - Any
   - MAC

     Selecting **MAC** enables the **Source Address** and **Source Mask** fields.

     a. Enter the source MAC address on which the configuration filters traffic in the **Source Address** field.

     b. Enter the mask associated with the source MAC address in the **Source Mask** field.
6. In the **Destination Address** list, select one of the following options:
   - Any
   - MAC

     Selecting **MAC** enables the **Destination Address** and **Destination Mask** fields.

     a. Enter the destination MAC address on which the configuration filters traffic in the **Destination Address** field.

     b. Enter the mask associated with the destination MAC address in the **Destination Mask** field.
7. Enter a specific VLAN ID or select **Any** from the **VLAN** list.
8. In the **Ethernet Type** list, select one of the following options to specify the Ethernet type being transferred in the Ethernet frame:
   - **ARP** — Address Resolution Protocol
   - **IPV4-L5** — Internet Protocol, version 4-L5
   - **IPV6** — Internet Protocol, version 6

- **Any** — Any of the protocols

9. (Deny actions only) Select the **Log Enable** check box to generate a log for this configuration.
10. Click the right arrow button.

    The new ACL rule displays in the **ACL Entries** list.
11. To create additional rules for the same ACL, repeat step 4 through step 10.
12. Click **OK** on the **Add - Layer 2 ACL Configuration** dialog box.

    The new ACL rule displays in the **ACLs** list. To create additional ACL, repeat step 2 through step 12.
13. Click **OK** on the *Device_Name* - **Layer 2 ACL Configuration** dialog box.

    The **Deploy to Products - Layer 2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 631.

Editing a Layer 2 ACL configuration (IronWare)

To edit a Layer 2 ACL configuration, complete the following steps.

1. Select the device and select **Configure > Security > Layer 2 ACL > Product**.

    The *Device_Name* - **Layer 2 ACL Configuration** dialog box displays.
2. Select the ACL configuration you want to edit and click **Edit**.

    The *ACL_Number* - **Edit Layer 2 ACL Configuration** dialog box displays.
3. Change the description of the ACL in the **Description** field.
4. To edit an existing ACL rule, complete the following steps.
    a. Select the ACL rule you want to edit in the **ACL Entries** list and click the left arrow button.
    b. Complete step 4 through step 10 in "Creating a Layer 2 ACL configuration (IronWare)" on page 562.

        The updated ACL rule displays in the **ACL Entries** list. To update additional rules for the same ACL, repeat step 4.
5. To add a new ACL rule, complete step 4 through step 10 in "Creating a Layer 2 ACL configuration (IronWare)" on page 562.

    The new ACL rule displays in the **ACL Entries** list. To create additional ACL rules, repeat step 4 through step 10.
6. To delete an ACL rule, select the rule in the **ACL Entries** list and click the left arrow button.
7. Click **OK** on the *ACL_Number* - **Edit Layer 2 ACL Configuration** dialog box.
8. Click **OK** on the *Device_Name* - **Layer 2 ACL Configuration** dialog box.

    The **Deploy to Products - Layer 2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 631.

Copying a Layer 2 ACL configuration (IronWare)

To copy a Layer 2 ACL configuration, complete the following steps.

1. Select a device and select **Configure > Security > Layer 2 ACL > Product**.

   The *Device_Name* - **Layer 2 ACL Configuration** dialog box displays.

2. Select the ACL configuration you want to copy and click **Duplicate**.

   The **Duplicate - Layer 2 ACL Configuration** dialog box displays.

3. Enter a number for the ACL in the **Number** field.

   For IronWare 5.4 and later, ACL numbers range from 400 through 1399.

   For IronWare 5.3, ACL numbers range from 400 through 599.

   For IronWare less than 5.3, ACL numbers range from 400 through 499.

4. Enter a description of the ACL in the **Description** field.

5. To edit an existing ACL rule, complete the following steps.

   a. Select the ACL rule you want to edit in the **ACL Entries** list and click the left arrow button.

   b. Complete step 4 through step 10 in "Creating a Layer 2 ACL configuration (IronWare)" on page 562.

      The updated ACL rule displays in the **ACL Entries** list. To update additional rules for the same ACL, repeat step 5.

6. To add a new ACL rule, complete step 4 through step 10 in "Creating a Layer 2 ACL configuration (IronWare)" on page 562.

   The new ACL rule displays in the **ACL Entries** list. To create additional ACL rules, repeat step 4 through step 10.

7. To delete an ACL rule, select the rule in the **ACL Entries** list and click the left arrow button.

8. Click **OK** on the **Duplicate - Layer 2 ACL Configuration** dialog box.

9. Click **OK** on the *Device_Name* - **Layer 2 ACL Configuration** dialog box.

   The **Deploy to Products - Layer 2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 631.

Assigning a Layer 2 ACL configuration to an interface (IronWare)

NOTE
You cannot modify or delete a Layer 2 ACL that is bound to a port.

To assign a Layer 2 ACL configuration to an interface, complete the following steps.

1. Select **Configure > Security > Layer 2 ACL > Port**.

   The **Port Selection - Layer 2 ACL** dialog box displays.

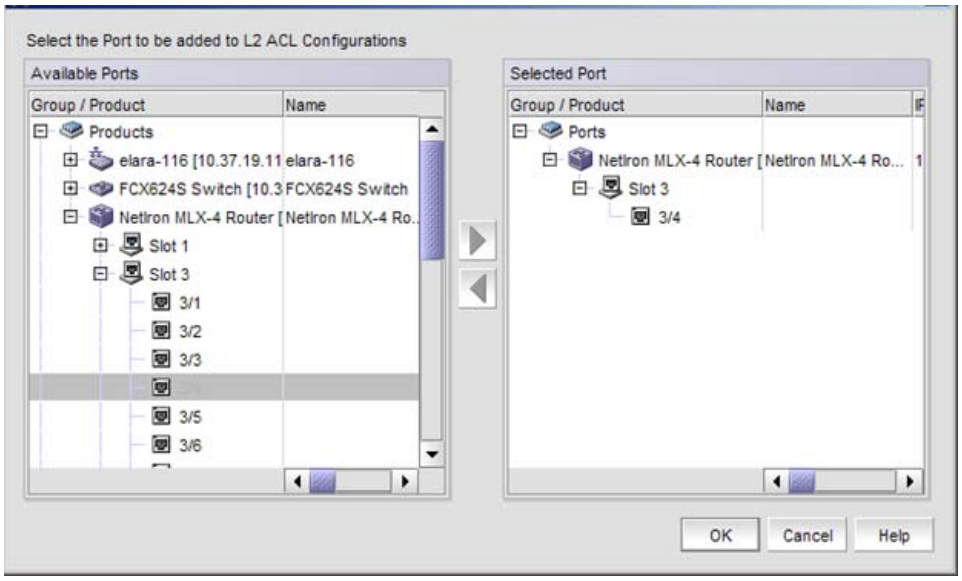


FIGURE 207 Port Selection - Layer 2 ACL dialog box

2. Select a port in the **Available Ports** list and click the right arrow button.
3. Click **OK**.

   The *Device_Name* - *Port_Number* - **Layer 2 ACL Configuration** dialog box displays.

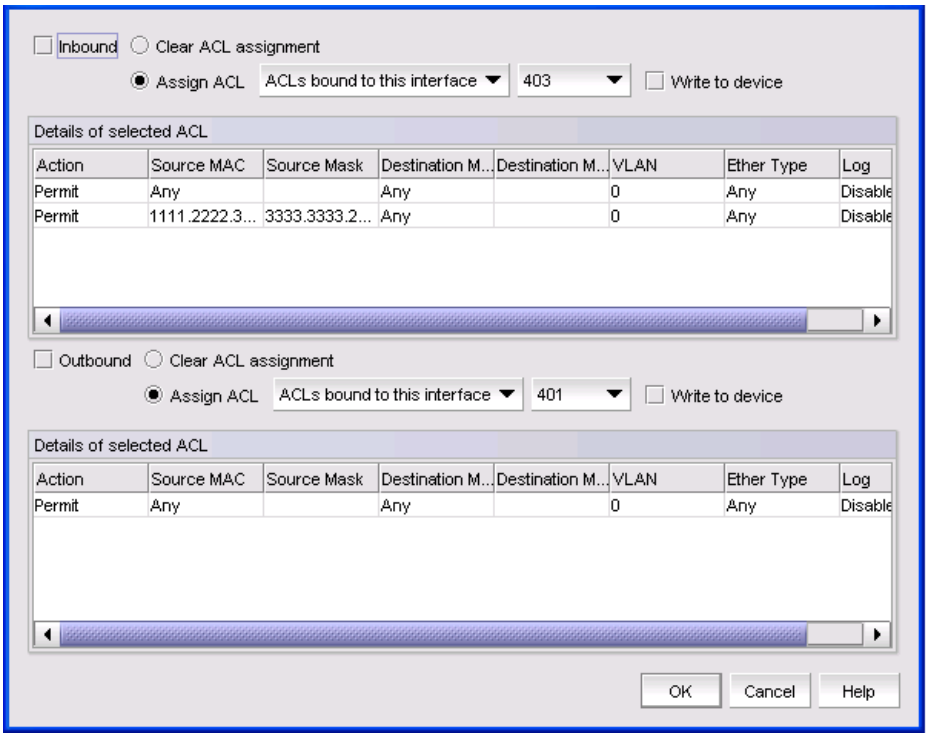


FIGURE 208 *Device_Name - Port_Number* - **Layer 2 ACL Configuration dialog box**

4. (Ethernet routers only) Select a duration (1 Second, 1 Minute, 5 Minutes, or Cumulative) to track the number of times an ACL filter is used in the **Hits Stats Duration** list.

   Click **Refresh** to collect the hit statistics. The application updates the **Hits** column of the **Details of Selected ACL** list.

5. To assign an ACL configuration to inbound messages, select the **Inbound** check box and complete the following steps:

   a. Select the **Assign ACL** option and choose one of the following options from the first **Assign ACL** list:

      - Select **ACLs on this Product** to assign ACLs deployed on the product to the port. The second list is populated with the ACLs deployed on the switch or associated with a save deployment object.
      - Select **ACLs bound to this port** to assign ACLs bound to the interface to the port. The second list is populated with the ACLs bound to the interface.
      - *Deployment_Name* — Select to assign a user-configured deployment on the port.

   b. Select the ACL you want to assign to the port from the second **Assign ACL** list.

   c. Select the **Write to Product** check box to create the selected ACL on the device if it does not already exist.

6. To assign an ACL configuration to outbound messages, select the **Outbound** check box and complete the following steps:

   NOTE
   You can only assign an ACL to an outbound message on an Application product.

   a. Select the **Assign ACL** option and choose one of the following options from the first **Assign ACL** list:

      - Select **ACLs on this Product** to assign ACLs deployed on the product to the port. The second list is populated with the ACLs deployed on the switch or associated with a save deployment object.
      - Select **ACLs bound to this port** to assign ACLs bound to the interface to the port. The second list is populated with the ACLs bound to the interface.
      - *Deployment_Name* — Select to assign a user-configured deployment on the port.

   b. Select the ACL you want to assign to the port from the second **Assign ACL** list.

   c. Select the **Write to Product** check box to create the selected ACL on the device if it does not already exist.

7. Click **OK** on the *Device_Name* - *Port_Number* - **Layer 2 ACL Configuration** dialog box.

   The **Deploy to Ports - Layer 2 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Clearing Layer 2 ACL assignments (IronWare)

To clear Layer 2 ACL configuration from interfaces, complete the following steps.

1. Select **Configure > Security > Layer 2 ACL > Port**.

   The **Port Selection - Layer 2 ACL** dialog box displays.

2. Select a port in the **Available Ports** list and click the right arrow button.

3. Click **OK**.

   The *Device_Name* - *Port_Number* - **Layer 2 ACL Configuration** dialog box displays.

4. To clear inbound messages, complete the following steps:

   a. Select the **Inbound** check box.

   b. Select the **Clear ACL Assignment** option.

5. To clear outbound messages, complete the following steps:

   a. Select the **Outbound** check box.

   b. Select the **Clear ACL Assignment** option.

6. Click **OK** on the *Device_Name* - *Port_Number* - **Layer 2 ACL Configuration** dialog box.

   The **Deploy to Ports - Layer 2 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Fabric OS Layer 2 ACL configuration

NOTE
Only available for Fabric OS DCB products.

This section provides procedures for configuring a standard for extended Layer 2 ACL on a device, assigning the Layer 2 ACL to an interface, as well as clearing Layer 2 ACL assignments from a device.

Creating a standard Layer 2 ACL configuration (Fabric OS)

To create a standard Layer 2 ACL configuration, complete the following steps.

1. Select the device and select **Configure > Security > Layer 2 ACL > Product**.

   The *Device_Name* - **Layer 2 ACL Configuration** dialog box displays.

2. Select **New** from the **Add** list.

   The *Device_Name* - **Layer 2 ACL Configuration** dialog box displays.

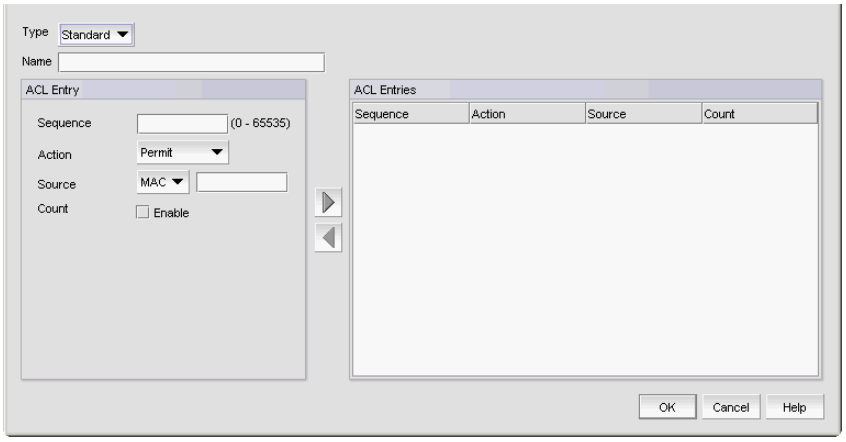


FIGURE 209 *Device_Name* - Layer 2 ACL Configuration (Standard) dialog box

3. Select **Standard** from the **Type** list.
4. Enter a name for the ACL in the **Name** field.
5. Enter a sequence number for the ACL in the **Sequence** field.
6. Select **Permit** or **Deny** from the Action list.
7. In the **Source** list, select one of the following options:
   - Any
   - MAC

     Selecting MAC enables the **Source** field. Enter the source MAC address on which the configuration filters traffic in the **Source** field.
8. Select the **Count** check box to enable counting.

   Count specifies the number of times the ACL rule is applied.
9. Click the right arrow button.

The new ACL entry displays in the **ACL Entries** list. To create additional ACL entries, repeat step 3 through step 9.

10. Click **OK** on the **Add - Layer 2 ACL Configuration** dialog box.

    The new ACL configuration displays in the **ACLs** list. To create additional ACLs, repeat step 2 through step 10.

11. Click **OK** on the *Device_Name* - **Layer 2 ACL Configuration** dialog box.

    The **Deploy to Products - Layer 2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 631

Editing a standard Layer 2 ACL configuration (Fabric OS)

To create a standard Layer 2 ACL configuration on a Fabric OS device, complete the following steps.

1. Select the device and select **Configure > Security > Layer 2 ACL > Product**.

   The *Device_Name* - **Layer 2 ACL Configuration** dialog box displays.

2. Select the ACL you want to edit in the **ACLs** list and click **Edit**.

   The *Configuration_Name* **Edit Standard Layer 2 ACL Configuration** dialog box displays.

3. To edit an existing ACL rule, complete the following steps.

   a. Select the rule you want to edit in the **ACL Entries** list and click the left arrow button.

   b. Complete step 5 through step 9 in "Creating a standard Layer 2 ACL configuration (Fabric OS)" on page 569.

      The updated ACL entry displays in the **ACL Entries** list. To edit additional ACL entries, repeat step 3.

4. To add a new ACL rule, complete step 4 through step 9 in "Creating a standard Layer 2 ACL configuration (Fabric OS)" on page 569.

   The new ACL entry displays in the **ACL Entries** list. To add additional ACL entries, repeat step 4.

5. To delete an existing ACL rule, select the rule you want to edit in the **ACL Entries** list and click the left arrow button.

6. Click **OK** on the **Edit - Layer 2 ACL Configuration** dialog box.

   The updated ACL configuration displays in the **ACLs** list. To edit additional ACLs, repeat step 2 through step 4.

7. Click **OK** on the *Device_Name* - **Layer 2 ACL Configuration** dialog box.

   The **Deploy to Products - Layer 2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 631

Copying a standard Layer 2 ACL configuration (Fabric OS)

To copy a standard Layer 2 ACL configuration on a Fabric OS device, complete the following steps.

1. Select the device and select **Configure > Security > Layer 2 ACL > Product**.

   The *Device_Name* - **Layer 2 ACL Configuration** dialog box displays.

2. Select the ACL you want to duplicate in the **ACLs** list and click **Duplicate**.

The **Duplicate - Layer 2 ACL Configuration** dialog box displays with the default name 'Copy of *Original_Name*'.

3. Enter a new name for the ACL in the **Name** field.
4. To edit an existing ACL rule, complete the following steps.
   a. Select the rule you want to edit in the **ACL Entries** list and click the left arrow button.
   b. Complete step 5 through step 9 in "Creating a standard Layer 2 ACL configuration (Fabric OS)" on page 569.

      The updated ACL entry displays in the **ACL Entries** list. To edit additional ACL entries, repeat step 4.
5. To add a new ACL rule, complete step 4 through step 9 in "Creating a standard Layer 2 ACL configuration (Fabric OS)" on page 569.

   The new ACL entry displays in the **ACL Entries** list. To add additional ACL entries, repeat step 5.
6. To delete an existing ACL rule, select the rule you want to edit in the **ACL Entries** list and click the left arrow button.
7. Click **OK** on the **Duplicate - Layer 2 ACL Configuration** dialog box.

   The new ACL configuration displays in the **ACLs** list. To copy additional ACLs, repeat step 2 through step 10.
8. Click **OK** on the *Device_Name* - **Layer 2 ACL Configuration** dialog box.

   The **Deploy to Products - Layer 2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 631

Creating an extended Layer 2 ACL configuration (Fabric OS)

To create an extended Layer 2 ACL configuration on a Fabric OS device, complete the following steps.

1. Select the device and select **Configure > Security > Layer 2 ACL > Product**.

   The *Device_Name* - **Layer 2 ACL Configuration** dialog box displays.
2. Select **New** from the **Add** list.

   The *Device_Name* - **Layer 2 ACL Configuration** dialog box displays.
3. Select **Extended** from the **Type** list.

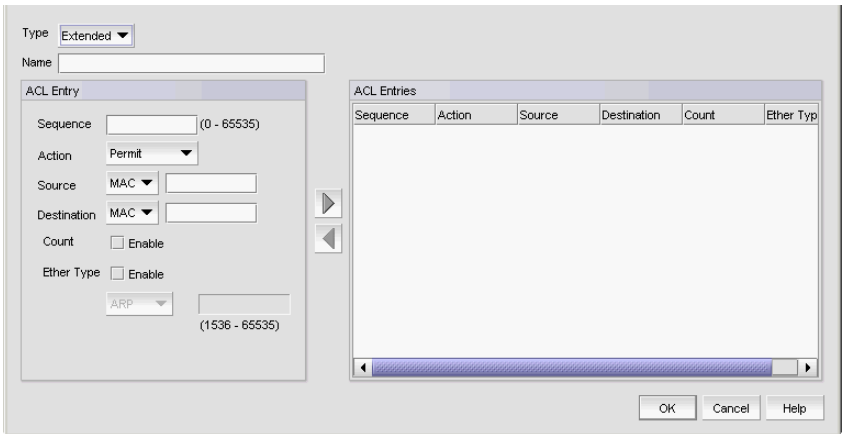


FIGURE 210 *Device_Name* - Layer 2 ACL Configuration (Extended) dialog box

4. Enter a name for the ACL in the **Name** field.
5. Enter a sequence number for the ACL in the **Sequence** field.
6. Select **Permit** or **Deny** from the Action list.
7. In the **Source** list, select one of the following options:
   - Any
   - Host
   - MAC

   Selecting MAC or Host enables the **Source** field. Enter the source address on which the configuration filters traffic in the **Source** field.
8. In the **Destination Address** list, select one of the following options:
   - Any
   - Host
   - MAC

   Selecting MAC or Host enables the **Destination** field. Enter the destination address on which the configuration filters traffic in the **Destination** field.
9. Select the **Count** check box to enable counting.

   Count specifies the number of packets filtered (allowed or denied) for the ACL rule.
10. Select the **Ether Type** check box to specify the Ethernet protocol.
11. In the **Ether Type** list, select one of the following to specify the Ethernet type being transferred in the Ethernet frame:
    - **ARP** — Address Resolution Protocol
    - **FCoE** — Fibre Channel over Ethernet
    - **IPV4**- — Internet Protocol, version 4
    - **Custom** — Enter a custom protocol. Valid values are 1536 through 65535.
12. Click the right arrow button.

The new ACL entry displays in the **ACL Entries** list. To create additional ACL entries, repeat step 5 through step 12.

13. Click **OK** on the **Add - Layer 2 ACL Configuration** dialog box.

    The new ACL displays in the **ACL Entries** list. To create additional ACL entries, repeat step 2 through step 13.

14. Click **OK** on the *Device_Name* - **Layer 2 ACL Configuration** dialog box.

    The **Deploy to Products - Layer 2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 631

Editing an extended Layer 2 ACL configuration (Fabric OS)

To edit an extended Layer 2 ACL configuration on a Fabric OS device, complete the following steps.

1. Select the device and select **Configure > Security > Layer 2 ACL > Product**.

   The *Device_Name* - **Layer 2 ACL Configuration** dialog box displays.

2. Select the ACL you want to edit in the **ACLs** list and click **Edit**.

   The *Configuration_Name* **Edit Extended Layer 2 ACL Configuration** dialog box displays.

3. To edit an existing ACL rule, complete the following steps.

   a. Select the rule you want to edit in the **ACL Entries** list and click the left arrow button.

   b. Complete step 5 through step 12 in "Creating an extended Layer 2 ACL configuration (Fabric OS)" on page 571.

      The updated ACL entry displays in the **ACL Entries** list. To edit additional ACL entries, repeat step 3.

4. To add a new ACL rule, complete step 4 through step 12 in "Creating an extended Layer 2 ACL configuration (Fabric OS)" on page 571.

   The new ACL entry displays in the **ACL Entries** list. To add additional ACL entries, repeat step 4.

5. To delete an existing ACL rule, select the rule you want to edit in the **ACL Entries** list and click the left arrow button.

6. Click **OK** on the **Edit - Layer 2 ACL Configuration** dialog box.

   The updated ACL displays in the **ACL Entries** list. To edit additional ACLs, repeat step 2 through step 6.

7. Click **OK** on the *Device_Name* - **Layer 2 ACL Configuration** dialog box.

   The **Deploy to Products - Layer 2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 631

Copying an extended Layer 2 ACL configuration (Fabric OS)

To copy an extended Layer 2 ACL configuration, complete the following steps.

1. Select the device and select **Configure > Security > Layer 2 ACL > Product**.

   The *Device_Name* - **Layer 2 ACL Configuration** dialog box displays.

2. Select the ACL you want to copy in the **ACLs** list and click **Duplicate**.

The **Duplicate - Layer 2 ACL Configuration** dialog box displays with the default name 'Copy of *Original_Name*'.

3. Enter a new name for the ACL in the **Name** field.
4. To edit an existing ACL rule, complete the following steps.
   a. Select the rule you want to edit in the **ACL Entries** list and click the left arrow button.
   b. Complete step 5 through step 12 in "Creating an extended Layer 2 ACL configuration (Fabric OS)" on page 571.

      The updated ACL entry displays in the **ACL Entries** list. To edit additional ACL entries, repeat step 4.
5. To add a new ACL rule, complete step 4 through step 12 in "Creating an extended Layer 2 ACL configuration (Fabric OS)" on page 571.

   The new ACL entry displays in the **ACL Entries** list. To add additional ACL entries, repeat step 5.
6. To delete an existing ACL rule, select the rule you want to edit in the **ACL Entries** list and click the left arrow button.
7. Click **OK** on the **Duplicate - Layer 2 ACL Configuration** dialog box.

   The new ACL displays in the **ACL Entries** list. To copy additional ACLs, repeat step 2 through step 7.
8. Click **OK** on the *Device_Name* - **Layer 2 ACL Configuration** dialog box.

   The **Deploy to Products - Layer 2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 631

Assigning a Layer 2 ACL configuration to an interface (Fabric OS)

To assign Layer 2 ACL configuration to a interface, complete the following steps.

1. Select **Configure > Security > Layer 2 ACL > Port**.

   The **Port Selection - Layer 2 ACL** dialog box displays.
2. Select a port or Link Aggregation Group (LAG) in the **Available Ports** list and click the right arrow button.

   LAGs display in the **Available Ports** list using the following convention: Po *LAG_Number.*
3. Click **OK**.

The *Device_Name* - *Port_Number*/**LAG** *LAG_Number*- **Layer 2 ACL Configuration** dialog box displays.

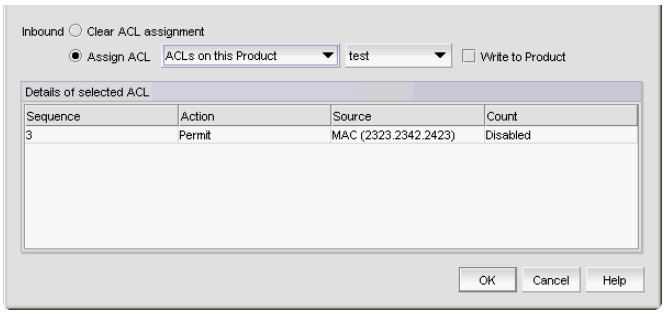


FIGURE 211 *Device_Name - Port_Number*- Layer 2 ACL Configuration dialog box

4. Select the **Assign ACL** option and choose one of the following options from the first **Assign ACL** list:
   - Select **ACLs on this Product** to assign ACLs deployed on the product to the port.

     The second list is populated with the ACLs deployed on the switch or associated with a save deployment object.
   - Select **ACLs bound to this port** to assign ACLs bound to the interface to the port.

     The second list is populated with the ACLs bound to the interface.
   - Select *Deployment_Name* (a user-configured deployment) to assign a user-configured deployment on the port.
5. Select the ACL you want to assign to the port from the second **Assign ACL** list.
6. Select the **Write to Product** check box to create the selected ACL on the device if it does not already exist.
7. Click **OK** on the *Device_Name* - *Port_Number* - **Layer 2 ACL Configuration** dialog box.

   The **Deploy to Ports - Layer 2 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Clearing Layer 2 ACL assignments (Fabric OS)

To clear Layer 2 ACL configuration from interfaces, complete the following steps.

1. Select **Configure > Security > Layer 2 ACL > Port**.

   The **Port Selection - Layer 2 ACL** dialog box displays.
2. Select a port or LAG in the **Available Ports** list and click the right arrow button.

   LAGs display in the **Available Ports** list using the following convention: Po *LAG_Number.*
3. Click **OK**.

   The *Device_Name* - *Port_Number*/**LAG** *LAG_Number* - **Layer 2 ACL Configuration** dialog box displays.
4. Select the **Clear ACL Assignment** option.
5. Click **OK** on the *Device_Name* - *Port_Number*/**LAG** *LAG_Number* - **Layer 2 ACL Configuration** dialog box.

The **Deploy to Ports - Layer 2 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Creating a Layer 2 ACL from a saved configuration

To create a Layer 2 ACL from a saved configuration, complete the following steps.

1. Select the device and select **Configure > Security > Layer 2 ACL > Product**.

   The *Device_Name* - **Layer 2 ACL Configuration** dialog box displays.

2. Select **From Saved Configurations** from the **Add** list.

   The **Layer 2 ACL Saved Configurations** dialog box displays.

3. Select one or more configurations to add to the new Layer 2 ACL configuration.

4. Click **OK** on the **Layer 2 ACL Saved Configurations** dialog box.

   The new ACL displays in the **ACLs** list.

5. Click **OK** on the *Device_Name* - **Layer 2 ACL Configuration** dialog box.

   The **Deploy to Products - Layer 2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 631

Deleting a Layer 2 ACL configuration from the application

To delete a Layer 2 ACL configuration from the application, complete the following steps.

1. Select the device and select **Configure > Security > Layer 2 ACL > Product**.

   The *Device_Name* - **Layer 2 ACL Configuration** dialog box displays.

2. Select the Layer 2 ACL you want to delete in the **ACLs** list and click **Delete**.

   This deletes the Layer 2 ACL configuration from the application.

3. Click **Yes** on the confirmation message.

4. Click **OK** on the *Device_Name* - **Layer 2 ACL Configuration** dialog box.

NOTE
The Layer 2 ACL configuration is not deleted from the switch until you deploy the configuration to the switch.

The **Deploy to Products - Layer 2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 631

Deleting a Layer 2 ACL configuration from the switch

To delete a Layer 2 ACL configuration from the switch, complete the following steps.

1. Select the device and select **Configure > Security > Layer 2 ACL > Product**.

   The *Device_Name* - **Layer 2 ACL Configuration** dialog box displays.

2. Select the **Incremental** option as the configuration type.

3. Select **Delete** from the **Operation** list for the Layer 2 ACL configuration you want to delete.

4. Click **OK** on the *Device_Name* - **Layer 2 ACL Configuration** dialog box.

NOTE
The Layer 2 ACL configuration is not deleted from the switch until you deploy the configuration to the switch.

The **Deploy to Products - Layer 2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 631.

Network OS Layer 2 ACL configuration

NOTE
You cannot configure a Layer 2 ACL using the Management application. You must configure the Layer 2 ACL through the Network OS CLI (refer to the *Network OS Command Reference*).

Once you configure Layer 2 ACLs through the Network OS CLI, you can use the Management application to view Layer 2 ACL configurations for a VCS fabric or standalone device. You can also view the Layer 2 ACL that are bound to an interface (ports, LAGs, vLAGs, VLANs, or ports in profile mode) on the fabric or device.

Viewing Layer 2 ACL configuration on a fabric (Network OS)

To view Layer 2 ACL configurations on a Network OS VCS fabric, complete the following steps.

1. Select the VCS fabric and select **Configure > Security > Layer 2 ACL > Product**.

   The *Fabric_Name* - **Layer 2 ACL Configuration** dialog box displays. Depending on the display label you chose on the **IP** tab, the *Fabric_Name* is the name of the fabric, the IP address of the fabric, or the name and IP address of the fabric.

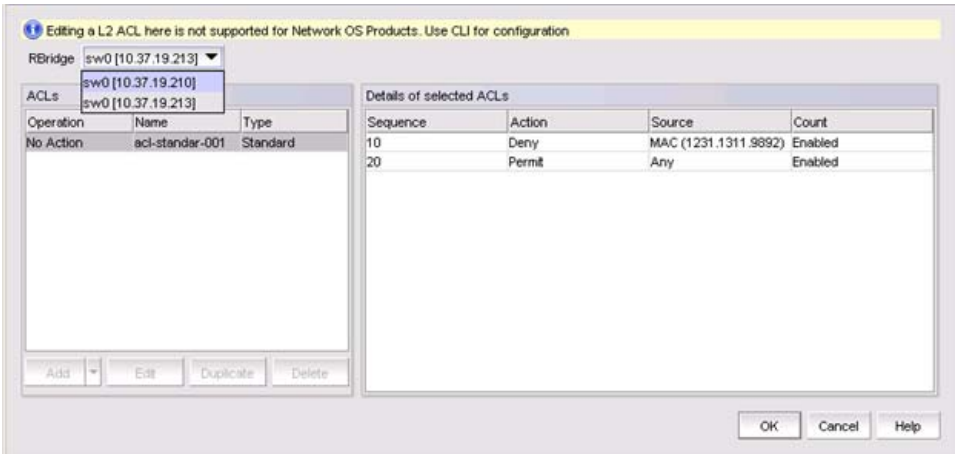


FIGURE 212 *Fabric_Name* - Layer 2 ACL Configuration dialog box

2. Select the fabric node from the **RBridge** list.

   By default, the principal switch of the fabric is selected.

3. Review the Layer 2 ACL configuration details.

- **RBridge** list — Only displays when you select a VCS fabric. Select a node from the fabric.
- **ACLs** list — Displays the ACLs to be deployed for this configuration. The **ACLs** list includes the following details:
  - **Operation —** Displays the ACL operation (no action) during deployment.
  - **Name** — The name of the ACL.
  - **Type** — The ACL type. Options include: Extended or Standard.
- **Details of Selected ACLs** list — Displays the details of the ACL selected in the **ACLs** list. The **Details of Selected ACLs** table includes the following details:
  - **Sequence** — The Layer 2 ACL entry sequence number.
  - **Action** — Whether the ACL permits or denies traffic.
  - **Source —** The source MAC address on which the ACL filters traffic.
  - **Destination** (Extended only) — The destination MAC address on which the ACL filters the traffic.
  - **Count** — Whether count is enabled or disabled.
  - **Ether Type** (Extended only) — The Ethernet protocol. Values include ARP, FCoE, IPv4, or Custom.
- **Add** button — The button appears dimmed because it is unavailable.
- **Edit** button — The button appears dimmed because it is unavailable.
- **Duplicate** button — The button appears dimmed because it is unavailable.
- **Delete** button — The button appears dimmed because it is unavailable.

4. Click **OK** to close on the *Fabric_Name* - **Layer 2 ACL Configuration** dialog box.

Viewing Layer 2 ACL configuration on a device (Network OS)

NOTE
You cannot configure a Layer 2 ACL using the Management application. You must configure the Layer 2 ACL through the Network OS CLI (refer to the *Network OS Command Reference*).

To view Layer 2 ACL configurations on a Network OS standalone device, complete the following steps.

1. Select the device and select **Configure > Security > Layer 2 ACL > Product**.

   The *Device_Name* - **Layer 2 ACL Configuration** dialog box displays. Depending on the display label you choose, the *Device_Name* is the name of the device, the IP address of the device, or the name and IP address of the device.

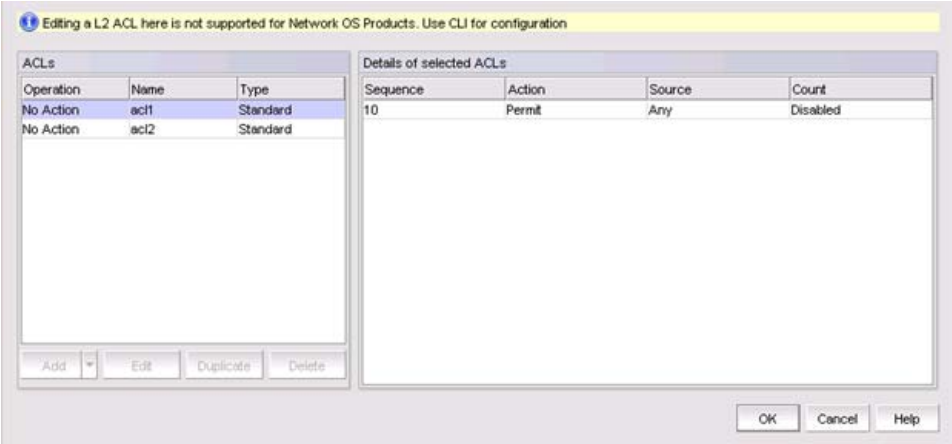


FIGURE 213 *Device_Name* - Layer 2 ACL Configuration dialog box

2. Review the Layer 2 ACL configuration details.

- **ACLs** list — Displays the ACLs to be deployed for this configuration. The **ACLs** list includes the following details:
  - **Operation** — Displays the ACL operation (no action) during deployment.
  - **Name** — The name of the ACL.
  - **Type** — The ACL type. Options include: Extended or Standard.
- **Details of Selected ACLs** list — Displays the details of the ACL selected in the **ACLs** list. The **Details of Selected ACLs** table includes the following details:
  - **Sequence** — The Layer 2 ACL entry sequence number.
  - **Action** — Whether the ACL permits or denies traffic.
  - **Source** — The source MAC address on which the ACL filters traffic.
  - **Destination** (Extended only) — The destination MAC address on which the ACL filters the traffic.
  - **Count** — Whether count is enabled or disabled.
  - **Ether Type** (Extended only) — The Ethernet protocol. Values include ARP, FCoE, IPv4, or Custom.
- **Add** button — Displays; however, is not available.
- **Edit** button — Displays; however, is not available.
- **Duplicate** button — Displays; however, is not available.
- **Delete** button — Displays; however, is not available.

3. Click **OK** to close on the *Device_Name* - **Layer 2 ACL Configuration** dialog box.

Viewing Layer 2 ACL configuration on an interface (Network OS)

NOTE
You cannot configure a Layer 2 ACL using the Management application. You must configure the Layer 2 ACL through the Network OS CLI (refer to the *Network OS Command Reference*).

To view Layer 2 ACL configurations on an interface, complete the following steps.

1. Select the fabric, a node in the fabric, or a standalone device and select **Configure > Security > Layer 2 ACL > Port**.
2. Select a port in the **Available Ports** list and click the right arrow button to move it to the **Selected Port** list.
3. Click **OK** on the **Port Selection - Layer 2 ACL** dialog box.

   The *Device/Fabric_Name* - *Port_Number* - **Layer 2 ACL Configuration** dialog box displays. Depending on the Display Label you choose, the *Device/Fabric_Name* is the name of the device or fabric, the IP address of the device or fabric, or the name and IP address of the device or fabric.

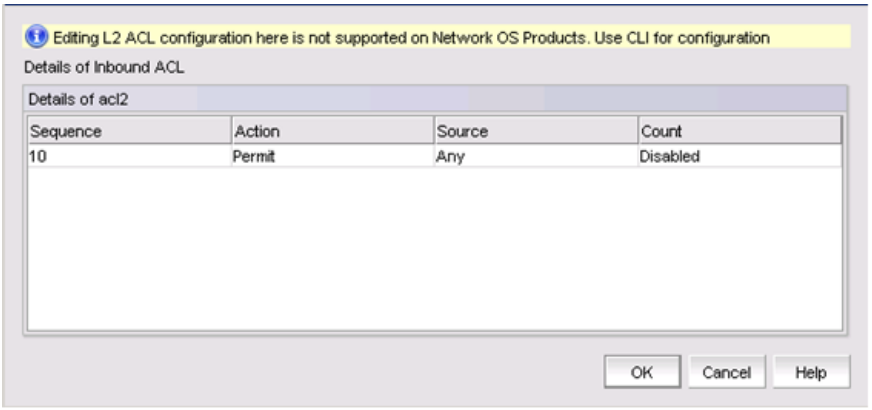


FIGURE 214 *Device/Fabric_Name - Port_Number* - **Layer 2 ACL Configuration dialog box**

4. Review the Layer 2 ACL configuration details.

   Details of Selected ACL table — Displays the details of the ACL selected in the **ACLs** list.The **Details of Selected ACL** table includes the following details:

   - **Sequence** — The Layer 2 ACL entry sequence number.
   - **Action** — Whether the ACL permits or denies traffic.
   - **Source** — The source MAC address on which the ACL filters traffic.
   - **Destination** (Extended only) — The destination MAC address on which the ACL filters the traffic.
   - **Count** — Whether count is enabled or disabled.
   - **Ether Type** (Extended only) — The Ethernet protocol. Values include ARP, FCoE, IPv4, or Custom.

5. Click **OK** to close on the *Device/Fabric_Name* - *Port_Number* - **Layer 2 ACL Configuration** dialog box.

Layer 3 access control list policy

A Layer 3 access control list (L3 ACL) enables you to filter incoming and outgoing traffic based on the information in the IP packet header.

An ACL is a unique collection of permit and deny statements (rules) that apply to frames. You can use ACLs to permit or deny incoming and outgoing frames from passing through an interface to which you assigned the ACLs. When the interface receives the frame, the device compares the fields in the frame against any ACLs assigned to the interface to verify that the frame has the required permissions to be forwarded. The device compares the frame, sequentially, against each rule in the assigned ACL. If the frame matches the 'permit' rule, the traffic is forwarded; otherwise, the traffic is dropped.

You must configure the ACL on the device before you assign the ACL to an interface. You can create multiple ACLs and save them to the device configuration. However, the ACL does not filter traffic until you assign it to an interface. You can assign an ACL on the following interface types: physical port, Virtual LAN (VLAN), or Link Aggregation Group (LAG).

You can create two types of ACLs:

- Standard ACL — Use to permit and deny traffic based on the source IP address, host name, or network. You should use standard ACLs when you only need to filter traffic based the source. You can create up to 99 standard ACLs ranging from 1 through 99. For more information, refer to "Creating a standard L3 ACL configuration" on page 581.
- Extended ACL — Use to permit and deny traffic based on the source and destination using the following:
  - Source and destination IP address
  - Host name
  - User-defined network and network groups
  - IP protocol
  - Source and destination port

  You can create up to 100 extended ACLs ranging from 100 through 199. For more information, refer to "Creating an extended L3 ACL configuration" on page 585.

Creating a standard L3 ACL configuration

To create a standard L3 ACL configuration, complete the following steps.

1. Select the device and select **Configure > Security > L3 ACL > Product**.

   The *Device_Name* - **L3 ACL Configuration** dialog box displays.

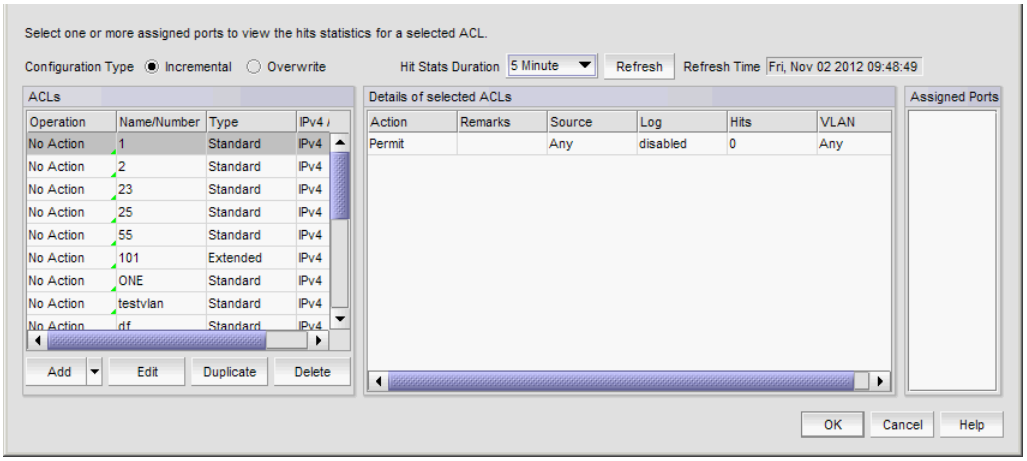


FIGURE 215 *Device_Name* - L3 ACL Configuration dialog box

2. Select **New IPv4** from the **Add** list.

   The **Add - L3 ACL Configuration** dialog box displays.

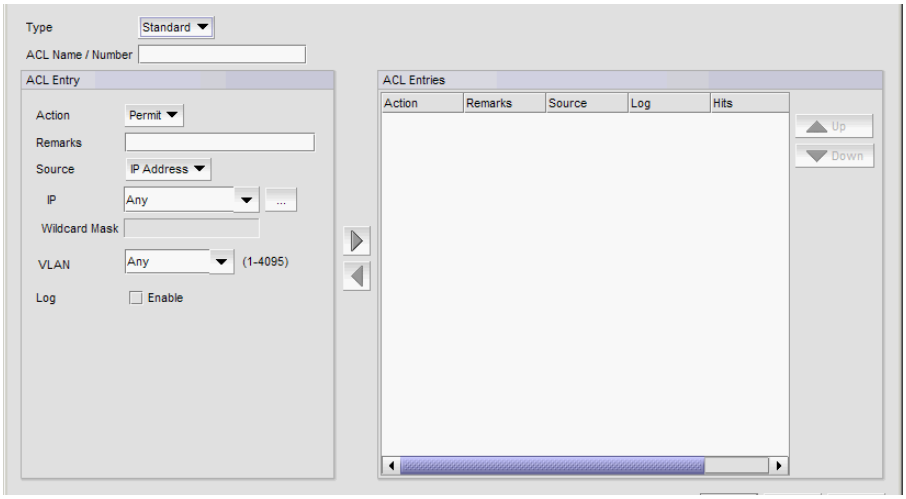


FIGURE 216 Add - L3 ACL Configuration (Standard) dialog box

3. Select **Standard** from the **Type** list.
4. Enter a name or number for the ACL in the **ACL Name/Number** field.
5. Select **Permit** or **Deny** from the **Action** list.
6. Enter a description for the ACL in the **Remarks** field.
7. Choose one of the following options from the **Source** list:

- To enter an IP address, select **IP Address** and complete the following steps:
  a. Enter the source IP address on which the ACL filters traffic in the **IP Address** list and text field.
  b. Enter a portion of the source IP address on which the ACL filters traffic in the **Wildcard Mask field**.
  The wildcard mask is a four-part value in IP address format consisting of ones and zeros. Use zeros in the mask if the packet source address must match the IP address. Use ones if to match any value.
  For example, if you enter '209.157.22.26' in the **IP Address** field and '0.0.0.255' in the **Wildcard Mask** field, then all hosts in the Class C subnet '209.157.22.x' match the ACL.
- To select a network, select **IP Address** and choose a network from the list.
  To configure a network, click the ellipsis button and refer to "Network configuration" on page 602.
- To enter a host name, select **Host** and enter the source host name on which the ACL filters traffic in the **Host** list and text field.

8. Enter a VLAN identifier (valid values are from 1 to 4095) from the **VLAN** list.
9. Select the **Log Enable** check box to enable logging.
10. Click the right arrow button.
11. Use the **Up** and **Down** arrow buttons to rearrange the ACLs in the **ACL Entries** list.
12. Click **OK** on the **Add - L3 ACL Configuration** dialog box.
  The *Device_Name* - **L3 ACL Configuration** dialog box displays.
13. To set the configuration type and operations, refer to "Configuring the ACL configuration type and operations" on page 597.
14. (Ethernet routers only) To set the hit statistics duration, refer to "Configuring hit statistics" on page 597.
15. To deploy the configuration, click **OK** on the *Device_Name* - **L3 ACL Configuration** dialog box.
  The **Deploy to Products - L3 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Creating a L3 ACL from a saved configuration

To create a ACL from a saved configuration, complete the following steps.

1. Select the device and select **Configure > Security > L3 ACL > Product**.
  The *Device_Name* - **L3 ACL Configuration** dialog box displays.
2. Select **From Saved Configurations** from the **Add** list.
  The **L3 ACL Saved Configurations** dialog box displays.
3. Select one or more configurations to add to the new ACL configuration.

4. Click **OK** on the **L3 ACL Saved Configurations** dialog box.

   The new ACL displays in the **ACLs** list.

5. To set the configuration type and operations, refer to "Configuring the ACL configuration type and operations" on page 597.

6. (Ethernet routers only) To set the hit statistics duration, refer to "Configuring hit statistics" on page 597.

7. To deploy the configuration, click **OK** on the *Device_Name* - **L3 ACL Configuration** dialog box.

   The **Deploy to Products - L3 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Editing a standard L3 ACL configuration

To edit a standard L3 ACL configuration, complete the following steps.

1. Select the device and select **Configure > Security > L3 ACL > Product**.

   The *Device_Name* - **L3 ACL Configuration** dialog box displays.

2. Select the standard ACL configuration you want to edit in the **ACLs** list.

3. Click **Edit**.

   The **Edit - L3 ACL Configuration** dialog box displays.

4. To edit an existing rule, complete the following steps.

   a. Select the rule you want to edit in the **ACL Entries** list and click the left arrow button.

      The rule displays in the **ACL Entry** area.

   b. Complete step 5 through step 10 in "Creating a standard L3 ACL configuration" on page 581.

      The updated ACL rule displays in the **ACL Entries** list. To update additional rules for the same ACL, repeat step 4.

5. To add a new rule, complete step 5 through step 10 in "Creating a standard L3 ACL configuration" on page 581.

   The updated ACL rule displays in the **ACL Entries** list. To update additional rules for the same ACL, repeat step 5.

6. To delete an existing rule, select the rule you want to delete in the **ACL Entries** list and click the left arrow button.

7. Use the **Up** and **Down** arrow buttons to rearrange the ACLs in the **ACL Entries** list.

8. Click **OK** on the **Edit - L3 ACL Configuration** dialog box.

9. To set the configuration type and operations, refer to "Configuring the ACL configuration type and operations" on page 597.

10. (Ethernet routers only) To set the hit statistics duration, refer to "Configuring hit statistics" on page 597.

11. To deploy the configuration, click **OK** on the *Device_Name* - **L3 ACL Configuration** dialog box.

    The **Deploy to Products - L3 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Copying a standard L3 ACL configuration

To copy a standard L3 ACL configuration, complete the following steps.

1. Select the device and select **Configure > Security > L3 ACL > Product**.

   The *Device_Name* - **L3 ACL Configuration** dialog box displays.

2. Select the standard ACL configuration you want to copy in the **ACLs** list.
3. Click **Duplicate**.

   The **Duplicate - L3 ACL Configuration** dialog box displays with the default name 'Copy of *Original_Name*'.

4. Enter a new name or number for the ACL in the **ACL Name/Number field.**
5. To edit an existing rule, complete the following steps.
   a. Select the rule you want to edit in the **ACL Entries** list and click the left arrow button.

      The rule displays in the **ACL Entry** area.

   b. Complete step 5 through step 10 in "Creating a standard L3 ACL configuration" on page 581.

      The updated ACL rule displays in the **ACL Entries** list. To update additional rules for the same ACL, repeat step 4.

6. To add a new rule, complete step 5 through step 10 in "Creating a standard L3 ACL configuration" on page 581.

   The updated ACL rule displays in the **ACL Entries** list. To update additional rules for the same ACL, repeat step 5.

7. To delete an existing rule, select the rule you want to delete in the **ACL Entries** list and click the left arrow button.
8. Use the **Up** and **Down** arrow buttons to rearrange the ACLs in the **ACL Entries** list.
9. Click **Close** on the **L3 ACL Advanced Settings** dialog box to close.
10. Click **OK** on the **Duplicate - L3 ACL Configuration** dialog box.
11. To set the configuration type and operations, refer to "Configuring the ACL configuration type and operations" on page 597.
12. (Ethernet routers only) To set the hit statistics duration, refer to "Configuring hit statistics" on page 597.
13. To deploy the configuration, click **OK** on the *Device_Name* - **L3 ACL Configuration** dialog box.

    The **Deploy to Products - L3 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Creating an extended L3 ACL configuration

To create an extended L3 ACL configuration, complete the following steps.

1. Select the device and select **Configure > Security > L3 ACL > Product**.

   The *Device_Name* - **L3 ACL Configuration** dialog box displays.

2. Select **New IPv4** from the **Add** list.

The **Add - L3 ACL Configuration** dialog box displays.

3. Select **Extended** from the **Type** list.

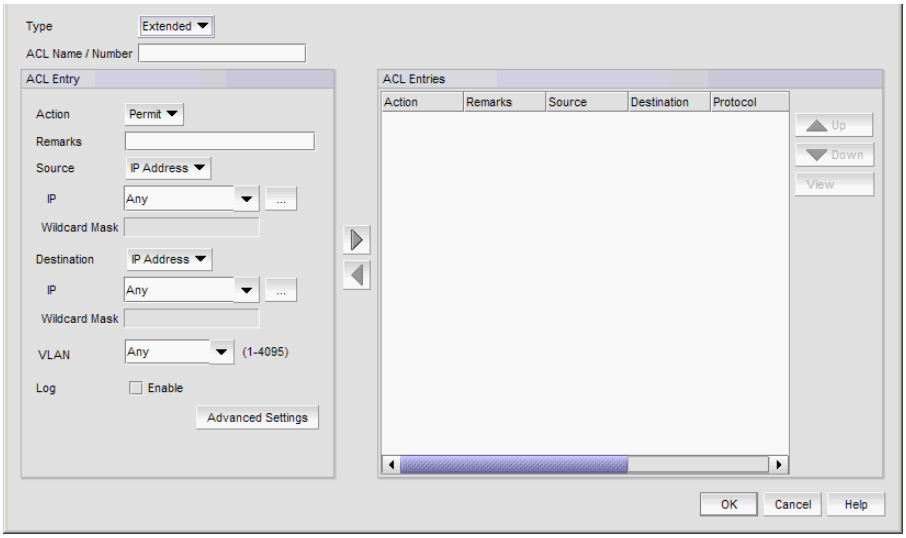


FIGURE 217 Add - L3 ACL Configuration (Extended) dialog box

4. Enter a name or number for the ACL in the **ACL Name/Number field.**
5. Select **Permit** or **Deny** from the **Action** list.
6. Enter a description for the ACL in the **Remarks field.**
7. Choose one of the following options from the **Source** list:
   - To enter an IP address, select **IP Address** and complete the following steps:
     a. Enter the source IP address on which the ACL filters traffic in the **IP Address** list and text field.
     b. Enter a portion of the source IP address on which the ACL filters traffic in the **Wildcard Mask field**.
     The wildcard mask is a four-part value in IP address format consisting of ones and zeros. Use zeros in the mask if the packet source address must match the IP address. Use ones if to match any value.
     For example, if you enter '209.157.22.26' in the **IP Address** field and '0.0.0.255' in the **Wildcard Mask** field, then all hosts in the Class C subnet '209.157.22.x' match the ACL.
   - To select a network, select **IP Address** and choose a network from the list.
     To configure a network, click the ellipsis button and refer to "Network configuration" on page 602.
   - To enter a host name, select **Host** and enter the source host name on which the ACL filters traffic in the **Host** list and text field.
8. Choose one of the following options from the **Destination** list:

- To enter an IP address, select **IP Address** and complete the following steps:
  a. Enter the destination IP address on which the ACL filters traffic in the **IP Address** list and text field.
  b. Enter a portion of the destination IP address on which the ACL filters traffic in the **Wildcard Mask field**.
- To select a network, select **IP Address** and choose a network from the list.

  To configure a network, click the ellipsis button and refer to "Network configuration" on page 602.
- To enter a host name, select **Host** and enter the destination host name on which the ACL filters traffic in the **Host** list and text field.

9. Enter a VLAN identifier (valid values are from 1 to 4095) from the **VLAN** list.
10. Select the **Log Enable** check box to enable logging.
11. Click **Advanced Settings** to configure additional settings for the ACL configuration.

NOTE
You must configure advanced settings to create an extended Layer 3 ACL.

The **L3 ACL Advanced Settings** dialog box displays. To configure additional settings, refer to "Configuring L3 ACL advanced settings" on page 598.

12. Click the right arrow button.

    The new ACL displays in the **ACL Entries** list.
13. Use the **Up** and **Down** arrow buttons to rearrange the ACLs in the **ACL Entries** list.
14. View the advanced settings for an ACL by selected the ACL in the **ACL Entries** list and clicking **View**.

    The **L3 ACL Advanced Settings** dialog box displays.
15. Click **Close** on the **L3 ACL Advanced Settings** dialog box to close.
16. Click **OK** on the **Add - L3 ACL Configuration** dialog box.

    The new ACL displays in the **ACLs** list.
17. To set the configuration type and operations, refer to "Configuring the ACL configuration type and operations" on page 597.
18. (Ethernet routers only) To set the hit statistics duration, refer to "Configuring hit statistics" on page 597.
19. To deploy the configuration, click **OK** on the *Device_Name* - **L3 ACL Configuration** dialog box.

    The **Deploy to Products - L3 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Editing an extended L3 ACL configuration

To edit an extended L3 ACL configuration, complete the following steps.

1. Select the device and select **Configure > Security > L3 ACL > Product**.

   The *Device_Name* - **L3 ACL Configuration** dialog box displays.

2. Select the ACL configuration you want to edit in the **ACLs** list and click **Edit**.

   The **Edit - L3 ACL Configuration** dialog box displays.

3. To edit an existing rule, complete the following steps.

   a. Select the rule you want to edit in the **ACL Entries** list and click the left arrow button.

      The rule displays in the **ACL Entry** area.

   b. Complete step 5 through step 12 in "Creating an extended L3 ACL configuration" on page 585.

      The updated ACL rule displays in the **ACL Entries** list. To edit additional rules for the same ACL, repeat step 3.

4. To add a new rule, complete step 5 through step 12 in "Creating an extended L3 ACL configuration" on page 585.

   The updated ACL rule displays in the **ACL Entries** list. To update additional rules for the same ACL, repeat step 4.

5. To delete an existing rule, select the rule you want to delete in the **ACL Entries** list and click the left arrow button.

6. Use the **Up** and **Down** arrow buttons to rearrange the ACLs in the **ACL Entries** list.

7. View the advanced settings for an ACL by selected the ACL in the **ACL Entries** list and clicking **View**.

   The **L3 ACL Advanced Settings** dialog box displays.

8. Click **Close** on the **L3 ACL Advanced Settings** dialog box to close.

9. Click **OK** on the **Edit - L3 ACL Configuration** dialog box.

   The updated ACL displays in the **ACLs** list.

10. To set the configuration type and operations, refer to "Configuring the ACL configuration type and operations" on page 597.

11. (Ethernet routers only) To set the hit statistics duration, refer to "Configuring hit statistics" on page 597.

12. To deploy the configuration, click **OK** on the *Device_Name* - **L3 ACL Configuration** dialog box.

    The **Deploy to Products - L3 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Copying an extended L3 ACL configuration

To copy an extended L3 ACL configuration, complete the following steps.

1. Select the device and select **Configure > Security > L3 ACL > Product**.

   The *Device_Name* - **L3 ACL Configuration** dialog box displays.

2. Select the ACL configuration you want to copy in the **ACLs** list and click **Duplicate**.

The **Duplicate - L3 ACL Configuration** dialog box displays with the default name 'Copy of *Original_Name*'.

3. Enter a new name or number for the ACL in the **ACL Name/Number field.**
4. To edit an existing rule, complete the following steps.
   a. Select the rule you want to edit in the **ACL Entries** list and click the left arrow button.

      The rule displays in the **ACL Entry** area.

   b. Complete step 5 through step 12 in "Creating an extended L3 ACL configuration" on page 585.

      The updated ACL rule displays in the **ACL Entries** list. To edit additional rules for the same ACL, repeat step 4.
5. To add a new rule, complete step 5 through step 12 in "Creating an extended L3 ACL configuration" on page 585.

   The updated ACL rule displays in the **ACL Entries** list. To update additional rules for the same ACL, repeat step 5.
6. To delete an existing rule, select the rule you want to delete in the **ACL Entries** list and click the left arrow button.
7. Use the **Up** and **Down** arrow buttons to rearrange the ACLs in the **ACL Entries** list.
8. View the advanced settings for an ACL by selected the ACL in the **ACL Entries** list and clicking **View**.

   The **L3 ACL Advanced Settings** dialog box displays.
9. Click **Close** on the **L3 ACL Advanced Settings** dialog box to close.
10. Click **OK** on the **Duplicate - L3 ACL Configuration** dialog box.

    The new ACL displays in the **ACLs** list.
11. To set the configuration type and operations, refer to "Configuring the ACL configuration type and operations" on page 597.
12. (Ethernet routers only) To set the hit statistics duration, refer to "Configuring hit statistics" on page 597.
13. To deploy the configuration, click **OK** on the *Device_Name* - **L3 ACL Configuration** dialog box.

    The **Deploy to Products - L3 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Creating an IPv6 L3 ACL configuration

To create an IPv6 L3 ACL configuration, complete the following steps.

1. Select an Ethernet router product and select **Configure > Security > L3 ACL > Product**.

   The *Device_Name* - **L3 ACL Configuration** dialog box displays.

2. Select **New IPv6** from the **Add** list.

   The **Add - L3 ACL (IPv6) Configuration** dialog box displays.

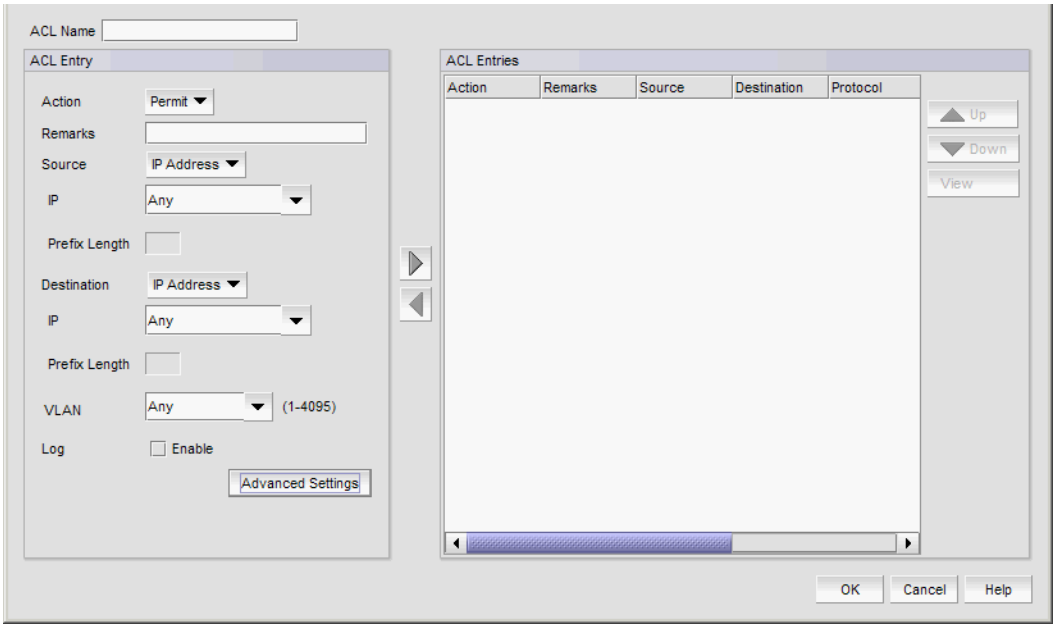


FIGURE 218 **Add - L3 ACL (IPv6) Configuration dialog box**

3. Enter a name or number for the ACL in the **ACL Name/Number** field.
4. Select **Permit** or **Deny** from the **Action** list.
5. Enter a description for the ACL in the **Remarks field.**
6. Choose one of the following options from the **Source** list:
   - To enter an IP address, select **IP Address** and complete the following steps:
     a. Enter the source IP address on which the ACL filters traffic in the **IP Address** list and text field.
        You can enter the IPv6 address in compressed (for example, you can compress 2001:db8:0:0:0:0:2:1 can be shortened to 2001:db8::2:1) or raw format.
     b. Enter the prefix length (1 through 128) in the **Prefix Length** field.
   - To enter an IPv6 address, select **IP Address** and complete enter the source IPv6 address on which the ACL filters traffic in the **IP** list and text field.
   - To select a network, select **IP Address** and choose a network from the list.
   - To enter a host name, select **Host** and enter the source host name on which the ACL filters traffic in the **Host** list and text field.
7. Choose one of the following options from the **Destination** list:

- To enter an IP address, select **IP Address** and complete the following steps:
  a. Enter the destination IP address on which the ACL filters traffic in the **IP Address** list and text field.
  You can enter the IPv6 address in compressed (for example, you can compress 2001:db8:0:0:0:0:2:1 can be shortened to 2001:db8::2:1) or raw format.
  b. Enter the prefix length (1 through 128) in the **Prefix Length** field.
- To select a network, select **IP Address** and choose a network from the list.
- To enter a host name, select **Host** and enter the destination host name on which the ACL filters traffic in the **Host** list and text field.

8. Enter a VLAN identifier (valid values are from 1 to 4095) from the **VLAN** list.
9. Select the **Log Enable** check box to enable logging.
10. Click **Advanced Settings** to configure additional settings for the ACL configuration.

NOTE
You must configure advanced settings to create an extended Layer 3 ACL.

The **L3 ACL Advanced Settings** dialog box displays.

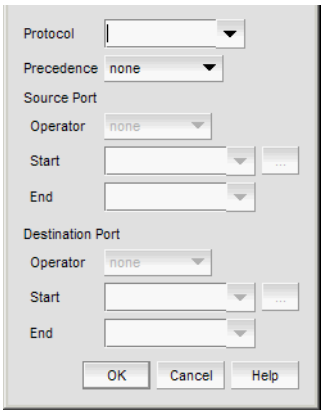


FIGURE 219 Add - L3 Advanced Settings dialog box (IPv6)

To configure additional settings, refer to "Configuring L3 ACL advanced settings" on page 598.

11. Click the right arrow button.
    The new ACL displays in the **ACL Entries** list.
12. Repeat step 4 through step 11 to add additional entries.
13. Use the **Up** and **Down** arrow buttons to rearrange the ACLs in the **ACL Entries** list.
14. View the advanced settings for an ACL by selected the ACL in the **ACL Entries** list and clicking **View**.
    The **L3 ACL Advanced Settings** dialog box displays.
15. Click **Close** on the **L3 ACL Advanced Settings** dialog box to close.
16. Click **OK** on the **Add - L3 ACL (IPv 6) Configuration** dialog box.

The new ACL displays in the **ACLs** list.

17. To set the configuration type and operations, refer to "Configuring the ACL configuration type and operations" on page 597.
18. (Ethernet routers only) To set the hit statistics duration, refer to "Configuring hit statistics" on page 597.
19. To deploy the configuration, click **OK** on the *Device_Name* - **L3 ACL Configuration** dialog box.

    The **Deploy to Products - L3 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Editing an IPv6 L3 ACL configuration

To edit an IPv6 L3 ACL configuration, complete the following steps.

1. Select an Ethernet router product and select **Configure > Security > L3 ACL > Product**.

   The *Device_Name* - **L3 ACL Configuration** dialog box displays.
2. Select the ACL configuration you want to copy in the **ACLs** list and click **Edit**.

   The **Edit - L3 ACL (IPv 6) Configuration** dialog box displays.
3. To add a new ACL entry, repeat step 4 through step 11 in "Creating an extended L3 ACL configuration" on page 585.
4. To edit an existing ACL entry, select the ACL you want to edit in the **ACL Entries** list, click the left arrow button and repeat step 4 through step 11 in "Creating an extended L3 ACL configuration" on page 585.
5. To delete an existing ACL entry, select the ACL you want to delete in the **ACL Entries** list and click the left arrow button.
6. Use the **Up** and **Down** arrow buttons to rearrange the ACLs in the **ACL Entries** list.
7. View the advanced settings for an ACL by selected the ACL in the **ACL Entries** list and clicking **View**.

   The **L3 ACL Advanced Settings** dialog box displays.
8. Click **Close** on the **L3 ACL Advanced Settings** dialog box to close.
9. Click **OK** on the **Edit - L3 ACL (IPv 6) Configuration** dialog box.

   The updated ACL displays in the **ACLs** list.
10. To set the configuration type and operations, refer to "Configuring the ACL configuration type and operations" on page 597.
11. (Ethernet routers only) To set the hit statistics duration, refer to "Configuring hit statistics" on page 597.
12. To deploy the configuration, click **OK** on the *Device_Name* - **L3 ACL Configuration** dialog box.

    The **Deploy to Products - L3 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Copying an IPv6 L3 ACL configuration

To copy an IPv6 L3 ACL configuration, complete the following steps.

1. Select an Ethernet router product and select **Configure > Security > L3 ACL > Product**.

   The *Device_Name* - **L3 ACL Configuration** dialog box displays.

2. Select the ACL configuration you want to copy in the **ACLs** list and click **Duplicate**.

   The **Duplicate - L3 ACL (IPv6) Configuration** dialog box displays with the default name 'Copy of *Original_Name*'.

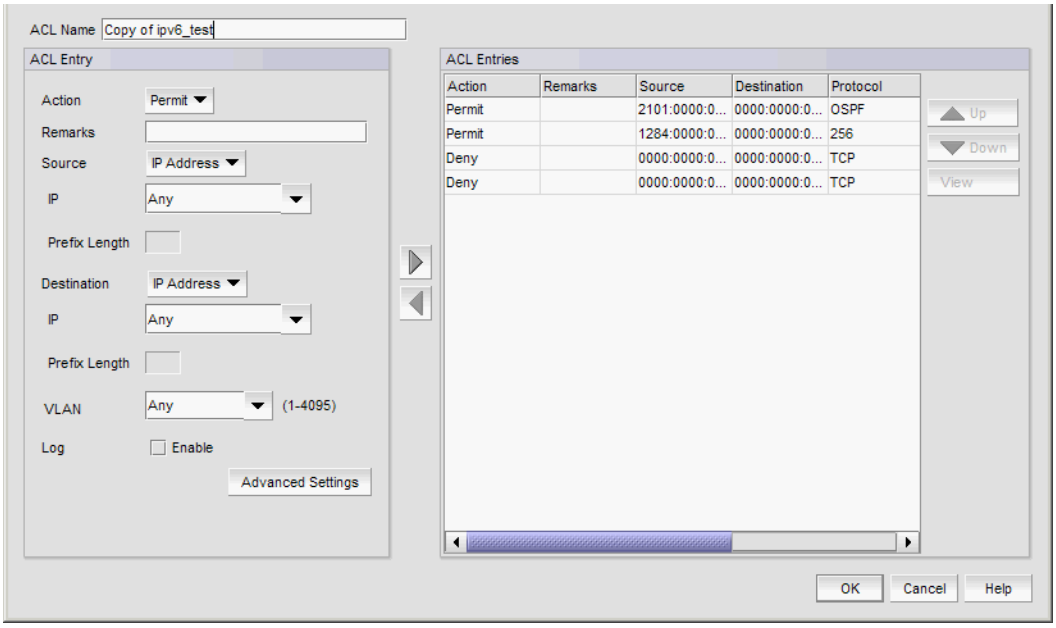


FIGURE 220 Duplicate - L3 ACL (IPv6) Configuration dialog box

3. Edit the name or number for the ACL in the **ACL Name/Number** field.
4. To add a new ACL entry, repeat step 4 through step 11 in "Creating an extended L3 ACL configuration" on page 585.
5. To edit an existing ACL entry, select the ACL you want to edit in the **ACL Entries** list, click the right arrow button and repeat step 4 through step 11 in "Creating an extended L3 ACL configuration" on page 585.
6. To delete an existing ACL entry, select the ACL you want to delete in the **ACL Entries** list and click the left arrow button.
7. Use the **Up** and **Down** arrow buttons to rearrange the ACLs in the **ACL Entries** list.
8. Select an ACL in the **ACL Entries** list and click **View** to the **L3 ACL Advanced Settings** dialog box for the ACL.
9. View the advanced settings for an ACL by selected the ACL in the **ACL Entries** list and clicking **View**.

   The **L3 ACL Advanced Settings** dialog box displays.

10. Click **Close** on the **L3 ACL Advanced Settings** dialog box to close.

11. Click **OK** on the **Duplicate - L3 ACL (IPv 6) Configuration** dialog box.

    The new ACL displays in the **ACLs** list.

12. To set the configuration type and operations, refer to "Configuring the ACL configuration type and operations" on page 597.

13. (Ethernet routers only) To set the hit statistics duration, refer to "Configuring hit statistics" on page 597.

14. To deploy the configuration, click **OK** on the *Device_Name* - **L3 ACL Configuration** dialog box.

    The **Deploy to Products - L3 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Deleting a L3 ACL configuration

NOTE
You cannot delete an IPv6 L3 ACL that is bound to a port.

To delete an ACL configuration, complete the following steps.

1. Select the device and select **Configure > Security > Layer 2 ACL > Product**.

   The *Device_Name* - **L3 ACL Configuration** dialog box displays.

2. Select the ACL you want to delete in the **ACLs** list and click **Delete**.

3. Click **Yes** on the confirmation message.

4. Click **OK** on the *Device_Name* - **L3 ACL Configuration** dialog box.

   The **Deploy to Products - L3 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 631

Assigning a L3 ACL configuration to an interface

To assign L3 ACL configuration to a interface, complete the following steps.

1. Select **Configure > Security > L3 ACL > Port**.

   The **Port Selection - L3 ACL** dialog box displays.

2. Select a port in the **Available Ports** list and click the right arrow button.

3. Click **OK**.

   The *Device_Name* - *Port_Number* - **ACL Port Configuration** dialog box displays.

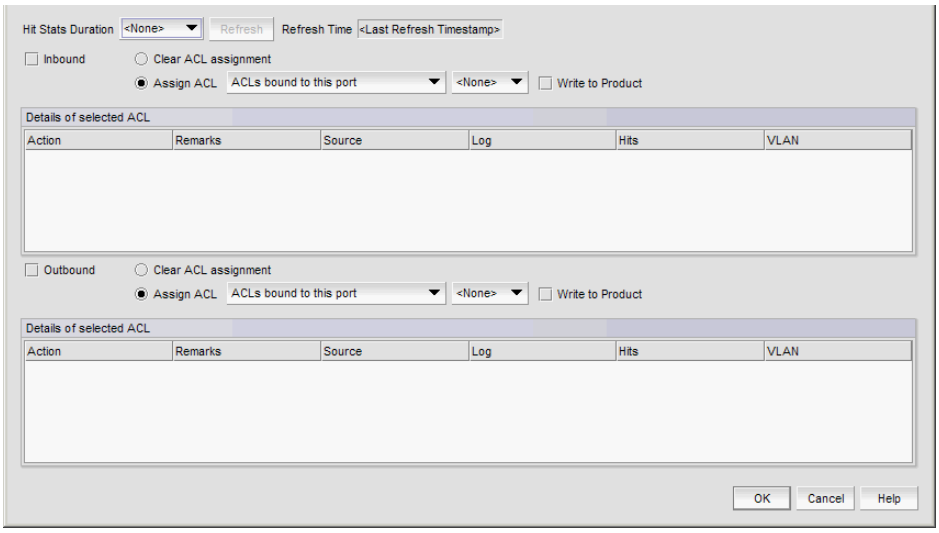


FIGURE 221 *Device_Name - Port_Number* - **ACL Port Configuration dialog box**

4. (Ethernet routers only) Select a duration (1 Second, 1 Minute, 5 Minutes, or Cumulative) to track the number of times an ACL filter is used in the **Hits Stats Duration** list.

   Click **Refresh** to collect the hit statistics. The application updates the **Hits** column of the **Details of Selected ACL** list.

5. To assign an ACL configuration to inbound messages, select the **Inbound** check box and complete the following steps:

   a. Select the **Assign ACL** option and choose one of the following options from the first **Assign ACL** list:

      - Select **ACLs on this Product** to assign ACLs deployed on the product to the port. The second list is populated with the ACLs deployed on the switch or associated with a save deployment object.
      - Select **ACLs bound to this port** to assign ACLs bound to the interface to the port. The second list is populated with the ACLs bound to the interface.
      - *Deployment_Name* — Select to assign a user-configured deployment on the port.

   b. Select the ACL you want to assign to the port from the second **Assign ACL** list.

      For Ethernet router products runing IronWare 5.4 or later, you can assign ACLs to IPv4 and IPv6 ports. To assign the ACL to an IPv4 port, select the **IPv4** check box and select an ACL from the **IPv4** list. To assign the ACL to an **IPv6** port, select the IPv6 check box and select an ACL from the **IPv6** list.

   c. Select the **Write to Product** check box to create the selected ACL on the device if it does not already exist.

6. To assign an ACL configuration to outbound messages, select the **Outbound** check box and complete the following steps:

NOTE
You can only assign an ACL to an outbound message on an Application product.

a. Select the **Assign ACL** option and choose one of the following options from the first **Assign ACL** list:

- Select **ACLs on this Product** to assign ACLs deployed on the product to the port. The second list is populated with the ACLs deployed on the switch or associated with a save deployment object.
- Select **ACLs bound to this port** to assign ACLs bound to the interface to the port. The second list is populated with the ACLs bound to the interface.
- *Deployment_Name* — Select to assign a user-configured deployment on the port.

b. Select the ACL you want to assign to the port from the second **Assign ACL** list.

For Ethernet router products runing IronWare 5.4 or later, you can assign ACLs to IPv4 and IPv6 ports. To assign the ACL to an IPv4 port, select the **IPv4** check box and select an ACL from the **IPv4** list. To assign the ACL to an **IPv6** port, select the IPv6 check box and select an ACL from the **IPv6** list.

c. Select the **Write to Product** check box to create the selected ACL on the device if it does not already exist.

7. Click **OK** on the *Device_Name* - *Port_Number* - **ACL Port Configuration** dialog box.

The **Deploy to Ports - L3 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629

Clearing L3 ACL assignments

NOTE
For Ethernet router products running 5.4 or later, if the selected port has an IPv6 ACL assigned, the ACL bound to the port field displays "0". You cannot clear the ACL on this port.

To clear L3 ACL configuration from interfaces, complete the following steps.

1. Select **Configure > Security > L3 ACL > Port**.

The **Port Selection - L3 ACL** dialog box displays.

2. Select a port in the **Available Ports** list and click the right arrow button.
3. Click **OK**.

The *Device_Name* - *Port_Number* - **ACL Port Configuration** dialog box displays.

4. To clear inbound messages, complete the following steps:
   a. Select the **Inbound** check box.
   b. Select the **Clear ACL Assignment** option.
5. To clear outbound messages, complete the following steps:
   a. Select the **Outbound** check box.
   b. Select the **Clear ACL Assignment** option.
6. Click **OK** on the *Device_Name* - *Port_Number* - **Layer 3 ACL Configuration** dialog box.

The **Deploy to Ports - L3 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629

Configuring the ACL configuration type and operations

To configure the ACL configuration type and operation, complete the following steps.

1. Select the configuration type by choosing one of the following options:
   - **Incremental —** Deploys add and delete operations. During deployment, the Management application checks all ACLs to determine if the ACL name or number matches any ACL number already deployed on a switch.

     If the ACL name or number matches, the following actions occur:

     - Add operation — The ACL on the switch is overwritten by the one in configuration during deployment.
     - Delete operation — Deletes the ACL from the switch during deployment.
     - No Action operation — Skips the ACL during deployment; however, if you save the deployment the 'no action' ACL remains part of the configuration and can be added or deleted at a later date.

     If the ACL name or number does not match, the following actions occur:

     - Add operation — The ACL is appended on the switch.
     - No Action operation — Skips the ACL during deployment; however, if you save the deployment the 'no action' ACL remains part of the configuration and can be added or deleted at a later date.
   - **Overwrite —** Only deploys add operations. During deployment, the Management application clears all ACLs currently on the switch and then applies the new configuration.
2. (Ethernet routers only) To set the hit statistics duration, refer to "Configuring hit statistics" on page 597.
3. To deploy the configuration, click **OK** on the *Device_Name* - **L3 ACL Configuration** dialog box.

   The **Deploy to Products - L3 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Configuring hit statistics

To configure hit statistics, complete the following steps.

1. Select an Ethernet router product and select **Configure > Security > L3 ACL > Product**.

   The *Device_Name* - **L3 ACL Configuration** dialog box displays.
2. Select a duration (1 second, 1 minute, 5 minutes, or Cumulative) from the **Hit Stats Duration** list.
3. Click **Refresh** to refresh the hit statistics.

   The **Refresh Time** field displays the last time the Management application client successfully collected the hit statistics.

Configuring L3 ACL advanced settings

You configure L3 ACL advanced settings for extended L3 ACL device configurations. To configure an extended L3 ACL, refer to one of the following procedures:

- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588
- "Creating an IPv6 L3 ACL configuration" on page 590
- "Editing an IPv6 L3 ACL configuration" on page 592
- "Copying an IPv6 L3 ACL configuration" on page 593

To configure advanced settings for an extended L3 ACL configuration, complete the following steps.

1. Click **Advanced Settings** on the **Add/Edit/Duplicate** - **L3 ACL Configuration** dialog box.

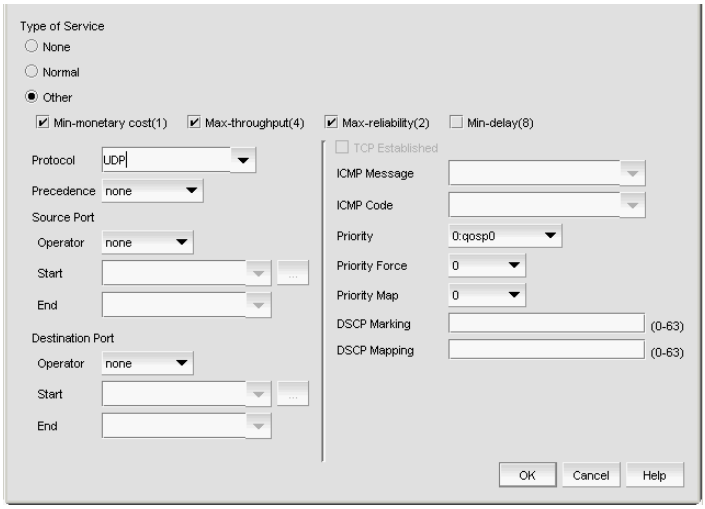


FIGURE 222 Advanced Settings dialog box

2. (IPv4 ACL only) Select one of the following types of service (TOS) to use to filter the packet from the **Type of Service** list.
   - **None** — Select to not filter by TOS.
   - **Normal** — Select to filter packets that match the normal TOS. The decimal value is 0.
   - **Other** — Select filter by one or more additional options.
3. (IPv4 ACL only) If you selected **Other** from the **Type of Service** list, select one or more of following additional options:
   - **Min-monetary cost (1)** — Select to have the ACL filter packets that match the minimum monetary cost TOS. The decimal value is 1.
   - **Max-reliability (2)** — Select to have the ACL filter packets that match the maximum reliability TOS. The decimal is 2.

- **Max-throughput (4)** — Select to have the ACL filters packets that match the maximum throughput TOS. The decimal value is 4.
- **Min-delay (8)** — Select to have the ACL filter packets that match the minimum delay TOS. The decimal value is 8.

4. Select one of the following protocols from the **Protocol** list to filter the packet by protocol.
   - **IP** (IPv4 ACL only) — Internet Protocol
   - **ICMP** (IPv4 ACL only) — Internet Control Message Protocol
   - **IGMP —** Internet Group Management Protocol
   - **IGRP** — Internet Gateway Routing Protocol
   - **OSPF —** Open Shortest Path First
   - **TCP —** Transmission Control Protocol
   - **UDP** — User Datagram Protocol

   If the protocol you use is not in the list, enter a value from 0 through 255 in the text field.
5. Select one of the following precedences from the **Precedence** list to filter the packet by precedence.
   - **none** — Select to not filter packets by precedence.
   - **routine** — Select to filter packets with the routine precedence.
   - **priority** — Select to filter packets with the priority precedence.
   - **immediate** — Select to filter packets with the immediate precedence.
   - **flash** — Select to filter packets with the flash precedence.
   - **flash-override** — Select to filter packets with the flash override precedence.
   - **critical** — Select to filter packets with the critical precedence.
   - **internet** — Select to filter packets with the internetwork control precedence.
   - **network** — Select to filter packets with the network control precedence.
6. (TCP and UDP protocols only) To filter packets by the source port, complete the following steps.

   Only available when you select **TCP** or **UDP** from the **Protocol** list.

   a. Select one of the following options:
      - **none** — Select to not use the source port numbers to filter packets.
      - **equals** — Select to use the TCP or UDP port name or number specified in the **Start** field.
      - **not equal** — Select to use all TCP or UDP port numbers except the port name or number specified in the **Start** field.
      - **greater than** — Select to use all TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name specified in the **Start** field.
      - **less than** — Select to use all TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name specified in the **Start** field.
      - **range** — Select to use all TCP or UDP port numbers between the TCP or UDP port name or number specified in the **Start** field and the **End** field.

b. Enter a port number or select a port application name from the **Start** list.

If you selected **range** from the **Operator** list, enter the port number or name of the lower numbered port in the range. Click the ellipsis button to launch the **Service** dialog box to see a list of services and service groups. For more information about services and service groups, refer to "Service configuration" on page 611.

c. Enter a port number or select a port application name from the **End** list.

If you selected **range** from the **Operator** list, enter the port number or name of the higher numbered port in the range.

7. (TCP and UDP protocols only) To filter packets by the destination port, complete the following steps.

Only available when you select **TCP** or **UDP** from the **Protocol** list.

a. Select one of the following options:

- **none** — Select to not use the destination port numbers to filter packets.
- **equals** — Select to use the TCP or UDP port name or number specified in the **Start** field.
- **not** equal — Select to use all TCP or UDP port numbers except the port name or number specified in the **Start** field.
- **greater than** — Select to use all TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name specified in the **Start** field.
- **less than** — Select to use all TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name specified in the **Start** field.
- **range** — Select to use all TCP or UDP port numbers between the TCP or UDP port name or number specified in the **Start** field and the **End** field.

b. Enter a port number or select a port application name from the **Start** list.

If you selected **range** from the **Operator** list, enter the port number or name of the lower numbered port in the range. Click the ellipsis button to launch the **Service** dialog box to see a list of services and service groups. For more information about services and service groups, refer to "Service configuration" on page 611.

c. Enter a port number or select a port application name from the **End** list.

If you selected **range** from the **Operator** list, enter the port number or name of the higher numbered port in the range.

8. (IPv4 ACL only - ICMP protocol only) To filter packets by the ICMP message type, complete the following steps.

a. Choose one of the following message types:T

- any-icmp-type
- echo
- echo-reply
- information request
- mask-reply
- mask-request
- parameter-problem
- redirect
- source-quench
- time-exceeded
- timestamp-reply
- timestamp-request
- unreachable

b. Choose one of the following code types:

The available code types vary depending on the selected message type.T

echo
- echo

echo-reply
- echo-reply

information-request
- information-request

mask-reply
- mask-reply

mask-request
- mask-request

parameter-problem
- parameter-problem
- general-parameter-problem

redirect
- net-redirect
- host-redirect
- net-tos-redirect
- host-tos-redirect

source-quench
- source-quench

time-exceeded
- ttl-exceeded
- reassembly-timeout

timestamp-reply
- timestamp-reply

timestamp-request
- timestamp-request

unreachable
- net-unreachable
- host-unreachable
- protocol-unreachable
- port-unreachable
- packet-too-big
- source-route-failed
- destination-network-unknown
- destination-host-unknown
- source-host-isolated
- destination-net-prohibited
- destination-host-prohibited
- net-tos-unreachable
- host-tos-unreachable
- administratively-prohibited
- host-precedence-violation
- precedence-cutoff

9. (IPv4 ACL only) Select one of the following options to match packets to a hardware forwarding queue from the **Priority** list.
   - 0:qosp0
   - 1:qosp1
   - 2:qosp2
   - 3:qosp3

   This changes the internal forwarding priority of the packet. If the outgoing interface is an 802.1Q interface, the specified priority is mapped to the equivalent 802.1p (CoS) priority and the packet is marked with the new 802.1p priority.
10. (IPv4 ACL only) Select the hardware forwarding queue to which you want to assign outgoing packets from the **Priority Force** list.
11. (IPv4 ACL only) Select a priority map to filter packets based on their 802.1p value from the **Priority Map** list.

    Selecting a priority map does not change the forwarding priority of the packet or mark the packet with a new priority.
12. (IPv4 ACL only) Enter a Differentiated Services Code Points (DSCP) marking value to mark packets with a specified TOS value in the **DSCP-Marking (0-63)** field.
13. Enter a DSCP mapping value to maps a DSCP value to an internal forwarding priority in the (IPv4 ACL only) **DSCP-Mapping (0-63)** field.

14. Click **OK** on the **Advanced Settings** dialog box.

To finish configuring the ACL, return to one of the following procedures:

- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588
- "Creating an IPv6 L3 ACL configuration" on page 590
- "Editing an IPv6 L3 ACL configuration" on page 592
- "Copying an IPv6 L3 ACL configuration" on page 593

Network configuration

The Management application allows you to filter traffic from a specific Network. A Network is made up of one or more devices in a subnet. Use the following procedures to configure a network:

- "Viewing existing networks" on page 602
- "Creating a network" on page 603
- "Editing a network" on page 604
- "Copying a network" on page 605
- "Deleting a network" on page 605

Viewing existing networks

You can access the **Network** dialog box when configuring a standard or extended L3 ACL device configuration. To configure a standard or extended L3 ACL, refer to one of the following procedures:

- "Creating a standard L3 ACL configuration" on page 581
- "Editing a standard L3 ACL configuration" on page 584
- "Copying a standard L3 ACL configuration" on page 585
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588

To view all existing networks, complete the following steps.

1. Click the **Networks** tab.

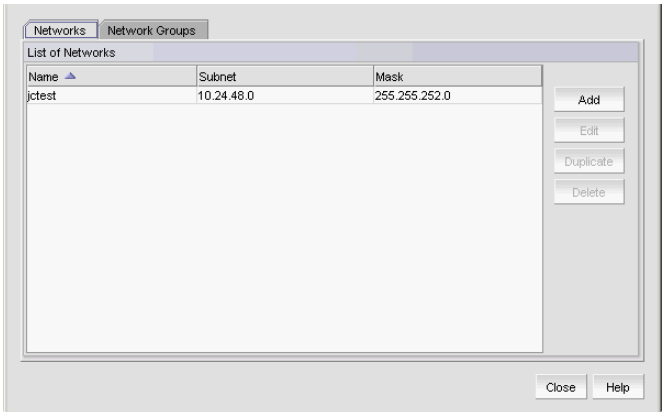


FIGURE 223 Network dialog box, Networks tab

2. Review the **List of Networks** table:
   - **Name** — The user-defined network name.
   - **Subnet** — The IP address of the subnet.
   - **Mask** — The IP address of the mask.
3. Click **Close** on the **Network** dialog box.

   To finish configuring the ACL, return to one of the above procedures.

Creating a network

You can access the **Network** dialog box when configuring a standard or extended L3 ACL device configuration. To configure a standard or extended L3 ACL, refer to one of the following procedures:

- "Creating a standard L3 ACL configuration" on page 581
- "Editing a standard L3 ACL configuration" on page 584
- "Copying a standard L3 ACL configuration" on page 585
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588

To create a network, complete the following steps.

1. Click the **Networks** tab.
2. Click **Add**.

   The **Add Network** dialog box displays.

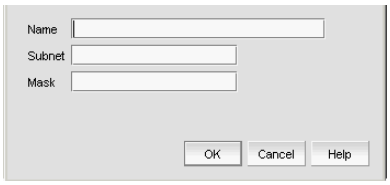


FIGURE 224 Add Network dialog box

3. Enter a name for the network in the **Name** field.
4. Enter a valid IP address (IPv4 format) in the **Subnet** field.
5. Enter a valid IP address in the **Mask** field.

   If you use the ACL Network as the source IP address, the Subnet mask from the ACL Network will be converted to Wildcard mask when deploying the ACL to the device.

   The Network dialog box only accepts subnet mask.
6. Click **OK** on the **Add Network** dialog box.
7. Click **Close** on the **Network** dialog box.

   To finish configuring the ACL, return to one of the above procedures.

Editing a network

You can access the **Network** dialog box when configuring a standard or extended L3 ACL device configuration. To configure a standard or extended L3 ACL, refer to one of the following procedures:

- "Creating a standard L3 ACL configuration" on page 581
- "Editing a standard L3 ACL configuration" on page 584
- "Copying a standard L3 ACL configuration" on page 585
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587

To edit a network, complete the following steps.

1. Click the **Networks** tab.
2. Select the network you want to edit in the **List of Networks** table and click **Edit**.

   The **Edit Network** dialog box displays.
3. Enter a valid IP address (IPv4 format) in the **Subnet** field.
4. Enter a valid IP address in the **Mask** field.
5. Click **OK** on the **Edit Network** dialog box.
6. Click **Close** on the **Network** dialog box.

   To finish configuring the ACL, return to one of the above procedures.

Copying a network

You can access the **Network** dialog box when configuring a standard or extended L3 ACL device configuration. To configure a standard or extended L3 ACL, refer to one of the following procedures:

- "Creating a standard L3 ACL configuration" on page 581
- "Editing a standard L3 ACL configuration" on page 584
- "Copying a standard L3 ACL configuration" on page 585
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588

To copy a network, complete the following steps.

1. Click the **Networks** tab.
2. Select the network you want to copy in the List of Networks table and click **Duplicate**.

   The **Duplicate Network** dialog box displays.
3. Enter a name for the network in the **Name** field.
4. Enter a valid IP address (IPv4 format) in the **Subnet** field.
5. Enter a valid IP address in the **Mask** field.
6. Click **OK** on the **Duplicate Network** dialog box.
7. Click **Close** on the **Network** dialog box.

   To finish configuring the ACL, return to one of the above procedures.

Deleting a network

NOTE
You cannot delete a network that is in use.

NOTE
You cannot delete a network that is in a Network Group.

You can access the **Network** dialog box when configuring a standard or extended L3 ACL device configuration. To configure a standard or extended L3 ACL, refer to one of the following procedures:

- "Creating a standard L3 ACL configuration" on page 581
- "Editing a standard L3 ACL configuration" on page 584
- "Copying a standard L3 ACL configuration" on page 585
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588

To delete a network, complete the following steps.

1. Click the **Networks** tab.
2. Select one or more networks that you want to delete in the **List of Networks** table and click **Delete**.

3. Click **Yes** on the confirmation message.
4. Click **Close** on the **Network** dialog box.

   To finish configuring the ACL, return to one of the above procedures.

Network group configuration

The Management application allows you to filter traffic from a specific network group. A network group is made up of one or more devices, networks, or network groups. Use the following procedures to configure a network:

- "Viewing existing network groups" on page 606
- "Creating a network group" on page 607
- "Editing a network group" on page 608
- "Copying a network group" on page 609
- "Deleting a network group" on page 611

Viewing existing network groups

You can access the **Network** dialog box when configuring a standard or extended L3 ACL device configuration. To configure a standard or extended L3 ACL, refer to one of the following procedures:

- "Creating a standard L3 ACL configuration" on page 581
- "Editing a standard L3 ACL configuration" on page 584
- "Copying a standard L3 ACL configuration" on page 585
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588

To view all existing network groups, complete the following steps.

1. Click the **Network Group** tab.

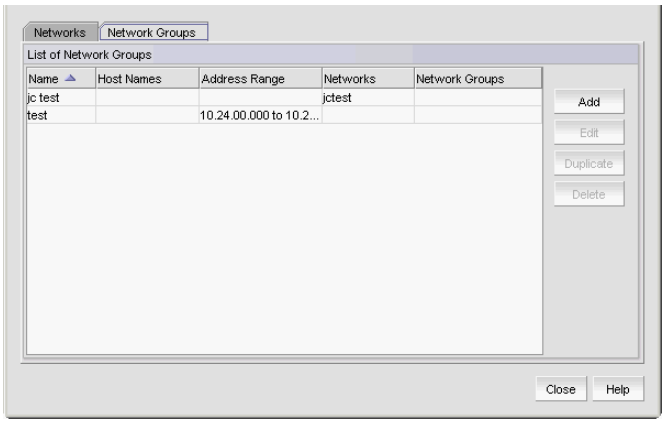


FIGURE 225 Network dialog box, Network Group tab

2. Review the **List of Network Groups** table:
   - **Name** — The user-defined network group name.
   - **Host Names** — The name of each host in the network group.
   - **Address Range** — The range of IP addresses for the network group.
   - **Networks** — The name of each network in the network group.
   - **Network Groups** — The name of each network group in the network group.
3. Click **Close** on the **Network** dialog box.

   To finish configuring the ACL, return to one of the above procedures.

Creating a network group

You can access the **Network** dialog box when configuring a standard or extended L3 ACL device configuration. To configure a standard or extended L3 ACL, refer to one of the following procedures:

- "Creating a standard L3 ACL configuration" on page 581
- "Editing a standard L3 ACL configuration" on page 584
- "Copying a standard L3 ACL configuration" on page 585
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588

To create a network group, complete the following steps.

1. Click the **Network Groups** tab.
2. Click **Add**.

   The **Add Network Group** dialog box displays.

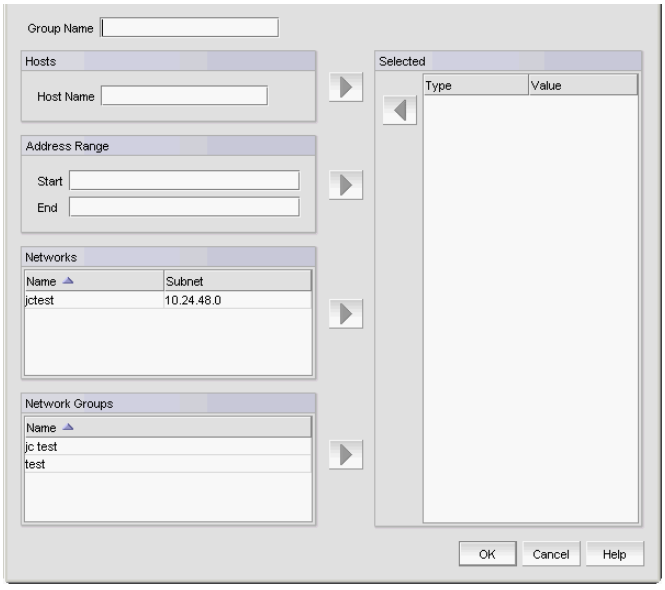


FIGURE 226 Network dialog box, Network Group tab

3. Enter a name for the network group in the **Group Name** field.

4. To add a host to the network group, complete the following steps.
    a. Enter a valid host name in the **Host Name** field.
    b. Click the right arrow button to move the host name to the **Selected** table.
5. To add an address range to the network group, complete the following steps.
    a. Enter an IP address for the start of the range in the **Start** field.
    b. Enter an IP address for the end of the range in the **End** field.
    c. Click the right arrow button to move the address range to the **Selected** table.
6. To add a network to the network group, complete the following steps.
    a. Select one or more networks from the **Networks** table.
    b. Click the right arrow button to move to the **Selected** table.
7. To add another network group to the network group, complete the following steps.
    a. Select one or more network groups from the **Network Groups** table.
    b. Click the right arrow button to move to the **Selected** table.
8. Click **OK** on the **Add Network Group** dialog box.

    The **Network** dialog box - **Network Groups** tab displays with the new network group in the **List of Network Groups** table.
9. Click **Close** on the **Network** dialog box.

    To finish configuring the ACL, return to one of the above procedures.

Editing a network group

You can access the **Network** dialog box when configuring a standard or extended L3 ACL device configuration. To configure a standard or extended L3 ACL, refer to one of the following procedures:

- "Creating a standard L3 ACL configuration" on page 581
- "Editing a standard L3 ACL configuration" on page 584
- "Copying a standard L3 ACL configuration" on page 585
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588

To edit a network group, complete the following steps.

1. Click the **Network Groups** tab.
2. Select the network group you want to edit in the **List of Network Groups** table and click **Edit**.

    The **Edit Network Group** dialog box displays.
3. To remove a component from the network group, select the component in the **Selected** table and click the left arrow button.
4. To add a host to the network group, complete the following steps.
    a. Enter a valid host name in the **Host Name** field.
    b. Click the right arrow button to move the host name to the **Selected** table.

5. To edit an address range to the network group, complete the following steps.
    a. Select the range you want to edit in the **Selected** table and click the left arrow button.
    b. Change the IP address for the start of the range in the **Start** field.
    c. Change the IP address for the end of the range in the **End** field.
    d. Click the right arrow button to move the address range back to the **Selected** table.
6. To add an address range to the network group, complete the following steps.
    a. Enter an IP address for the start of the range in the **Start** field.
    b. Enter an IP address for the end of the range in the **End** field.
    c. Click the right arrow button to move the address range to the **Selected** table.
7. To add a network to the network group, complete the following steps.
    a. Select one or more networks from the **Networks** table.
    b. Click the right arrow button to move to the **Selected** table.
8. To add another network group to the network group, complete the following steps.
    a. Select one or more network groups from the **Network Groups** table.
    b. Click the right arrow button to move to the **Selected** table.
9. Click **OK** on the **Edit Network Group** dialog box.

    The **Network** dialog box - **Network Groups** tab displays.
10. Click **Close** on the **Network** dialog box.

    To finish configuring the ACL, return to one of the above procedures.

Copying a network group

You can access the **Network** dialog box when configuring a standard or extended L3 ACL device configuration. To configure a standard or extended L3 ACL, refer to one of the following procedures:

- "Creating a standard L3 ACL configuration" on page 581
- "Editing a standard L3 ACL configuration" on page 584
- "Copying a standard L3 ACL configuration" on page 585
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588

To copy a network group, complete the following steps.

1. Click the **Network Groups** tab.
2. Select the network group you want to copy in the List of Network Groups table and click **Duplicate**.

    The **Duplicate Network Group** dialog box displays.
3. Enter a name for the network group in the **Group Name** field.
4. To remove a component from the network group, select the component in the **Selected** table and click the left arrow button.

5. To add a host to the network group, complete the following steps.
    a. Enter a valid host name in the **Host Name** field.
    b. Click the right arrow button to move the host name to the **Selected** table.
6. To edit an address range to the network group, complete the following steps.
    a. Select the range you want to edit in the **Selected** table and click the left arrow button.
    b. Change the IP address for the start of the range in the **Start** field.
    c. Change the IP address for the end of the range in the **End** field.
    d. Click the right arrow button to move the address range back to the **Selected** table.
7. To add an address range to the network group, complete the following steps.
    a. Enter an IP address for the start of the range in the **Start** field.
    b. Enter an IP address for the end of the range in the **End** field.
    c. Click the right arrow button to move the address range to the **Selected** table.
8. To add a network to the network group, complete the following steps.
    a. Select one or more networks from the **Networks** table.
    b. Click the right arrow button to move to the **Selected** table.
9. To add another network group to the network group, complete the following steps.
    a. Select one or more network groups from the **Network Groups** table.
    b. Click the right arrow button to move to the **Selected** table.
10. Click **OK** on the **Duplicate Network Group** dialog box.

    The **Network** dialog box - **Network Groups** tab displays with the new network group in the **List of Network Groups** table.
11. Click **Close** on the **Network** dialog box.

    To finish configuring the ACL, return to one of the above procedures.

Deleting a network group

NOTE
You cannot delete a network group that is in use.

You can access the **Network** dialog box when configuring a standard or extended L3 ACL device configuration. To configure a standard or extended L3 ACL, refer to one of the following procedures:

- "Creating a standard L3 ACL configuration" on page 581
- "Editing a standard L3 ACL configuration" on page 584
- "Copying a standard L3 ACL configuration" on page 585
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588

To delete a network group, complete the following steps.

1. Click the **Network Groups** tab.
2. Select one or more network groups that you want to delete in the **List of Network Groups** table and click **Delete**.
3. Click **Yes** on the confirmation message.
4. Click **Close** on the **Network** dialog box.

   To finish configuring the ACL, return to one of the above procedures.

Service configuration

The Management application allows you to filter traffic from a specific service source or destination port. A service is either TCP or UDP port. Use the following procedures to configure a service:

- "Viewing existing services" on page 612
- "Creating a service" on page 613
- "Editing a service" on page 614
- "Copying a service" on page 614
- "Deleting a service" on page 615

Viewing existing services

You can access the **Service** dialog box when configuring an extended L3 ACL device configuration. To configure an extended L3 ACL, refer to one of the following procedures:

- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an IPv6 L3 ACL configuration" on page 592
- "Copying an IPv6 L3 ACL configuration" on page 593

To view all existing services, complete the following steps.

1. Click the **Services** tab.

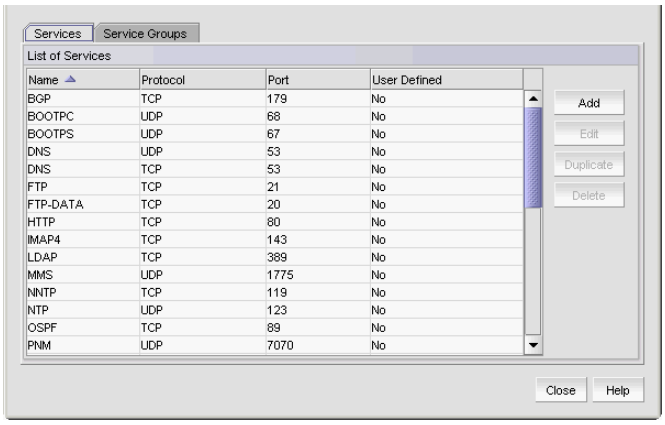


FIGURE 227 Service dialog box, Services tab

2. Review the **List of Services** table:
   - **Name** — The service name.
   - **Protocol** — Whether the service uses the TCP or UDP protocol.
   - **Port** — The port number.
   - **User-defined** — Whether the service is user-defined or not.
3. Click **Close** on the **Network** dialog box.

   To finish configuring the advanced settings, refer to "Configuring L3 ACL advanced settings" on page 598.

Creating a service

You can access the **Service** dialog box when configuring an extended L3 ACL device configuration. To configure an extended L3 ACL, refer to one of the following procedures:

- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an IPv6 L3 ACL configuration" on page 592
- "Copying an IPv6 L3 ACL configuration" on page 593

To create a service, complete the following steps.

1. Click the **Services** tab.
2. Click **Add**.

   The **Add Service** dialog box displays.

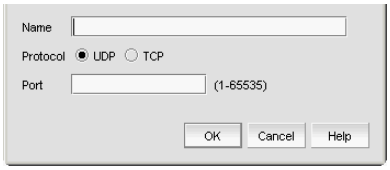


FIGURE 228 Add Service dialog box

3. Enter a name for the service in the **Name** field.
4. Select one of the following protocol options:
   - TCP
   - UDP
5. Enter a port number in the **Port** field.
6. Click **OK** on the **Add Service** dialog box.
7. Click **Close** on the **Service** dialog box.

   To finish configuring the advanced settings for the ACL, refer to "Configuring L3 ACL advanced settings" on page 598.

Editing a service

You can access the **Service** dialog box when configuring an extended L3 ACL device configuration. To configure an extended L3 ACL, refer to one of the following procedures:

- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an IPv6 L3 ACL configuration" on page 592
- "Copying an IPv6 L3 ACL configuration" on page 593

To edit a service, complete the following steps.

1. Click the **Services** tab.
2. Select the service you want to edit and click **Edit**.

   The **Edit Service** dialog box displays.
3. Select one of the following protocol options:
   - TCP
   - UDP
4. Enter a port number in the **Port** field.
5. Click **OK** on the **Edit Service** dialog box.
6. Click **Close** on the **Service** dialog box.

   To finish configuring the advanced settings for the ACL, refer to "Configuring L3 ACL advanced settings" on page 598.

Copying a service

You can access the **Service** dialog box when configuring an extended L3 ACL device configuration. To configure an extended L3 ACL, refer to one of the following procedures:

- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an IPv6 L3 ACL configuration" on page 592
- "Copying an IPv6 L3 ACL configuration" on page 593

To copy a service, complete the following steps.

1. Click the **Services** tab.
2. Select the service you want to copy and click **Duplicate**.

   The **Duplicate Service** dialog box displays.
3. Enter a name for the service in the **Name** field.

4. Select one of the following protocol options:
   - TCP
   - UDP
5. Enter a port number in the **Port** field.
6. Click **OK** on the **Duplicate Service** dialog box.
7. Click **Close** on the **Service** dialog box.

   To finish configuring the advanced settings for the ACL, refer to "Configuring L3 ACL advanced settings" on page 598.

Deleting a service

You can access the **Service** dialog box when configuring an extended L3 ACL device configuration. To configure an extended L3 ACL, refer to one of the following procedures:

- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an IPv6 L3 ACL configuration" on page 592
- "Copying an IPv6 L3 ACL configuration" on page 593

To delete one or more services, complete the following steps.

1. Click the **Services** tab.
2. Select one or more services that you want to delete and click **Delete**.
3. Click **Yes** on the confirmation message.
4. Click **Close** on the **Service** dialog box.

   To finish configuring the advanced settings for the ACL, refer to "Configuring L3 ACL advanced settings" on page 598.

Service group configuration

The Management application allows you to filter traffic from a specific service group. A service group is made up of one or more port ranges, services, or service groups. Use the following procedures to configure a service group:

- "Viewing existing service groups" on page 616
- "Creating a service group" on page 617
- "Editing a service group" on page 618
- "Copying a service group" on page 619
- "Deleting a service group" on page 620

Viewing existing service groups

You can access the **Service** dialog box when configuring an extended L3 ACL device configuration. To configure an extended L3 ACL, refer to one of the following procedures:

- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an IPv6 L3 ACL configuration" on page 592
- "Copying an IPv6 L3 ACL configuration" on page 593

To view all existing service groups, complete the following steps.

1. Click the **Service Groups** tab.

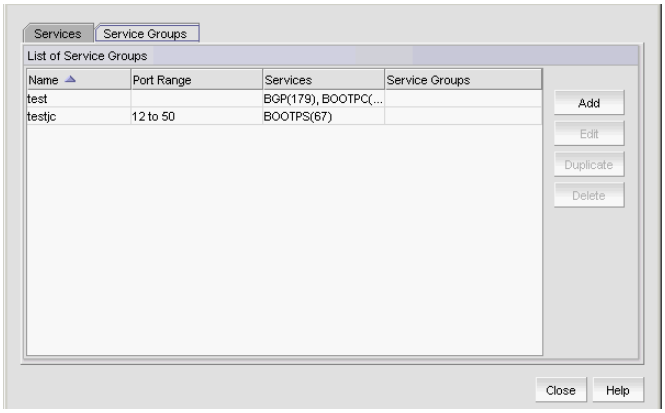


FIGURE 229 Service dialog box, Service Group tab

2. Review the **List of Service Groups** table:
   - **Name** — The service group name.
   - **Port Range** — The range (1 — 65535) of port numbers.
   - **Services** — The name of each service in the service group.
   - **Service Groups** — The name of each service group in the service group.

3. Click **Close** on the **Service** dialog box.

   To finish configuring the advanced settings for the ACL, refer to "Configuring L3 ACL advanced settings" on page 598.

Creating a service group

You can access the **Service** dialog box when configuring an extended L3 ACL device configuration. To configure an extended L3 ACL, refer to one of the following procedures:

- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an IPv6 L3 ACL configuration" on page 592
- "Copying an IPv6 L3 ACL configuration" on page 593

To create a service group, complete the following steps.

1. Click the **Service Groups** tab.
2. Click **Add**.

   The **Add Service Group** dialog box displays.

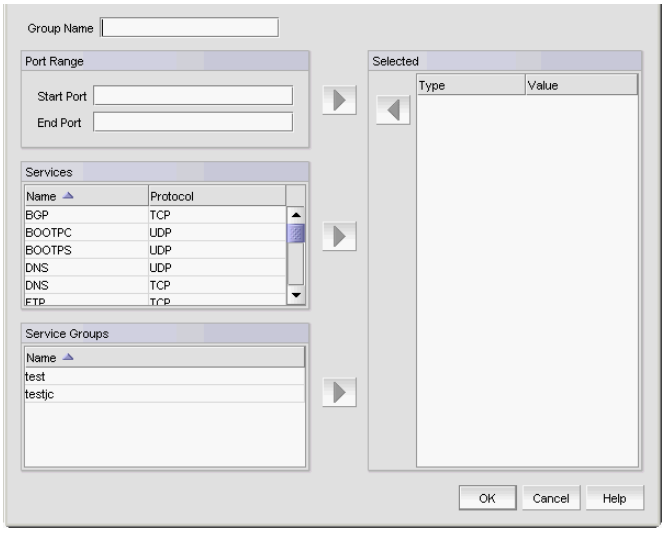


FIGURE 230 Add Service Group dialog box

3. Enter a name for the service group in the **Name** field.
4. To enter a range of ports, complete the following steps.
   a. Enter the starting port number in the **Start Port** field.
   b. Enter the ending port number in the **End Port** field.
   c. Click the right arrow button to move the address range to the **Selected** table.

5. To add a service to the group, complete the following steps.
    a. Select one or more services to add to the group in the Services table.
    b. Click the right arrow button to move the selected services to the **Selected** table.
6. To add a service group to the group, complete the following steps.
    a. Select one or more service groups to add to the group in the Services table.
    b. Click the right arrow button to move the selected service groups to the **Selected** table.
7. Click **OK** on the **Add Service** dialog box.

    The **Service** dialog box, **Service Group** tab displays with the new group in the **List of Service Groups** table.
8. Click **Close** on the **Service** dialog box.

    To finish configuring the advanced settings for the ACL, refer to "Configuring L3 ACL advanced settings" on page 598.

Editing a service group

You can access the **Service** dialog box when configuring an extended L3 ACL device configuration. To configure an extended L3 ACL, refer to one of the following procedures:

- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an IPv6 L3 ACL configuration" on page 592
- "Copying an IPv6 L3 ACL configuration" on page 593

To edit a service, complete the following steps.

1. Click the **Service Groups** tab.
2. Select the service group you want to edit and click **Edit**.

    The **Edit Service Group** dialog box displays.
3. To enter a range of ports, complete the following steps.
    a. Enter the starting port number in the **Start Port** field.
    b. Enter the ending port number in the **End Port** field.
    c. Click the right arrow button to move the address range to the **Selected** table.
4. To add a service to the group, complete the following steps.
    a. Select one or more services to add to the group in the Services table.
    b. Click the right arrow button to move the selected services to the **Selected** table.
5. To add a service group to the group, complete the following steps.
    a. Select one or more service groups to add to the group in the Services table.
    b. Click the right arrow button to move the selected service groups to the **Selected** table.

6. Click **OK** on the **Edit Service Group** dialog box.

   The **Service** dialog box, **Service Group** tab displays with the new group in the **List of Service Groups** table.

7. Click **Close** on the **Service** dialog box.

   To finish configuring the advanced settings for the ACL, refer to "Configuring L3 ACL advanced settings" on page 598.

Copying a service group

You can access the **Service** dialog box when configuring an extended L3 ACL device configuration. To configure an extended L3 ACL, refer to one of the following procedures:

- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an IPv6 L3 ACL configuration" on page 592
- "Copying an IPv6 L3 ACL configuration" on page 593

To copy a service, complete the following steps.

1. Click the **Service Groups** tab.
2. Select the service group you want to copy and click **Duplicate**.

   The **Duplicate Service Group** dialog box displays.

3. Enter a name for the service group in the **Name** field.
4. To enter a range of ports, complete the following steps.
   a. Enter the starting port number in the **Start Port** field.
   b. Enter the ending port number in the **End Port** field.
   c. Click the right arrow button to move the address range to the **Selected** table.
5. To add a service to the group, complete the following steps.
   a. Select one or more services to add to the group in the Services table.
   b. Click the right arrow button to move the selected services to the **Selected** table.
6. To add a service group to the group, complete the following steps.
   a. Select one or more service groups to add to the group in the Services table.
   b. Click the right arrow button to move the selected service groups to the **Selected** table.
7. Click **OK** on the **Duplicate Service Group** dialog box.

   The **Service** dialog box, **Service Group** tab displays with the new group in the **List of Service Groups** table.

8. Click **Close** on the **Service** dialog box.

   To finish configuring the advanced settings for the ACL, refer to "Configuring L3 ACL advanced settings" on page 598.

Deleting a service group

You can access the **Service** dialog box when configuring an extended L3 ACL device configuration. To configure an extended L3 ACL, refer to one of the following procedures:

- "Creating an extended L3 ACL configuration" on page 585
- "Editing an extended L3 ACL configuration" on page 587
- "Copying an extended L3 ACL configuration" on page 588
- "Creating an extended L3 ACL configuration" on page 585
- "Editing an IPv6 L3 ACL configuration" on page 592
- "Copying an IPv6 L3 ACL configuration" on page 593

To delete one or more services, complete the following steps.

1. Click the **Service Groups** tab.
2. Select one or more services that you want to delete and click **Delete**.
3. Click **Yes** on the confirmation message.
4. Click **Close** on the **Service** dialog box.

   To finish configuring the advanced settings for the ACL, refer to "Configuring L3 ACL advanced settings" on page 598.

Media Access Control (MAC) filter management

The Media Access Control (MAC) layer controls the movement of data packets to and from one computer to another across a network. Security Management enables you to filter access based on the MAC layer headers in the Ethernet frame.

You can only configure MAC filters on the following IronWare devices:

- Ethernet Layer 2/L3 Edge switch (FastIron CX)
- Ethernet Layer 2/L3 Access switch (FastIron GS)
- Enterprise LAN switch (FastIron LS)
- Enterprise LAN chassis (FastIron SX)
- Enterprise LAN Edge switch (FastIron Edge X)
- Data Center switch (TurboIron)
- Application product (ServerIron (SI) – SI-4G-SSL)

NOTE
If you add an unsupported device to the security configuration, the Management application skips the unsupported devices during deployment.

You can configure a MAC filter to forward or drop incoming packets using the following criteria:

- Source MAC address
- Destination MAC address
- Encapsulation type and Ethertype

You can configure and manage MAC filters at the device or interface (port/trunk) level.

NOTE
You can only apply MAC filters inbound traffic.

When you configure MAC filters on a device, the MAC filter does not execute until you deploy it on an interface. Once deployed to an interface, the device performs the action associated with the first matching filter (of all filters deployed to the device) to the packet. If the packet does not match any of the filters deployed on the interface, the device drops the packet.

You can only apply MAC filters to physical ports and trunks. If you apply a MAC filter to a trunk, you must apply the MAC filter to the primary port of the trunk.

NOTE
You cannot apply a MAC filter to a virtual interface.

Creating a MAC filter configuration

To create a MAC filter configuration, complete the following steps.

1. Select **Configure > Security > MAC Filter > Product**.

   The *Device_Name* - **MAC Filter Configuration** dialog box displays.

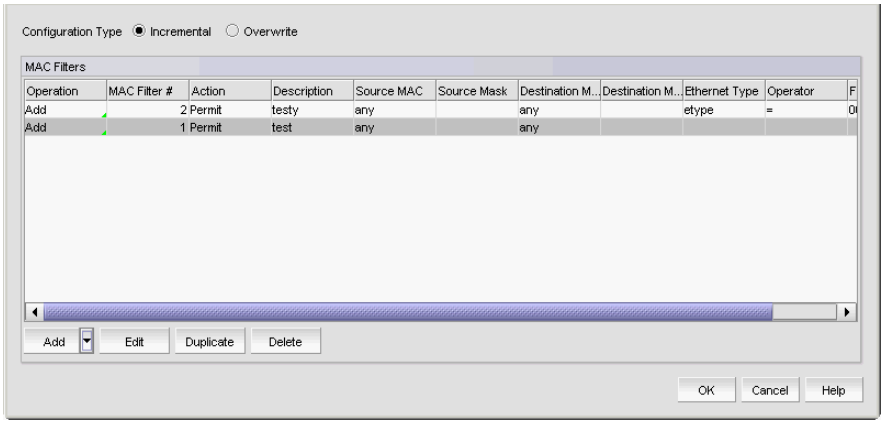


FIGURE 231 ***Device_Name*** **- MAC Filter Configuration dialog box**

2. Select **New** from the **Add** list.

   The **Add MAC Filter** dialog box displays.

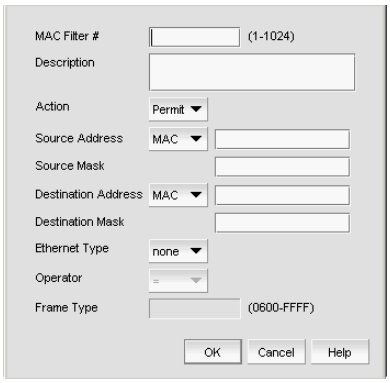


FIGURE 232 Add MAC Filter dialog box

3. Enter a MAC filter number in the **MAC Filter #** field.

   MAC filter numbers range from 1 through 1024.

4. (Optional) Enter a description of the MAC filter in the **Description** field.

   The description is saved to the Management application database only. It is not saved to the switch.

5. Select **Permit** or **Deny** from the Action list.

6. In the **Source Address** list, select one of the following options:

   - Any
   - MAC

     Selecting MAC enables the **Source Address** and **Source Mask** fields.

     a. Enter the source MAC address on which the configuration filters traffic in the **Source Address** field.

     b. Enter the mask associated with the source MAC address in the **Source Mask** field.

7. In the **Destination Address** list, select one of the following options:

   - Any
   - MAC

     Selecting MAC enables the **Destination Address** and **Destination Mask** fields.

     a. Enter the destination MAC address on which the configuration filters traffic in the **Destination Address** field.

     b. Enter the mask associated with the destination MAC address in the **Destination Mask** field.

8. In the **Ethernet Type** list, select one of the following to specify the Ethernet type being transferred in the Ethernet frame:

   - **etype** — EtherType
   - **llc** — IEEE 802.2 Logical Link Control
   - **snap** — Subnetwork Access Protocol
   - **none** — no type

9. In the **Operator** list, select one of the following to specify a binary operator:
   - **=** (equal to)
   - **!=** (not equal to)
   - **>** (greater than)
   - **<** (less than).

   This field is not available when the **Ethernet Type** is none.

10. Enter the type of frame in the **Frame Type** field.

    This ia 2 byte hexadecimal value. Valid values include 0600 to FFFF. This field is not available when the **Ethernet Type** is none.

11. Click **OK** on the **Add MAC Filter** dialog box.

    The new MAC filter displays in the **MAC Filters** table. To create additional MAC filters, repeat step 2 through step 11.

12. Click **OK** on the *Device_Name* - **MAC Filter Configuration** dialog box displays.

    The **Deploy to Products - MAC Filter** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Creating a MAC filter from a saved configuration

To create a MAC filter configuration from a saved configuration objects, complete the following steps.

1. Select **Configure > Security > MAC Filter > Product**.

   The *Device_Name* - **MAC Filter Configuration** dialog box displays.

2. Select **From Saved Configurations** from the **Add** list.

   The **MAC Filter Saved Configurations** dialog box displays.

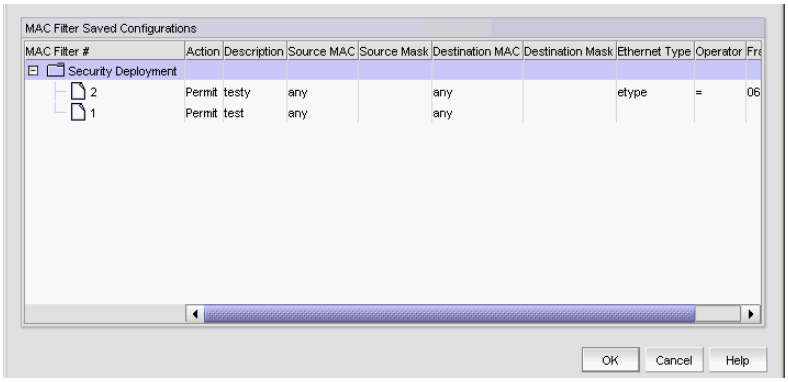


FIGURE 233 MAC Filter Saved Configurations dialog box

3. Select one or more objects from the **MAC Filter Saved Configurations** table.

   You can select one or more MAC filters, one or more saved deployment configurations, or a combination of both.

4. Click **OK** on the **MAC Filter Saved Configurations** dialog box.

   The *Device_Name* - **MAC Filter Configuration** dialog box displays with the selected MAC filters in the **MAC Filters** table. If you selected a saved deployment configuration, all MAC filters associated with the saved deployment configuration display in the **MAC Filters** table.

5. Click **OK** on the *Device_Name* - **MAC Filter Configuration** dialog box.

   The **Deploy to Products - MAC Filter** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Editing a MAC filter

To edit a MAC filter configuration, complete the following steps.

1. Select **Configure > Security > MAC Filter > Product**.

   The *Device_Name* - **MAC Filter Configuration** dialog box displays.

2. Select the configuration you want to edit in the MAC Filters table and click **Edit**.

   The **Edit MAC Filter** dialog box displays.

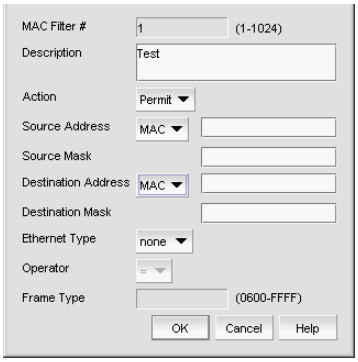


FIGURE 234 Edit MAC Filter dialog box

3. Change the description of the MAC filter in the **Description** field.
4. Select **Permit** or **Deny** from the Action list.
5. In the **Source Address** list, select one of the following options:
   - Any
   - MAC

     Selecting MAC enables the **Source Address** and **Source Mask** fields.

     a. Enter the source MAC address on which the configuration filters traffic in the **Source Address** field.

     b. Enter the mask associated with the source MAC address in the **Source Mask** field.

6. In the **Destination Address** list, select one of the following options:
   - Any
   - MAC

     Selecting MAC enables the **Destination Address** and **Destination Mask** fields.

     a. Enter the destination MAC address on which the configuration filters traffic in the **Destination Address** field.

     b. Enter the mask associated with the destination MAC address in the **Destination Mask** field.
7. In the **Ethernet Type** list, select one of the following to specify the Ethernet type being transferred in the Ethernet frame:
   - **etype** — EtherType
   - **llc** — IEEE 802.2 Logical Link Control
   - **snap** — Subnetwork Access Protocol
   - **none** — no type
8. In the **Operator** list, select one of the following to specify a binary operator:
   - **=** (equal to)
   - **!=** (not equal to)
   - **>** (greater than)
   - **<** (less than).

   This field is not available when the **Ethernet Type** is none.
9. Enter the type of frame in the **Frame Type** field.

   This ia 2 byte hexadecimal value. Valid values include 0600 to FFFF. This field is not available when the **Ethernet Type** is none.
10. Click **OK** on the **Edit MAC Filter** dialog box.

    The updated MAC filter displays in the **MAC Filters** table.
11. Click **OK** on the *Device_Name* - **MAC Filter Configuration** dialog box displays.

    The **Deploy to Products - MAC Filter** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Copying a MAC filter

To copy a MAC filter configuration, complete the following steps.

1. Select **Configure > Security > MAC Filter > Product**.

   The *Device_Name* - **MAC Filter Configuration** dialog box displays.
2. Select the configuration you want to copy in the MAC Filters table and click **Duplicate**.

   The **Duplicate MAC Filter** - *MAC_Filter_Number* dialog box displays.
3. Enter a MAC filter number in the **MAC Filter #** field.

   MAC filter numbers range from 1 through 1024.

4. Enter a description of the MAC filter in the **Description** field.
5. Select **Permit** or **Deny** from the Action list.
6. In the **Source Address** list, select one of the following options:
   - Any
   - MAC

     Selecting MAC enables the **Source Address** and **Source Mask** fields.

     a. Enter the source MAC address on which the configuration filters traffic in the **Source Address** field.

     b. Enter the mask associated with the source MAC address in the **Source Mask** field.
7. In the **Destination Address** list, select one of the following options:
   - Any
   - MAC

     Selecting MAC enables the **Destination Address** and **Destination Mask** fields.

     a. Enter the destination MAC address on which the configuration filters traffic in the **Destination Address** field.

     b. Enter the mask associated with the destination MAC address in the **Destination Mask** field.
8. In the **Ethernet Type** list, select one of the following to specify the Ethernet type being transferred in the Ethernet frame:
   - **etype** — EtherType
   - **llc** — IEEE 802.2 Logical Link Control
   - **snap** — Subnetwork Access Protocol
   - **none** — no type
9. In the **Operator** list, select one of the following to specify a binary operator:
   - **=** (equal to)
   - **!=** (not equal to)
   - **>** (greater than)
   - **<** (less than).

   This field is not available when the **Ethernet Type** is none.
10. Enter the type of frame in the **Frame Type** field.

    This ia 2 byte hexadecimal value. Valid values include 0600 to FFFF. This field is not available when the **Ethernet Type** is none.
11. Click **OK** on the **Duplicate MAC Filter** - *MAC_Filter_Number* dialog box.

    The new MAC filter displays in the **MAC Filters** table.
12. Click **OK** on the *Device_Name* - **MAC Filter Configuration** dialog box.

    The **Deploy to Products - MAC Filter** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Deleting a MAC filter

1. Select **Configure > Security > MAC Filter > Product**.

   The *Device_Name* - **MAC Filter Configuration** dialog box displays.

2. Select the MAC filter you want to delete in the **MAC Filters** table and click **Delete**.
3. Click **Yes** on the confirmation message.
4. Click **OK** on the *Device_Name* - **MAC Filter Configuration** dialog box.

NOTE
The MAC Filter is not deleted from the switch until you deploy the configuration to the switch.

The **Deploy to Products - MAC Filter** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 631

Assigning MAC filters

To assign a MAC filter configuration to a port or product, complete the following steps.

1. Select **Configure > Security > MAC Filter > Port**.

   The **Port Selection - MAC Filter** dialog box displays.

2. Select the port you want to add to the MAC filter in the **Available Ports** list and click the right arrow button.
3. Click **OK** on the **Port Selection - MAC Filter** dialog box.

   The *Device_Name* - *Port_Number* - **MAC Filter Configuration** dialog box displays.

4. Select the **Assign MAC Filter** option.
5. Choose one of the following options from the first list:
   - **MAC Filters bound to this interface** — Select to assign an ACL deployment saved on the port.
   - **From the Product** — Select to assign an MAC filter deployment saved on the product.
   - *Deployment_Name* — Select to assign a user-configured deployment on the port.
6. Select the MAC filter number from the second list.
7. Click **Add**.

   The MAC filter you selected displays in the **MAC Filters** table. Repeat step 5 through step 7 for each MAC filter you want to assign to the product or port.

8. Click OK on the *Device_Name* - *Port_Number* - **MAC Filter Configuration** dialog box.

   The **Deploy to Ports - MAC Filter** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Clearing MAC filter assignments

To clear a MAC filter assignment from a port or product, complete the following steps.

1. Select **Configure > Security > MAC Filter > Port**.

   The **Port Selection - MAC Filter** dialog box displays.

2. Select the port you want to clear the MAC filter from in the **Available Ports** list and click the right arrow button.

   You can select more ports or products from the **Deploy to Ports - MAC Filter** dialog box.

3. Click **OK** on the **Port Selection - MAC Filter** dialog box.

   The *Device_Name - Port_Number* - **MAC Filter Configuration** dialog box displays.

4. Select the **Clear MAC Filter Assignment** option.

5. Click **OK** on the *Device_Name - Port_Number* - **MAC Filter Configuration** dialog box.

   The **Deploy to Ports - MAC Filter** dialog box displays. To deploy the configuration, refer to "Deploying a security configuration on demand" on page 630.

Adding a MAC filter configuration to an interface

To add a MAC filter configuration to an interface, complete the following steps.

1. Select **Configure > Security > MAC Filter > Port**.

   The **Port Selection - MAC Filter** dialog box displays.

2. Select the port or trunk you want to add to the MAC filter in the **Available Ports** list and click the right arrow button.

3. Click **OK** on the **Port Selection - MAC Filter** dialog box.

   The *Device_Name - Port_Number* - **MAC Filter Configuration** dialog box displays.

4. Select the **Assign MAC Filter** option.

5. Choose one of the following options from the first list:

   - **MAC Filters bound to this interface** — Select to assign an ACL deployment saved on the port.
   - **From the Product** — Select to assign an MAC filter deployment saved on the product.
   - *Deployment_Name* — Select to assign a user-configured deployment on the port.

6. Select the MAC filter number from the second list.

7. Click **Add**.

   The MAC filter you selected displays in the **MAC Filters** table. Repeat step 5 through step 7 for each MAC filter you want to assign to the port.

8. Click OK on the *Device_Name - Port_Number* - **MAC Filter Configuration** dialog box.

   The **Deploy to Ports - MAC Filter** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 629.

Security configuration deployment

Figure 235 shows the standard interface used to deploy security configurations.

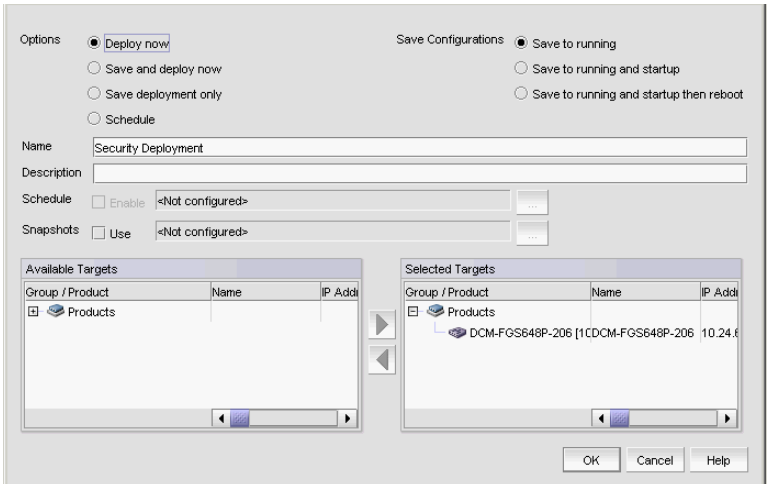


FIGURE 235 Deploy to Product/Ports dialog box

Before you can deploy a security configuration, you must create the security configuration. For step-by-step instructions, refer to the following sections:

- "Layer 2 access control list management" on page 561
- "Layer 3 access control list policy" on page 580
- "Media Access Control (MAC) filter management" on page 620

Security Management enables you to configure, persist, and manage a security configuration as a "deployment configuration object". A deployment configuration object is comprised of the following parts:

- Security configuration (Layer 2 ACL, L3 ACL, or MAC filter)
- Target information
- Deployment option
- Persistence option
- Scheduling option
- Snapshot option

To create a deployment configuration object, you must save the deployment. Once you create a deployment configuration object, you can access the security configuration from the Deployment manager. For more information about the Deployment manager, refer to "Deployment Manager" on page 963.

Deploying a security configuration on demand

To deploy a security configuration immediately, complete the following steps.

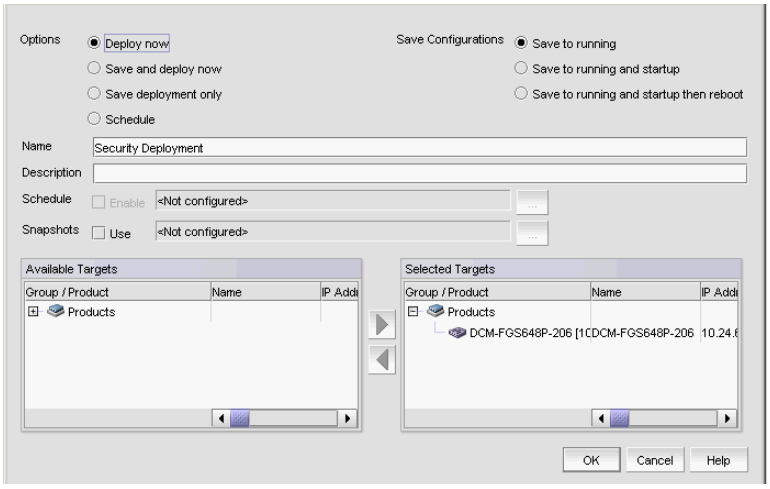


FIGURE 236 Deploy to Product/Ports dialog box

1. Choose one of the following options:
   - **Deploy now** — Select to deploy the configuration immediately on the product or port without saving the deployment definition.
   - **Save and deploy now** — Select to deploy the configuration immediately on the product or port and save the deployment definition for future deployment.
2. Select one of the following save configuration options:
   - **Save to running** — Select to update the running configuration; however, the deployment is not saved to the product's flash memory.
   - **Save to running and startup** — Select to update the running configuration as well as save the deployment configuration to the product's flash memory. Selecting this option is the equivalent to a write memory command on the product CLI.
   - **Save to running and startup then reboot** — Select to update the running configuration, save the deployment configuration to the product's flash memory, and reboot the product. Selecting this option is the equivalent to entering a write memory and a reload command on the product CLI.
3. Enter a name for the deployment in the **Name** field.
4. Enter a description for the deployment in the **Description** field.
5. Click the **Snapshot Use** check box and click the ellipsis button to select the product monitoring template.

   NOTE
   The **Snapshot Use** check box is only available for IronWare products.

   The **Pre-Post Snapshot Properties** dialog box displays.
6. Select the product monitoring template you want to use from the **CLI Template** list.
7. Select one or more of the following to capture snapshots:

- Select the **Pre-deployment** check box to capture a snapshot of the product's configuration prior to deployment of the security configuration.
- Select the **Post-deployment** check box to capture a snapshot of the product's configuration after deployment of the security configuration.

  If you select the **Post-deployment** check box, enter the amount of time (between 1 and 300 seconds) you want the application to wait before capturing the snapshot in the **Delay** field.

8. Select one or more ports or products to which you want to deploy the configuration in the **Available Targets** list and click the right arrow button to move them to the **Selected Targets** list.
9. Click **OK** on the **Deploy to Products - Layer 2 ACL** dialog box.

Saving a security configuration deployment

To save a security configuration deployment, complete the following steps.

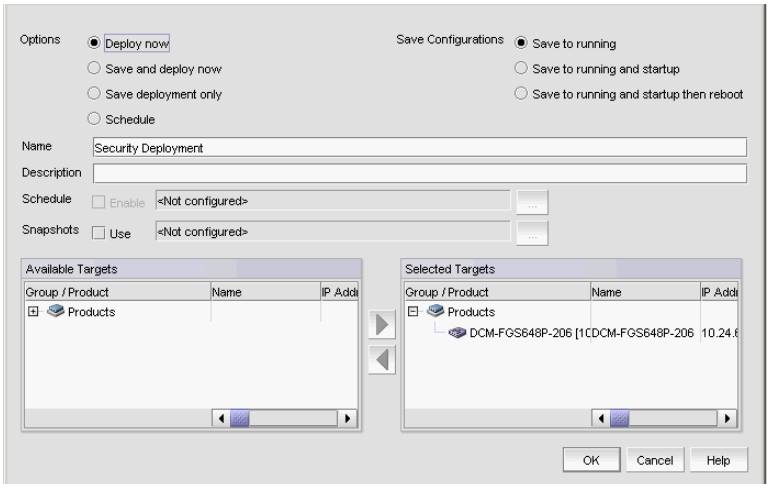


FIGURE 237 Deploy to Product/Ports dialog box

1. Select the **Save deployment only** option to save the deployment definition for future deployment.
2. Select one of the following save configuration options:
   - **Save to running** — Select to update the running configuration; however, the deployment is not saved to the product's flash memory.
   - **Save to running and startup** — Select to update the running configuration as well as save the deployment configuration to the product's flash memory. Selecting this option is the equivalent to a write memory command on the product CLI.
   - **Save to running and startup then reboot** — Select to update the running configuration, save the deployment configuration to the product's flash memory, and reboot the product. Selecting this option is the equivalent to entering a write memory and a reload command on the product CLI.
3. Enter a name for the deployment in the **Name** field.
4. Enter a description for the deployment in the **Description** field.

5. Click the **Snapshot Use** check box and click the ellipsis button to select the product monitoring template.

NOTE
The **Snapshot Use** check box is only available for IronWare products.

The **Pre-Post Snapshot Properties** dialog box displays.

6. Select the product monitoring template you want to use from the **CLI Template** list.
7. Select one or more of the following to capture snapshots:
   - Select the **Pre-deployment** check box to capture a snapshot of the product's configuration prior to deployment of the security configuration.
   - Select the **Post-deployment** check box to capture a snapshot of the product's configuration after deployment of the security configuration.

     If you select the **Post-deployment** check box, enter the amount of time (between 1 and 300 seconds) you want the application to wait before capturing the snapshot in the **Delay** field.
8. Select one or more ports or products to which you want to deploy the configuration in the **Available Targets** list and click the right arrow button to move them to the **Selected Targets** list.
9. Click **OK** on the **Deploy to Products - Layer 2 ACL** dialog box.

Scheduling a security configuration deployment

To schedule a security configuration deployment, complete the following steps.

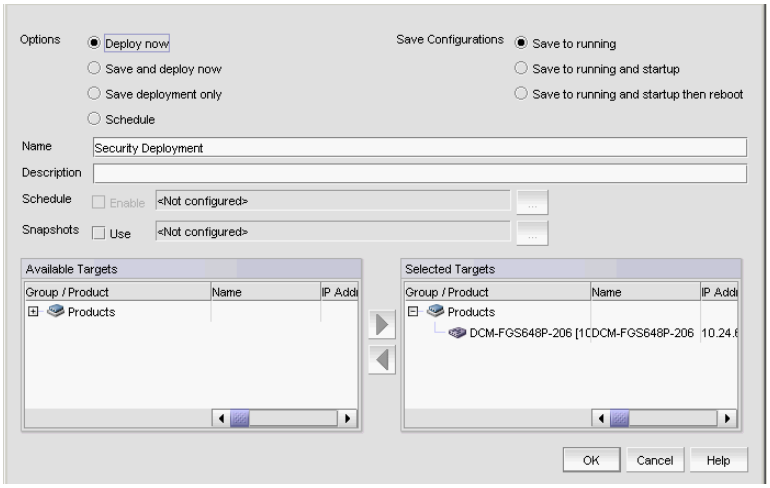


FIGURE 238 Deploy to Product/Ports dialog box

1. Select **Configure > Security > Layer 2 ACL > Product**.

   The *Device_Name* - **Layer 2 ACL Configuration** dialog box displays.

2. Choose one of the following options:
   - Select **New** from the **Add** list.

     The **Add - Layer 2 ACL Configuration** dialog box displays.
   - Select an ACL in the list and click **Edit**.

     The **Edit - Layer 2 ACL Configuration** dialog box displays.
3. Configure the Layer 2 ACL and click **OK** on the **Add/Edit - Layer 2 ACL Configuration** dialog box.
4. Click **OK** on the *Device_Name* **- Layer 2 ACL Configuration** dialog box.

   The **Deploy to Products - Layer 2 ACL** dialog box displays.
5. Select the **Schedule** option.
6. Select one of the following save configuration options:
   - Save to running
   - Save to running and startup
   - Save to running and startup then reboot
7. Enter a name for the deployment in the **Name** field.
8. Enter a description for the deployment in the **Description** field.
9. Click the **Schedule Enable** check box and click the ellipsis button to schedule deployment.

   The **Schedule Properties** dialog box displays.
10. Choose one of the following options to configure the frequency at which deployment runs for the schedule:
    - To configure deployment to run only once, refer to "Configuring a one-time deployment schedule" on page 634.
    - To configure hourly deployment, refer to "Configuring an hourly deployment schedule" on page 634.
    - To configure daily deployment, refer to "Configuring a daily deployment schedule" on page 634.
    - To configure weekly deployment, refer to "Configuring a weekly deployment schedule" on page 634.
    - To configure monthly deployment, refer to "Configuring a monthly deployment schedule" on page 635.
11. Click **OK** on the **Schedule Properties** dialog box.
12. Click the **Snapshot Use** check box and click the ellipsis button to select the product monitoring template.

    NOTE
    The **Snapshot Use** check box is only available for IronWare products.

    The **Pre-Post Snapshot Properties** dialog box displays.
13. Select one or more ports or products to which you want to deploy the configuration in the **Available Targets** list and click the right arrow button to move them to the **Selected Targets** list.
14. Click **OK** on the **Deploy to Products - Layer 2 ACL** dialog box.

Configuring a one-time deployment schedule

To configure a one-time schedule, complete the following steps.

1. Select **One Time** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
3. Click the **Date** list to select a date from the calendar.

   To configure security configuration schedule, refer to step 11 of "Scheduling a security configuration deployment" on page 632.

Configuring an hourly deployment schedule

To configure an hourly schedule, complete the following steps.

1. Select **Hourly** from the **Frequency** list.
2. Select the minute past the hour you want deployment to run from the **Minutes past the hour** list.

   Where the minute value is from 00 through 59.

   To configure security configuration schedule, refer to step 11 of "Scheduling a security configuration deployment" on page 632.

Configuring a daily deployment schedule

To configure a daily deployment schedule, complete the following steps.

1. Select **Daily** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

   To configure security configuration schedule, refer to step 11 of "Scheduling a security configuration deployment" on page 632.

Configuring a weekly deployment schedule

To configure a weekly schedule, complete the following steps.

1. Select **Weekly** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
3. Select the day you want deployment to run from the **Day of the Week** list.

   To configure security configuration schedule, refer to step 11 of "Scheduling a security configuration deployment" on page 632.

Configuring a monthly deployment schedule

To configure a monthly schedule, complete the following steps.

1. Select **Monthly** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
3. Select the day you want deployment to run from the **Day of the Month** list (1 through 31).

   To configure security configuration schedule, refer to step 11 of "Scheduling a security configuration deployment" on page 632.

Chapter

19

Zoning

In this chapter

Zoning overview

Zoning is a fabric-based service that enables you to partition your network into logical groups of devices that can access each other and prevent access from outside the group. Grouping devices into zones in this manner not only provides security, but also relieves the network from Registered State Change Notification (RSCN) storms that occur when too many native FCoE devices attempt to communicate with one another.

You can use zoning to partition your network in many ways. For example, you can partition your network into two zones, *winzone* and *unixzone*, so that your Windows servers and storage do not interact with your UNIX servers and storage. You can use zones to logically consolidate equipment for efficiency or to facilitate time-sensitive functions; for example, you can create a temporary zone to back up nonmember devices.

A device in a zone can communicate only with other devices connected to the fabric within the same zone. A device not included in the zone is not available to members of that zone. When zoning is enabled, devices that are not included in *any* zone configuration are inaccessible to all other devices in the fabric.

Zones can be configured dynamically. They can vary in size, depending on the number of fabric-connected devices, and devices can belong to more than one zone.

Consider Figure 239, which shows configured zones, Red, Green, and Blue.

- Server 1 can communicate only with the Storage 1 device.
- Server 2 can communicate only with the RAID and Storage 2 devices.
- Server 3 can communicate with the RAID and Storage 1 devices.
- The Storage 3 device is not assigned to a zone; no other zoned fabric device can access it.

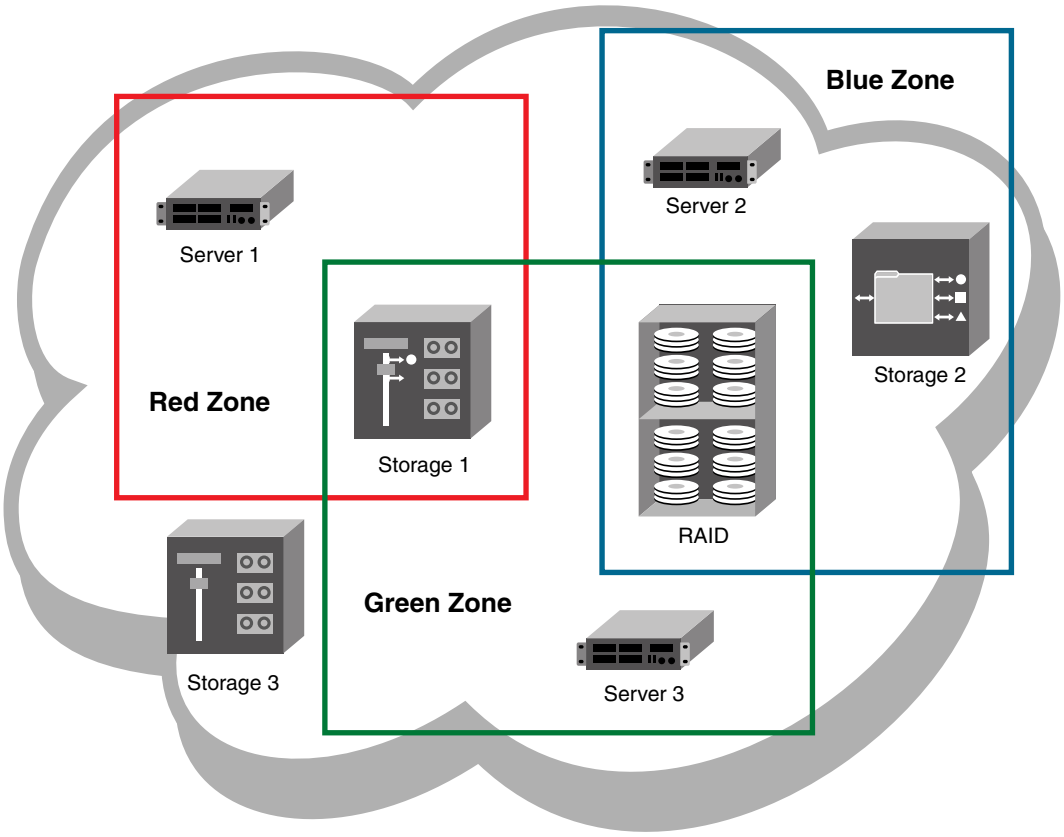


FIGURE 239 Zoning

NOTE
A Network OS fabric supports zoning only if all devices in the fabric are running Network OS v2.1.0 or later.

NOTE
Zone objects based on physical port number or port ID (D,I ports) are not supported in Network OS fabrics.

Online zoning

Online zoning allows you to do the following:

- View both defined and active zone information in the fabric.
- Create and modify zones and zone configurations in the software zone database.
- Activate a zone configuration in order to publish the zone information in the selected fabric.
- Deactivate the current active zone configuration.
- Configure zoning policies in the selected fabric.
- Generate zoning reports for the fabric.

Offline zoning

Offline zoning is supported in Network OS fabrics.

Offline zoning is supported in Network OS and Fabric OS fabrics.

NOTE
Offline zoning is available only for Enterprise and Professional Plus editions.

Offline zoning enables you to copy a fabric zone database and edit it offline. The benefits to offline zoning include the following:

- You want to make changes to the zone database now, but apply them later.

  For example:

  - If you make incremental changes to zoning on an ongoing basis, but want to apply the changes to the fabric during scheduled downtime.
  - If you are expecting new servers to be delivered, but want to make changes to zoning now and apply the changes after the servers are delivered and ready to go online.
- You want to keep multiple copies of the zone database and switch between them.

  For example, if you want to allow specific servers access to tape drives for backup during specific time windows, you can have multiple zone databases (one or more for backup and one for normal operation) and switch between them easily.
- You want to analyze the impact of changes to storage access before applying the changes.

  For example, if you deploy a new server and want to ensure that the zoning changes result in only the new server gaining access to specific storage devices and nothing else. Refer to "Comparing zone databases" on page 662.

Zoning naming conventions

The naming rules for zone names, zone aliases, and zone configuration names vary with the type of fabric. The following conventions apply:

- Names must start with an alphabetic character and may contain alphanumeric characters and the underscore (_) character.
- Names are not case-sensitive.
- Zone, alias, and configuration names cannot begin with "bfa_","red_", "lsan_red_", or "d__efault__". Zone configuration names cannot begin with "r_e_d_i_r_c__fg". These prefixes are reserved.
- Names cannot begin with a numeric character or a special character.
- The recommended character limit is 64 characters.
- Duplicate names are not allowed between zones, zone aliases, and zone configurations within a zone database.

If you enter an invalid zone or zone configuration name, an error or warning message displays depending on the type of fabric you are trying to zone.

Zone database size

The supported maximum zone database size is 1 MB.

If the fabric contains only Backbone Chassis platforms, the supported maximum zone database size is 2 MB.

NOTE
Network OS recommends a maximum zone database size of 150 KB. As the size of the zone database increases, performance decreases.

The Professional Edition does not support large zone databases. In the Professional Edition, the maximum size of the zone database without zone aliases is 32 KB. If the zone database contains aliases, the maximum size is less than 32 KB.

Zoning configuration

At a minimum, zoning configuration entails creating zones and zone members. However, you can also create zone aliases, zone configurations and zone databases. You can define multiple zone configurations, deactivating and activating individual configurations as your needs change. Zoning configuration can also involve enabling or disabling the default zone.

Configuring zoning

The following procedure provides an overview of the steps you must perform to configure zoning.

Note that for any zoning-related procedure, changes to a zone database are not saved until you click **OK** or **Apply** on the **Zoning** dialog box. If you click **Cancel** or the close button (X), no changes are saved.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. If you want to show all the discovered fabrics in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.
5. Create the zones.

   For specific instructions, refer to "Creating a zone" on page 641.

6. Add members to each zone.

   For specific instructions, refer to "Adding members to a zone" on page 642.

7. Create a zone configuration.

   For specific instructions, refer to "Creating a zone configuration" on page 650.

8. Activate the zone configuration.

For specific instructions, refer to "Activating a zone configuration" on page 652.

9. Set zoning policies, if necessary.

   For specific instructions, refer to "Enabling or disabling the default zone for fabrics" on page 646.

10. Click **OK** or **Apply** to save your changes.

    Any zones or zone configurations you have changed are saved in the zone database.

Creating a zone

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Click **New Zone**.

   A new zone displays in the **Zones** list.

5. Type the name for the zone.

   For zone name requirements and limitations, refer to "Zoning naming conventions" on page 639.

The new, empty zone is created. You cannot save an empty zone. Refer to "Adding members to a zone" on page 642 for instructions on adding members and saving the zone.

Viewing zone properties

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the zone you want to review in the **Zones** list and select **Properties**.

   The **Zone Properties** dialog box displays.

5. Review the zone properties.

   Note that when any modifications are made to an active zone, the **Zone Properties** dialog box continues to show the status as Active until the changes are saved to the zone database.

   You can change the zone name by double-clicking the name and then modifying the name in the editable field.

6. Click **OK** to close the **Zone Properties** dialog box.

Adding members to a zone

Use this procedure to add a member to a zone when the member is listed in the **Potential Members** list of the **Zone DB** tab.

Enterprise and Professional Plus editions: For instructions to add a member to a zone when the member is not listed in the **Potential Members** list, refer to the procedure "Creating a member in a zone" on page 643.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

   If you want to show all the discovered fabrics in your fabric group in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.

4. Select one or more zones to which you want to add members in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)
5. Select an option from the **Type** list.

   By default, the first time you launch the **Zoning** dialog box for a zoning scope, the **Potential Members** list displays valid members using the following rules:

   - If you select the **WWN** type, the valid members display by the Attached Ports.
   - If you select the **Alias** type, the valid members display by the device Alias.

6. Select one or more members to add to the zone in the **Potential Members** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member. To add all ports on a device, select the device.)

   You cannot add duplicate members to the same zone.

7. Click the right arrow between the **Potential Members** list and **Zones** list to add the selected members to the zone.

   A message is displayed if unsupported potential members are moved to the **Zones** list. Click **OK** to close the message box. Reconsider your selections and make corrections as appropriate.

8. For offline zone databases only, complete the following steps to save the zone configuration into the switch from the offline zone database:

   a. Select **Save to Switch** from the **Zone DB Operation** list.

   b. Click **Yes** on the confirmation message.

      The selected zone database is saved to the fabric without enabling a specific zone configuration.

9. Click **OK** or **Apply** to save your changes.

   Any zones or zone configurations you have changed are saved in the zone database.

Creating a member in a zone

Use this procedure to add a member to a zone when the member is not listed in the **Potential Members** list of the **Zone DB** tab.

For instructions to add a member to a zone when the member is listed in the **Potential Members** list, refer to the procedure "Adding members to a zone" on page 642.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zones to which you want to add members in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)

5. Click **New Member**.

   The **Add Zone Member** dialog box displays.

6. Select an option from the **Member Type** list.

   The fields in the dialog box vary based on the **Member Type** option you select.

7. Fill in the remaining fields in the dialog box.

   Click the **Help** button for additional information on each field.

8. Click **OK** to save your changes and close the **Add Zone Member** dialog box.

   OR

   Click **Apply** to save your changes and keep the **Add Zone Member** dialog box open so you can add more new members. Repeat step 5 through step 8 as many times as needed, and proceed to step 9 when appropriate.

9. For offline zone databases only, complete the following steps to save the zone configuration into the switch from the offline zone database:

   a. Select **Save to Switch** from the **Zone DB Operation** list.

   b. Click **Yes** on the confirmation message.

      The selected zone database is saved to the fabric without enabling a specific zone configuration.

10. Click **OK** or **Apply** to save your changes.

    Any zones or zone configurations you have changed are saved in the zone database.

Removing a member from a zone

Use the following procedure to remove one or more members from a zone or zones. Note that the member is not deleted; it is only removed from the zone.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Click the plus sign (+) by the appropriate zone in the **Zones** list to expand the listing and show the zone's members.
5. Perform one of the following actions:
   - Right-click the name of the zone member you want to remove in the **Zones** list and select one of the following options from the shortcut menu that displays:
     - **Remove** - To remove the zone member from the selected zone.
     - **Remove All** - To remove the zone member from all zones to which it belongs.
   - To remove multiple zone members, select the members to be removed from the zone, and click the left arrow between the **Potential Members** list and the **Zones** list.

   When successful, the zone member is removed from the **Zones** list.
6. Click **OK** or **Apply** to save your changes.

   Any zones or zone configurations you have changed are saved in the zone database.

Renaming a zone

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Right-click the name of the zone you want to change in the **Zones** list and select **Rename**.
5. Type the new name for the zone.

   For zone name requirements and limitations, refer to "Zoning naming conventions" on page 639.
6. Press **Enter** to save the new name.

   For Network OS fabrics, if an invalid name is entered for a zone or zone configuration, the application displays a warning message. If there is a naming violation according to the vendor, the switch returns the error message for the exact information along with the zone configuration activation failure message.
7. Click **OK** or **Apply** to save your changes.

   Any zones or zone configurations you have changed are saved in the zone database.

Deleting a zone

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zones in the **Zones** list that you want to delete, then right-click and select **Delete**.

   A message displays asking you to confirm the deletion.

5. Click **Yes** to delete the selected zones.

   The message closes and the zone or zones are removed from the **Zones** list.

   NOTE
   If you delete something in error, click **Cancel** on the **Zoning** dialog box to exit without saving changes. When you reopen the dialog box, the zone is restored.

6. Click **OK** or **Apply** to save your changes.

   Any zones or zone configurations you have changed are saved in the zone database.

Duplicating a zone

When you duplicate a zone, you make a copy of it in the same zone database. The first time a zone is duplicated, the duplicate is automatically given the name <*zonelabel*>*_copy*. On subsequent duplications, a sequential number is assigned to the zone name, such as <*zonelabel*>*_copy_1*, <*zonelabel*>*_copy_2,* and <*zonelabel*>*_copy_3*.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zones in the **Zones** list that you want to duplicate, then right-click and select **Duplicate**.

   The duplicated zone or zones display in the **Zones** list.

5. (*Optional*) Type a new name for the zone and press **Enter** to save the name.

   Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors. Click **OK** and enter a different name or accept the default name assigned to the zone. (For zone name requirements and limitations, refer to "Zoning naming conventions" on page 639.)

6. Click **OK** or **Apply** to save your changes.

   Any zones or zone configurations you have changed are saved in the zone database.

Customizing the zone member display

In the **Zoning** dialog box, you can customize which properties are displayed and in what order.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays, based on the **Configure > Zoning** menu selection.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Click the plus sign (+) by the appropriate zone in the **Zones** list to expand the listing and show the zone members.
5. Right-click the name of any zone member and select **Member Display**.

   The **Zone Member Display** dialog box displays.

6. Select or clear the check boxes for the properties you want to display or hide.

   All of the options are selected by default. You cannot clear the **WWN/Domain,Port Index** check box. It is always selected.

7. Select a property and click the **Up** or **Down** buttons to rearrange the order in which the properties are displayed.
8. Click **OK**.

   The display is changed for all zone members in the **Zones** list.

Enabling or disabling the default zone for fabrics

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zoning database you want from the **Zone DB** list.
5. Click **Zoning Policies**.

   The **Zoning Policies** dialog box displays.

6. Make sure the appropriate fabric is named on the **Zoning Policies** dialog box.
7. Perform one of the following actions based on the task you want to complete:
   - To enable the default zone, click **Enable**, and then click **OK**.
   - To disable the default zone, click **Disable**, and then click **OK**.

The **Zoning Policies** dialog box closes and the **Zone DB** tab displays.

8. Click **OK** or **Apply** to save your changes.

   Any zones or zone configurations you have changed are saved in the zone database.

Creating a zone alias

An alias is a logical group of port index numbers and WWNs. Specifying groups of ports or devices as an alias makes zone configuration easier by enabling you to configure zones using an alias rather than inputting a long string of individual members. You can specify members of an alias using the following methods:

- Identifying members by switch domain and port index (D,I) number pair.
- Identifying members by device node and device port WWNs.

Zone aliases are supported only in Network OS.

For Network OS, only device node and device port WWNs are supported as members of the zone alias. Network OS does not support D,I members.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.
4. Select **Alias** from the **Type** list.
5. Click **New Alias**.

   The **New Alias** dialog box displays.

6. Type a name for the alias in the **Alias Name** field.

   Refer to "Zoning naming conventions" on page 639 for rules about zone alias names.

7. (*Optional*) Show all discovered fabrics in the **Potential Members** list by right-clicking in the **Potential Members** list and selecting **Display All**.
8. Select one or more members that you want to add to the alias in the **Potential Members** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member.)

   You can also add WWNs not listed in the **Potential Members** list by entering the WWN in the **Detached WWN** field and clicking **Add**.

9. Click the right arrow between the **Potential Members** list and the **Selected Member(s)** list to add the selected members to the alias.
10. Click **OK** or **Apply** on the **New Alias** dialog box to save your changes.
11. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Editing a zone alias

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select a fabric from the **Zoning Scope** list.
4. Select **Alias** from the **Type** list.
5. Select the alias you want to edit in the **Alias** list and click **Edit**.

   The **Edit Alias** dialog box displays.
6. Add members to the alias by completing the following steps.
   a. Select an option from the **Type** list to choose how to display the objects in the **Potential Members** list.

      For Network OS fabrics, WWN is selected by default and cannot be changed.
   b. Show all discovered fabrics in the **Potential Members** list by right-clicking in the **Potential Members** list and selecting **Expand All**.
   c. Select one or more members that you want to add to the alias in the **Potential Members** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member.)

      You can also add WWNs not listed in the **Potential Members** list by entering the WWN in the **Detached WWN** field and clicking **Add**.
   d. Click the right arrow between the **Potential Members** list and the **Selected Member(s)** list to add the selected members to the alias.
7. Remove members from the alias by completing the following steps.
   a. Select one or more members that you want to remove from the alias in the **Selected Member(s)** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member.)
   b. Click the left arrow between the **Potential Members** list and the **Selected Member(s)** list to remove the selected members from the alias.
8. Click **OK** or **Apply** on the **Edit Alias** dialog box to save your changes.
9. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Removing an object from a zone alias

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.
4. Select **Alias** from the **Type** list.
5. Show all objects in the **Alias** list by right-clicking an object and selecting **Tree > Expand All**.
6. Select one or more objects that you want to remove from the alias in the **Alias** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member.)

   You can select objects from different zone aliases.
7. Right-click one of the selected objects and select **Remove.**

   The selected objects are removed from the associated zone aliases.
8. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Exporting zone aliases

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.
4. Select **Alias** from the **Type** list.
5. Click **Export.**

   The **Export Alias** dialog box displays.
6. Browse to the location to which you want to export the zone alias data.
7. Enter a name for the export file in the **File Name** field.
8. Click **Export Alias**.
9. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Renaming a zone alias

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.
4. Select **Alias** from the **Type** list.
5. Right-click the zone alias you want to rename and select **Rename.**
6. Edit the name and press **Enter**.

   Refer to "Zoning naming conventions" on page 639 for rules about zone alias names.
7. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Deleting a zone alias

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.
4. Select **Alias** from the **Type** list.
5. Right-click the zone alias you want to delete and select **Delete.**
6. Click **Yes** on the confirmation message.

   The selected zone alias is deleted from the **Alias** list.
7. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Duplicating a zone alias

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.
4. Select **Alias** from the **Type** list.
5. Right-click the zone alias you want to duplicate and select **Duplicate.**

   The duplicated zone alias displays in the **Alias** list (for example, <*Zone_Alias*>_Copy).

6. Edit the name.

   To edit the name, refer to "Renaming a zone alias" on page 649.

7. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Creating a zone configuration

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Click **New Configuration**.

   A new configuration displays in the **Zone Configurations** list.

5. Enter a name for the zone configuration.

   For zone name requirements and limitations, refer to "Zoning naming conventions" on page 639.

6. Press **Enter**.

   Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors. Click **OK** and enter a different name or accept the default name assigned to the zone. (For zone name requirements and limitations, refer to "Zoning naming conventions" on page 639.)

7. Add zones to the zone configuration.

   For step-by-step instructions, refer to "Adding zones to a zone configuration" on page 651.

8. Click **OK** or **Apply** to save your changes.

   Any zones or zone configurations you have changed are saved in the zone database.

Viewing zone configuration properties

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Potential Members** list.
4. Right-click the zone configuration you want to review in the **Zone Configurations** list and select **Properties**.

   The **Zone Configuration Properties** dialog box displays.

5. Review the zone configuration properties.
6. Click **OK** to close the **Zone Configuration Properties** dialog box.

Adding zones to a zone configuration

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zone configurations to which you want to add zones in the **Zone Configurations** list. (Press **SHIFT** or **CTRL** and click each zone configuration name to select more than one zone configuration.)
5. Select one or more zones to add to the zone configurations in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)
6. Click the right arrow between the **Zones** list and the **Zone Configurations** list to add the zones to the zone configurations.
7. Click **OK** or **Apply** to save your changes.

   Any zones or zone configurations you have changed are saved in the zone database.

Removing a zone from a zone configuration

Use the following procedure to remove a zone from a zone configuration. Note that the zone is not deleted; it is only removed from the zone configuration.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Click the plus sign (+) by the appropriate zone configuration in the **Zone Configurations** list to expand the listing and show the zone configuration members.
5. Perform one of the following actions:
   - Right-click the name of the zone you want to remove in the **Zone Configurations** list and select **Remove**.
   - To remove multiple zones, select the zones to be removed from the zone configuration, and click the left arrow between the **Zones** list and the **Zone Configurations** list.

   When successful, the zone is removed from the **Zone Configurations** list.
6. Click **OK** or **Apply** to save your changes.

   Any zones or zone configurations you have changed are saved in the zone database.

Activating a zone configuration

When a zone configuration is active, its members can communicate with one another. Only one zone configuration can be active at any given time.

NOTE
Only one server should be run at a time (actual servers performing discovery) or logon conflicts may occur. Also, activation speeds may differ depending on the hardware vendor and type of zoning used.

You cannot activate a zone configuration if any of the following is true:

- You do not have access privileges to activate zone configurations. You will not be able to activate a zone configuration unless your access privileges are redefined.
- The fabric is not manageable.
- You do not have Read/Write or Activate privileges for the selected fabric and the selected zone database (for FC fabrics and Network OS fabrics only).
- The selected fabric is not supported by the Management application.
- The selected fabric is no longer discovered.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. (*Optional*) Select a zone database from the **Zone DB** list (Enterprise and Professional Plus editions only).
5. Select the zone configuration you want to activate in the **Zone Configurations** list.
6. Click **Activate**.
7. Review the information in the **Activate Zone Configuration** dialog box.

a. Make sure the selected zone configuration is the one you want to activate.

b. (*Optional*) Select the **Generate a report with the activation of new zone configuration** check box to generate the Zone Configuration Activation report.

c. If you are activating a zone configuration from the offline zone database, select or clear the **Save only the selected zone configuration to the existing zone database in the fabric** check box.

- If the check box is cleared (default), the entire offline zone database is saved to the switch and replaces the existing online zone database.
- If the check box is selected, only the selected zone configuration in the offline zone database are saved to the switch and are added to the existing online zone database.

8. Click **OK** to activate the zone configuration.

   A message displays informing you that the zones and zone configurations you change will be saved in the zone database and asking whether you want to proceed. Click **Yes** to confirm the activation, or click **No** to cancel the activation.

   When you click **Yes**, a busy window displays indicating the activation is in progress. A status field informs you whether the activation succeeded or failed. When it succeeds, icons for the active zone configuration and its zones display green. When it fails, the message includes the reason for the failure.

9. Click **OK** to continue.

   The **Activate Zone Configuration** dialog box is closed and the **Zone DB** tab displays.

10. Click **OK**.

The zone configuration is activated and the entire zone database is sent to the fabric.

Deactivating a zone configuration

Use this procedure to deactivate the active zone configuration.

There are several conditions that could cause the **Deactivate** button to be unavailable. They include the following:

- There is no active zone configuration in the selected fabric.
- The fabric is not manageable.
- You do not have Read/Write or Activate privileges for the selected fabric and the selected zone database (for FC fabrics and Network OS fabrics only).
- The selected fabric is not supported by the Management application.
- The selected fabric is no longer discovered.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Active Zone Configuration** tab.

3. Select a fabric from the **Active Zone Configuration** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Click **Deactivate**.

5. Click **Yes** on the confirmation message.

   If the deactivation succeeded, the zone configuration no longer displays in the **Active Zone Configuration** tab.
   If the deactivation failed, the zone configuration still displays in the **Active Zone Configuration** tab.

6. Click **OK** or **Apply** to save your changes.

   Any zones or zone configurations you have changed are saved in the zone database.

Renaming a zone configuration

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the name of the zone configuration you want to change in the **Zone Configurations** list and select **Rename**.
5. Type the new name for the zone configuration.

   For zone configuration name requirements and limitations, refer to "Zoning naming conventions" on page 639.

6. Press **Enter** to save the new name.
7. Click **OK** or **Apply** to save your changes.

   Any zones or zone configurations you have changed are saved in the zone database.

Deleting a zone configuration

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zone configurations in the **Zone Configurations** list that you want to delete, then right-click and select **Delete**.

   A message displays asking you to confirm the deletion.

5. Click **Yes** to delete the selected zone configuration.

   The message closes and the selected zone configurations are removed from the **Zone Configurations** list.

NOTE
If you select "**Do not show me this again.**" on the confirmation message, the next time you delete a zone configuration, it will be deleted without requesting confirmation from you. If you delete something in error, click **Cancel** on the **Zoning** dialog box to exit without saving changes since the last operation (**Apply** or **Activate**). When you reopen the dialog box, the zone configuration is restored.

6. Click **OK** or **Apply** to save your changes.

   Any zones or zone configurations you have changed are saved in the zone database.

Duplicating a zone configuration

When you duplicate a zone configuration, you make a copy of it in the same zone database. The first time a zone configuration is duplicated, the duplicate is automatically given the name *<zonesetlabel>_copy*. On subsequent duplications, a sequential number is assigned to the zone configuration name, such as *<zonesetlabel>_copy_1*, *<zonesetlabel>_copy_2,* and *<zonesetlabel>_copy_3*.

Note that these naming conventions apply to both duplicate and deep duplicate operations.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zone configurations in the **Zone Configurations** list that you want to duplicate, then right-click and select one of the following options:
   - **Duplicate** - To duplicate the zone configuration or configurations.
   - **Deep Duplicate** - To duplicate the zone configuration or configurations *and* all included zones.

   The duplicated zone configuration or sets display in the **Zone Configurations** list.

5. (*Optional*) Type a new name for the zone configuration and press **Enter** to save the name.

   For zone name requirements and limitations, refer to "Zoning naming conventions" on page 639.

6. Click **OK** or **Apply** to save your changes.

   Any zones or zone configurations you have changed are saved in the zone database.

Creating an offline zone database

Offline zone databases are supported only in Enterprise and Professional Plus editions. Use this procedure to create a zone database and save it offline.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a zone database from the **Zone DB** list.
4. Select **Save As** from the **Zone DB Operation** list.

   The **Save Zone DB As** dialog box displays.
5. Enter a name for the database in the **Zone DB Name** field and click **OK**.
6. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

   If you want to show all discovered fabrics in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.
7. Create the desired zones.

   For specific instructions, refer to "Creating a zone" on page 641.
8. Add members to each zone.

   For specific instructions, refer to "Adding members to a zone" on page 642 and "Creating a member in a zone" on page 643.
9. Create a zone configuration.

   For specific instructions, refer to "Creating a zone configuration" on page 650.
10. Activate the zone configuration.

    For specific instructions, refer to "Activating a zone configuration" on page 652.
11. Set zoning policies, if necessary.

    For specific instructions, refer to "Enabling or disabling the default zone for fabrics" on page 646.
12. Click **OK** or **Apply** to save your changes.

    Any zones or zone configurations you have changed are saved in the zone database.

Deleting an offline zone database

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning databases for the selected entity.
3. Select the offline zone database you want to delete in the **Zone DB** list.

   NOTE
   Only offline databases can be deleted.
4. Select **Delete** from the **Zone DB Operation** list.
5. Click **Yes** on the confirmation message.

The message closes and the selected zone configurations are removed from the **Zone Configurations** list.

6. Click **OK** to save your work and close the **Zoning** dialog box.

   Any zones or zone configurations you have changed are saved in the zone database.

Refreshing a zone database

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a zone database from the **Zone DB** list.
4. Select **Refresh** from the **Zone DB Operation** list.

   A message displays informing you that refresh will overwrite the selected database. Click **Yes** to continue.

5. Click **OK**.

   Any zones or zone configurations you have changed are saved in the zone database.

Merging fabrics

When you merge fabrics, the defined and active zone configurations in both fabrics must match.

1. Compare and merge the two zone databases, and save the database to the offline repository.

   Refer to "Merging two zone databases" on page 658.

2. Ensure that the active zone configurations in each fabric are the same, including the same name.

   Refer to "Renaming a zone configuration" on page 654.

3. Load the newly merged zone database from the offline repository.
4. Activate the zone configuration.
5. If the active zone configuration names are the same in each fabric, then load the offline repository, and activate the zone configuration on each fabric.
6. If the active configuration names are different in each fabric, rename the zone configurations to be the same, and copy the zones.
7. Ensure that the active configurations are the same.
   a. Load the newly created offline zone database.
   b. Add the active zones to the zone configuration that is the active configuration on the other fabric.
   c. Rename the inactive configuration.

Merging two zone databases

If a zone or zone configuration is merged, the resulting zone or zone configuration includes *all* members that were marked for addition or removal as well as all members not otherwise marked.

NOTE: You cannot merge the following zones with a Network OS fabric:

- Zones with aliases (can merge with Network OS 3.0.0 and later)
- Zones with D,I members
- TI zones
- QoS zones
- Redirection zones

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Select **Compare** from the **Zone DB Operation** list.

   The **Compare/Merge Zone DBs** dialog box displays, as shown in Figure 240.

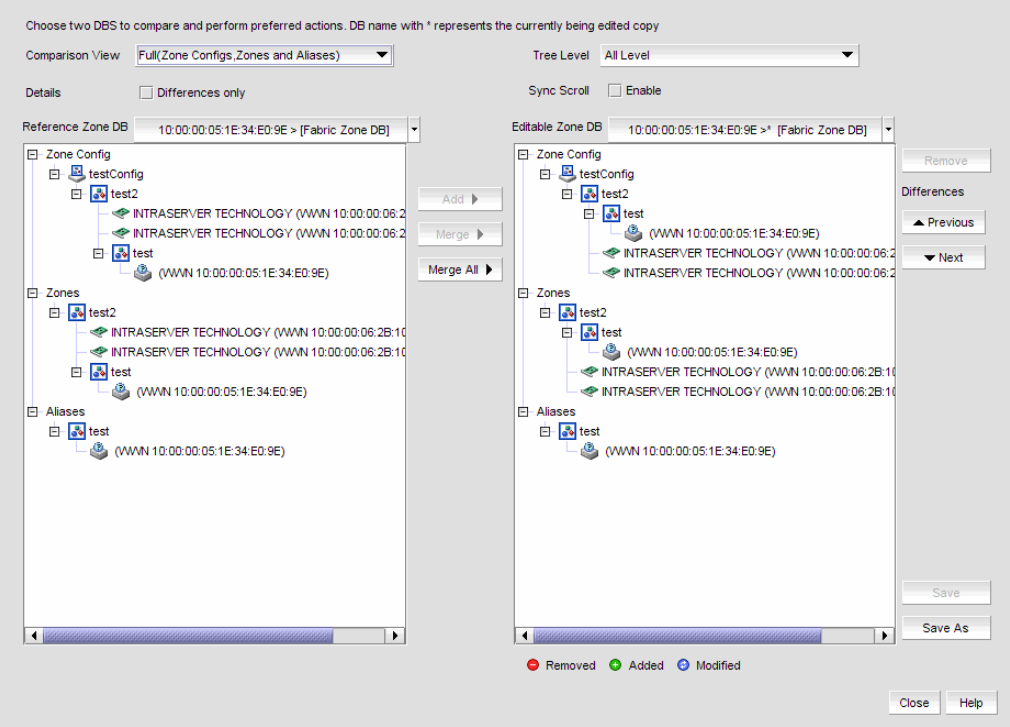


FIGURE 240 **Compare/Merge Zone DBs** dialog box

3. Select a database from the **Reference Zone DB** list.
4. Select a database from the **Editable Zone DB** list.

   The **Reference Zone DB** and **Editable Zone DB** areas display all available element types (zone configurations, zones, and aliases) for the two selected zone databases. In the **Editable Zone DB** area, each element type and element display with an icon indicator (Table 72) to show the differences between the two databases.

5. (*Optional*) Merge elements (zone configurations, zones, or aliases) by completing the following steps:
    a. Select one or more of the same element type from the **Reference Zone DB** area.

        You can select zone configurations, zones, or aliases, but do not mix element types.

    b. Select the same type of element in the **Editable Zone DB** area.

        If you selected a zone configuration in the **Reference Zone DB** area, you must select a zone configuration in the **Editable Zone DB** area.

    c. Click **Merge**.

        If the **Merge** button is inactivated, check that you have selected similar element types in both the **Reference Zone DB** area and the **Editable Zone DB** area. You can merge elements only with similar elements. You cannot merge a zone with a zone configuration, for example.
6. (*Optional*) Merge all elements by clicking **Merge All**.
7. (*Optional*) Add elements (aliases, zones, and zone configurations) to the editable database by completing the following steps.
    a. Select one or more of the same element type in the **Reference Zone DB** area.

        These are the elements that are added to the editable zone database.

    b. Select an element in the **Editable Zone DB** area.

        You can add zone aliases and zone members to a zone. You can add zones to a zone configuration. And you can add zone configurations to the zone database.

    c. Click **Add**.

        If the **Add** button is inactivated, check that you have selected appropriate element types in both the **Reference Zone DB** area and the **Editable Zone DB** area.
8. (*Optional*) Remove elements from the editable zone database by selecting an available element (one that you have added) from the **Editable Zone DB** area and clicking **Remove**.

    Note that if a zone is removed from a zone configuration, it is removed *only* from that single zone configuration. However, if the zone is removed from the list of zones, it is removed from *all* zone configurations.
9. Click **Save As** to save the editable zone database in the offline repository (for Enterprise and Professional Plus editions only).

Creating a common active zone configuration in two fabrics

Before you can merge two fabrics, the defined and active zone configurations in both fabrics must match. Refer to "Merging two zone databases" on page 658 for instructions on how to merge the zone databases in two fabrics.

After you merge the two zone databases, you create a common active zone configuration before physically merging the fabrics.

1. Select **Configure > Zoning > Fabric**.

    The **Zoning** dialog box displays.

2. Select **Compare** from the **Zone DB Operation** list.

   The **Compare/Merge Zone DBs** dialog box displays, as shown in Figure 240.

3. Select the database for the first fabric from the **Reference Zone DB** list.
4. Select the database for the second fabric from the **Editable Zone DB** list.
5. Set up a zone configuration that contains the active zones in both fabrics:
   a. Select the name of the active zone configuration from the **Reference Zone DB** area.
   b. Select the name of the active zone configuration in the **Editable Zone DB** area.
   c. Click **Merge**.

      All of the active zones from both fabrics are now in one zone configuration.
6. Click **Save As** to save the editable zone database in the offline repository for the second fabric.
7. Click **Save As** again, and select the name of the first fabric from the **Fabric** list to save the editable zone database in the offline repository for the first fabric.
8. Click **Close** to close the **Compare/Merge Zone DBs** dialog box and return to the **Zoning** dialog box.
9. In both fabrics, load the offline repository and activate the zone configuration from step b.

   Refer to "Activating a zone configuration" on page 652 for instructions.

Saving a zone database to a switch

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Select a zone database from the **Zone DB** list.
3. Select **Save to Switch** from the **Zone DB Operation** list.
4. Click **Yes** on the confirmation message.

   The selected zone database is saved to the fabric without enabling a specific zone configuration.

5. Click **OK** to save your work and close the **Zoning** dialog box.

Exporting an offline zone database

NOTE
You cannot export an online zone database.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Select an offline zone database from the **Zone DB** list.
3. Select **Export** from the **Zone DB Operation** list.

   The **Export Zone DB** dialog box displays.

4. Browse to the location where you want to export the zone database file (.xml format).

5. Click **Export Zone DB**.
6. Click **OK** to save your work and close the **Zoning** dialog box.

Importing an offline zone database

NOTE
You cannot import an online zone database. You cannot import a zone database that contains zones with duplicate members.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Select an offline zone database from the **Zone DB** list.
3. Select **Import** from the **Zone DB Operation** list.

   The **Import Zone DB** dialog box displays.
4. Browse to the zone database file (.xml format).
5. Click **Import Zone DB**.
6. Click **OK** to save your work and close the **Zoning** dialog box.

Rolling back changes to the offline zone database

Use this procedure to reverse changes made to an offline zone database.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Select the zone database you want to roll back from the **Zone DB** list.

   You must select an offline zone database that has a value in the **Last Saved to Fabric** column. You cannot roll back changes for zone databases that were never saved to the fabric.
3. Select **Roll Back** from the **Zone DB Operation** list.

   The selected zone database reverts back to what it was before the changes were applied.
4. Click **OK** to save your work and close the **Zoning** dialog box.

Zoning administration

This section provides instructions for performing administrative functions with zoning. You can rename, duplicate, delete, and perform other tasks on zone members, zones, and zone configurations.

Comparing zone databases

You can compare zone databases against one another to identify any and all differences between their memberships prior to sending them to the switch. Once the two databases have been compared, icons display to show the differences between the two databases. These icons are illustrated and described in Table 72.

TABLE 72 Compare icon indicators

Icon	Description
	Added — Displays when an element is added to the editable database.
	Modified — Displays when an element is modified on the editable database.
	Removed — Displays when an element is removed from the editable database.

To compare two zone databases, complete the following steps.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Select **Compare** from the **Zone DB Operation** list.

   The **Compare/Merge Zone DBs** dialog box displays, as shown in Figure 241.

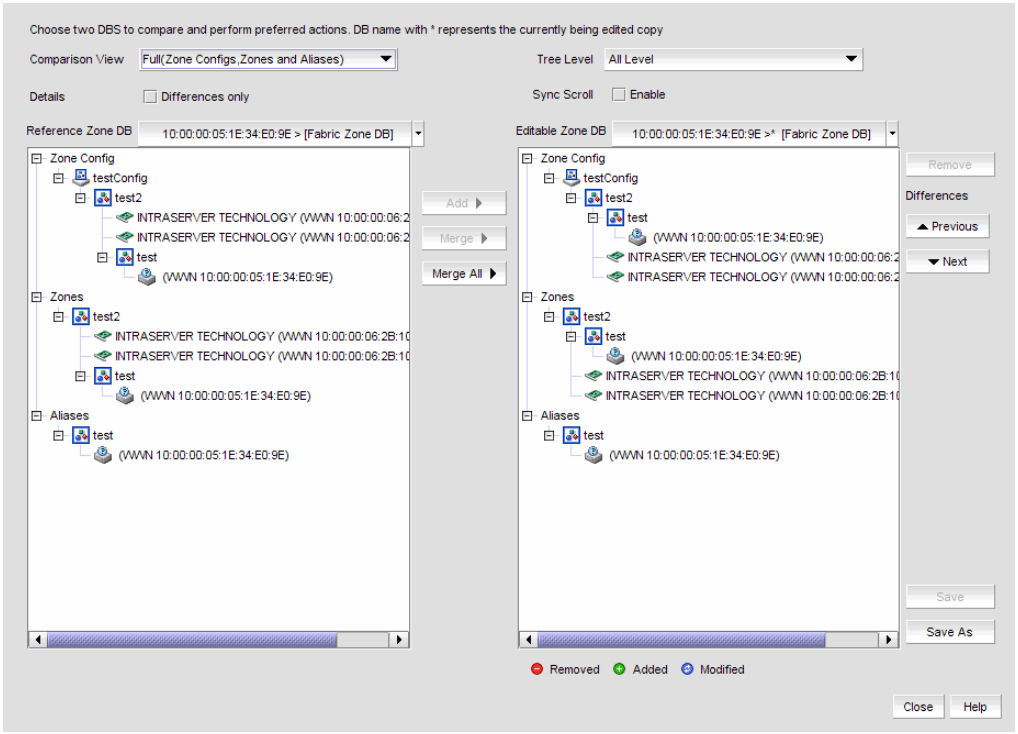


FIGURE 241 Compare/Merge Zone DBs dialog box

3. Select a database from the **Reference Zone DB** list.
4. Select a database from the **Editable Zone DB** list.

The **Reference Zone DB** and **Editable Zone DB** areas display all available element types (zone configurations, zones, and aliases) for the two selected zone databases. In the **Editable Zone DB** area, each element type and element display with an icon indicator (Table 72) to show the differences between the two databases.

5. Set the display for the database areas by selecting one of the following from the **Comparison View** list:
   - **Storage-to-Host Connectivity** — Displays only storage and host devices.
   - **Host-to-Storage Connectivity** — Displays only host and storage devices.
   - **Full** — Displays all zone configurations, zones, and aliases.
6. Set the level of detail for the database areas by selecting one of the following options from the **Tree Level** list:

   NOTE
   This list is only available when you set the **Comparison View** to **Full** .

   - **All Level** — Displays all zone configurations, zones, and aliases.
   - **Zone Configurations** — Displays only zone configurations.
   - **Zones** — Displays only zones.
7. Select the **Differences only** check box to display only the differences between the selected databases.
8. Select the **Sync Scroll Enable** check box to synchronize scrolling between the selected databases.
9. Click **Previous** or **Next** to navigate line-by-line in the **Editable Zone DB** area.
10. Click **Close**.

To merge two zone databases, refer to "Merging two zone databases" on page 658.

Managing zone configuration comparison alerts

You can turn off the automatic zone configuration comparison function if you no longer want to see two of the alert messages that the comparison can produce. When a zone configuration is successfully activated, the comparison function can display an alert icon if either of two conditions exist.

The messages are "The active zone configuration does not exist in the zone database" and "The active zone configuration does not match <*zone configuration*> in the zone database." To turn off the icons and the messages, complete the following steps.

1. After successfully activating a zone configuration, click the **Active Zone Configuration** tab in the **Zoning** dialog box.
2. Select **Turn off the comparison alerts between the active zone configuration and the zone database** check box.

   Any existing alert icons and messages are cleared and further comparisons are prevented.

Setting change limits on zoning activation

Use this procedure to set a limit on the number of changes a user can make to the zone database before activating a zone configuration. If the user exceeds the limit, zone configuration activation is not allowed. By default, all fabrics allow unlimited changes. Changes include adding, removing, or modifying zones, aliases, and zone configurations.

Use this procedure to set the following limits:

- Set a different limit for each fabric.
- Set limits on some fabrics while allowing other fabrics to have unlimited changes.
- Set a limit for fabrics that will be discovered later.

NOTE
You must have the Zoning Set Edit Limits privilege to perform this task.

1. Select **Configure > Zoning > Set Change Limits**.

   The **Set Change Limits for Zoning Activation** dialog box displays.

2. Click **Change Count** for the fabric on which you want to set limits.

   The field changes to an editable field.

3. Enter the maximum number of zone database changes that can be made for that fabric before a zone configuration is activated.

   To set a limit, enter a positive integer.

   To allow unlimited changes, enter 0.

4. Repeat step 2 and step 3 for each fabric on which you want to set limits.

5. To set a limit for new, undiscovered fabrics, enter a value in the **Default Change Count for New Fabrics** field.

   This limit is enforced on all new fabrics as they are discovered. The default value is 0 (Unlimited).

6. Select the **Enforce change limits during zone activation** check box to enforce the change limits.

   If you want to set the limits now, but turn on enforcement of the limits at a later time, make sure the check box is clear.

7. Click **OK** to save your changes and close the dialog box.

Clearing the fabric zone database

ATTENTION
Clearing the zone database removes all zoning configuration information, including all aliases, zones, and zone configurations, in the fabric.

Clearing the fabric zone database is disruptive to the fabric.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Select a fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning databases for the selected entity.

3. Select the Fabric Zone DB from the **Zone DB** list.
4. Select **Clear All** from the **Zone DB Operation** list.
5. Click **Yes** on the confirmation message.

   The message closes and the Fabric Zone DB is cleared of all zoning configurations.
6. Click **OK** to close the **Zoning** dialog box.

Removing all user names from a zone database

Use this procedure to remove all user names from the selected offline zone database.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning databases for the selected entity.
3. Select a zone database that you have checked out (your user name is in the **Current User** column) in the **Zone DB** list.
4. Select **Undo CheckOut** from the **Zone DB Operation** list.
5. Click **Yes** in the confirmation message.

   This removes the user names of users currently logged in to the client from the **Current User** column for this zone database.
6. Click **OK** to save your work and close the **Zoning** dialog box.

   Any zones or zone configurations you have changed are saved in the zone database.

Finding a member in one or more zones

Use this procedure to locate all instances of a member in the **Zones** list on the **Zone DB** tab.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. If you want to show all fabrics discovered in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.
5. Select the devices or ports you want to find in the **Potential Members** list.
6. Click **Find >** between the **Potential Members** list and the **Zones** list.

If the member is found, all instances of the zone member found are highlighted in the **Zones** list.

Finding a zone member in the potential member list

Use this procedure to locate a zone member in the **Potential Members** list on the **Zone DB** tab.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zone member in the **Zones** list that you want to find in the **Potential Members** list. (Press **SHIFT** or **CTRL** and click each zone member to select more than one zone member.)
5. Click **Find <** between the **Potential Members** list and the **Zones** list.

   If the member is found, it is highlighted in the **Potential Members** list.

Finding zones in a zone configuration

Use this procedure to locate all instances of a zone in the **Zone Configurations** list on the **Zone DB** tab.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zone you want to find in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone to select more than one zone.)
5. Click **Find >** between the **Zones** list and the **Zone Configurations** list.

   If the zone is found, all instances of the zone are highlighted in the **Zone Configurations** list.

Finding a zone configuration member in the zones list

Use this procedure to locate a zone configuration member in the **Zones** list on the **Zone DB** tab.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zone configuration member (for example, the zone) in the **Zone Configurations** list that you want to find in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone configuration member to select more than one zone configuration member.)
5. Click **Find <** between the **Zones** list and the **Zone Configurations** list.

   If the zone is found, it is highlighted in the **Zones** list.

Listing zone members

Use this procedure to identify the zone in the active zone configuration of the fabric to which an individual port belongs and the members of that zone.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Right-click in the **Potential Members** list and select **List Zone Members**.

   The **List Zone Members** dialog box displays. If the port is a member of a zone, the fabric name, the port name, and WWN zone members display.
5. Click **Close** to exit the **List Zone Members** dialog box.

Listing un-zoned members

Use this procedure to identify the device ports in the current fabric that are not part of the active zone configuration.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Right-click in the **Potential Members** list and select **List Un-Zone Members**.

   The **Un-Zone Members** dialog box displays. The dialog box shows the fabric name and the connected device ports that are not part of the active zone configuration.
5. Click **Close** to exit the **Un-Zone Members** dialog box.

Removing an offline device

The Management application enables you to remove an offline device from all zones and zone aliases in the selected zone DB.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

3. Select **Offline Utility** from the **Zone DB Operation** list.

   The **Offline Device Management** dialog box displays.

4. Select the check box for the offline device you want to remove in the **Remove** column.

   Select the **Remove** check box to select all offline devices.

5. Click **OK** on the **Offline Device Management** dialog box.

   A warning message displays informing you that the selected zone members will be replaced from all zones and aliases in the selected zone DB.

6. Click **OK** on the message.

7. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

   Any zones or zone configurations you have changed are saved in the zone database.

Replacing zone members

You can replace one instance of a zone member in one zone, or all instances of the zone member in all the zones to which it belongs.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the zone member you want to replace in the **Zones** list and select one of the following options from the shortcut menu that displays:

   - **Replace** - To replace the zone member in a selected zone.
   - **Replace All** - To replace all instances of the selected zone member.

   The **Replace Zone Member** dialog box displays.

5. Select the option from the **Member Type** list that you want to use to identify the replacement zone member.

   For Network OS fabrics, only **WWN** and **Alias** are supported.

6. Enter the WWN, name, domain and port index numbers, or alias — whichever is appropriate for the method you chose in step 5.

   When you choose the WWN method, you may define a name for the replacement zone member.

7. Click **OK**.

   The new zone member replaces the old zone member in the **Zones** list and the **Replace Zone Member** dialog box closes.

8. Click **OK** or **Apply** to save your changes.

   Any zones or zone configurations you have changed are saved in the zone database.

Replacing an offline device by WWN

The Management application enables you to replace an offline device by WWN from all zones and zone aliases in the selected zone DB.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

3. Select **Offline Utility** from the **Zone DB Operation** list.

   The **Offline Device Management** dialog box displays.

4. Clear the **Remove** column check box for the offline device you want to replace.

5. Select **WWN** (default) in the corresponding **Replace Using** list.

6. Enter the WWN or select the name of the offline device in the corresponding **Replace Value** list.

   If the selected name has multiple device or device port WWNs assigned (names are set to non-unique in the Management application), the **Device or Device Port WWN of Non-unique Name** dialog box displays. The **WWN** list includes all device and device port WWNs assigned to the selected name.

7. Click **OK** on the **Offline Device Management** dialog box.

   A warning message displays informing you that the selected zone members will be removed from all zones and aliases in the selected zone DB.

8. Click **OK** on the message.

9. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

   Any zones or zone configurations you have changed are saved in the zone database.

Replacing an offline device by name

The Management application enables you to replace an offline device by name from all zones and zone aliases in the selected zone DB.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Select a fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

3. Select **Offline Utility** from the **Zone DB Operation** list.

   The **Offline Device Management** dialog box displays.

4. Clear the **Remove** column check box for the offline device you want to replace.

5. Select **Name** in the corresponding **Replace Using** list.

6. Select the name of the offline device in the corresponding **Replace Value** list.

   If the selected name has multiple device or device port WWNs assigned (names are set to non-unique in the Management application), the **Device or Device Port WWN of Non-unique Name** dialog box displays. The **WWN** list includes all device and device port WWNs assigned to the selected name.

7. Select the WWN you want to use from the **WWN** list and click **OK**.

8. Click **OK** on the **Offline Device Management** dialog box.

   A warning message displays informing you that the selected zone members will be removed from all zones and aliases in the selected zone DB.

9. Click **OK** on the message.

10. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

    Any zones or zone configurations you have changed are saved in the zone database.

Chapter

Port Fencing

20

In this chapter

About port fencing

NOTE
This feature is only available for Fabric OS devices.

NOTE
All Fabric OS devices must have Fabric Watch and must be running firmware Fabric OS 6.2 or later.

NOTE
This feature requires a Trial or Licensed version.

Port Fencing allows you to protect your SAN from repeated operational problems experienced by ports. Use Port Fencing to set threshold limits for the number of specific port events permitted during a given time period on the selected object. For default threshold values for Fabric OS devices, refer to Chapter 7 of the *Fabric Watch Administrator's Guide*.

Port Fencing objects include the SAN, Fabrics, Directors, Switches (physical), Virtual Switches, Ports, as well as Port Types (E_port, F_port, and FX_port). Use Port Fencing to directly assign a threshold to these objects. When a switch does not support Port Fencing, a “No Fencing Changes” message displays in the **Threshold** field in the **Ports** table.

If the port detects more events during the specified time period, the device firmware blocks the port, disabling transmit and receive traffic until you investigate, solve the problem, and manually unblock the port.

Physical fabrics, directors, switches, port types, and ports display when you have the privileges to manage that object and are indicated by the standard product icons.

NOTE
Port Fencing displays any existing thresholds discovered on manageable fabrics, directors, and switches running firmware version Fabric OS 6.2 or later.

Viewing port fencing configurations

NOTE
This feature is only available for Fabric OS devices.

NOTE
This feature requires a Trial or Licensed version.

Port Fencing allows you to protect your SAN from repeated operational problems experienced by ports. Use Port Fencing to set threshold limits for the number of specific port events permitted during a given time period on the selected object. For default threshold values for Fabric OS devices, refer to Chapter 7 of the *Fabric Watch Administrator's Guide*.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays (Figure 243).

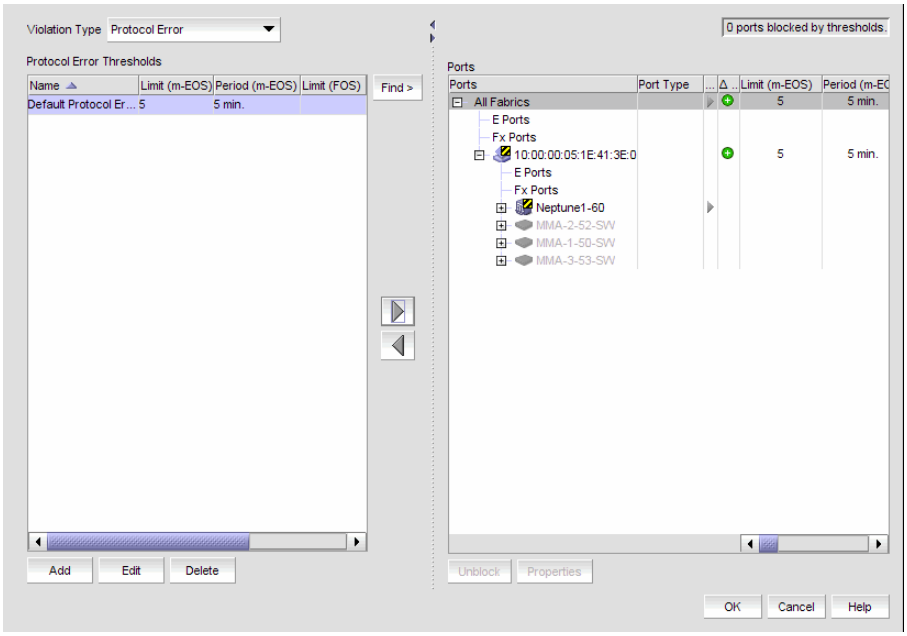


FIGURE 242 Port Fencing dialog box

The Port Fencing dialog box contains the following field and components:

- **Violation Type** list — The name of the ISL, Link, or Security threshold currently active on this port. If the object does not support Port Fencing, this field displays "# No Fencing Support #". This field displays as inactive (grayed-out) when the object is only partially managed by the management application.
  (ISL Threshold only) If the port type is E_port, the ISL Threshold name displays in a bold font to indicate when the threshold is currently active on the port type.

- Thresholds table — List of configured thresholds based on the threshold type selected in the **Violation Type** list.
  - **Limit (Fabric OS) —** The number of events allowed for the assigned threshold. If the object has no fencing support or no fencing changes, this field displays two hyphens separated by a space (- -). When the object is only partially managed by the management application, this field displays as inactive (grayed-out).
  - **Period (Fabric OS) —** The time limit (in seconds or minutes) for the assigned threshold. This field displays as inactive (grayed-out) when the object is only partially managed by the management application.
  - **Ports Affected** — The total number of ports on all objects that could be affected by the threshold setting. It does not show the current number of ports affected. This value updates in real time as you add and subtract each threshold from each object.
- Find button — Select a threshold in the thresholds table and click the find button (>) to highlight each instance of the selected threshold in the **Ports** table.
- Right arrow button — Select a threshold in the thresholds table and click the right arrow button to add the selected threshold to the selected fabrics, switches, or switch ports (refer to "Assigning thresholds" on page 685).
- Left arrow button — Select a threshold in the Ports table and click the left arrow button to remove the selected threshold from the associated fabrics, switches, or switch ports (refer to "Removing thresholds from individual objects" on page 692).
- **Add** button — Click to add an ISL protocol threshold (refer to "Adding thresholds" on page 677).
- **Edit** button — Click to edit an ISL protocol threshold (refer to "Editing thresholds" on page 687).
- **Delete** button — Click to delete an ISL protocol threshold (refer to "Removing thresholds from the thresholds table" on page 693).

- **Ports** table — All managed fabric, director, switch, port type, and port objects (label and icon) in its hierarchical relationship to the other objects in the tree.
  - **Ports** — Displays all discovered fabrics, devices, and ports as both text and icons.
  - **Port Type** — The operational port type of the port. This field displays as inactive (grayed-out) when either the object's firmware does not support Port Fencing or the object is only partially managed by the management application.
  - **Directly Assigned** — A right arrow icon to indicate that the threshold is directly assigned to this object and is inherited by all objects below it in the tree. This field displays as inactive (grayed-out) when either the object's firmware does not support Port Fencing or the object is only partially managed by the management application.
  - **Changed** indicator — The change icons in real time when you change information in the dialog box. One change icon indicates a new threshold was applied (either directly or inherited) to the port, and another indicates that a threshold was removed from this object (during this session) and no threshold applies to the port.
  - *Threshold_type* **Threshold** — The name of the ISL threshold policy.
  - **Limit (Fabric OS) —** The number of events allowed for the assigned threshold. If the object has no fencing support or no fencing changes, this field displays two hyphens separated by a space (- -). When the object is only partially managed by the management application, this field displays as inactive (grayed-out).
  - **Period (Fabric OS) —** The time limit (in seconds or minutes) for the assigned threshold. This field displays as inactive (grayed-out) when the object is only partially managed by the management application.
  - **Operational State** — The operational state of the port.
  - **Blocked Configuration** — The current configuration of the port (Blocked or Unblocked).
  - **Port WWN** — The port world wide name of the port.
  - **Connected Product** — The device label of the connected object.
  - **Connected Port # —** The port number of the connected port.
  - **Connected Port WWN** — The port world wide name of the connected port.
  - **Connected Port Name** — The name of the connected port configured in the Element Manager.
  - **FC Address** — The FC address of the port.
- **Properties** button — Click to display the **Properties** dialog box for the fabric, switch, or port selected in the **Ports** table. The All Fabrics and Port Type objects do not have properties. For more information, refer to "Viewing SAN device properties" on page 1302.
- **Unblock** button — Click to unblock a blocked port after a warning message displays (refer to "Unblocking a port" on page 686). This button becomes active after you select a blocked port in the **Ports** table.

2. Click **OK** on the **Port Fencing** dialog box.

Thresholds

You can create thresholds, which you can then assign to available objects in the tree. Port Fencing threshold types include the following:

- C3 Discard Frames (Fabric OS only)
- Invalid CRCs (Fabric OS only)

- Invalid Words (Fabric OS only)
- Link Reset (Fabric OS only)
- Protocol Errors (Fabric OS)
- State Change (Fabric OS only)

NOTE
Fabric OS devices are allowed only 2 defined thresholds (one default and one custom) for each threshold type and only one of these thresholds can be active on the device.

During the dynamic operation of a Fabric, any port could be any type. For example, a technician could disconnect a port from a switch and reconnect that port to a storage port, or the port could change from an E_port to an F_port. Therefore, when calculating the **Affected Ports** value the Management application does not look for the current port type, but looks at the policy priority level in relation to the other policies currently assigned to this switch.

When there are two or more policies on a switch, the total number of **Affected Ports** may be more than the total number of ports on the switch (the same port may adopt different policies depending on changes in the port's port type).

For default threshold values for Fabric OS devices, refer to Chapter 7 of the *Fabric Watch Administrator's Guide*.

C3 Discard Frames threshold

NOTE
This threshold is only available for Fabric OS devices running 6.3 or later.

Use this type of threshold to block a port when a C3 Discard Frames violation meets the Fabric OS switch threshold. This threshold is only supported on directors, switches, and blades with a 4 Gbps, 8 Gbps, or 16 Gbps ASIC.

- 32-port, 4 Gbps FC Switch
- 64-port, 4 Gbps FC Switch
- 32-port, 4 Gbps FC Interop Switch
- 4 Gbps Router, Extension Switch
- 4 Gbps Extension Switch
- 4 Gbps 32-port Switch
- 8 Gbps 32-port Switch
- 8 Gbps 40-port Switch
- 8 Gbps 24-port Embedded Switch
- 8 Gbps 16-port Embedded Switch
- 8 Gbps 8-FC port, 10 GbE 24-DCB port Switch
- 16 Gbps 24-port Edge switch
- 16 Gbps 48-port Edge switch
- Director Chassis
- 8-slot Backbone Chassis
- 4-slot Backbone Chassis

- 16 Gbps 8-slot Backbone Chassis
- 16 Gbps 4-slot Backbone Chassis
- 8 Gbps Encryption Switch
- Encryption Blade
- 10 Gbps FCoE Port Router Blade
- FC 8 GB 64-port Blade
- 8 Gbps Extension Blade
- FC 8 Gbps 16-port Blade
- FC 8 Gbps 32-port Blade
- FC 8 Gbps 48-port Blade
- FC 8 Gbps 64-port Blade
- FC 16 Gbps 32-port Blade
- FC 16 Gbps 48-port Blade

Invalid CRCs threshold

NOTE
This threshold is only available for Fabric OS devices.

Use this type of threshold to block a port when an Invalid CRCs violation meets the Fabric OS switch threshold.

Invalid words threshold

NOTE
This threshold is only available for Fabric OS devices.

Use this type of threshold to block a port when an Invalid Words violation meets the Fabric OS switch threshold.

Link Reset threshold

NOTE
This threshold is only available for Fabric OS devices.

Use this type of threshold to block a port when the link timeout errors meet the threshold.

Protocol error threshold

Use Protocol Error thresholds to block a port when one of the following protocol errors meet the threshold:

- ISL Bouncing–ISL has repeatedly become unavailable due to link down events.
- ISL Protocol Mismatch–ISL has been repeatedly put into the Invalid Attachment state due to a protocol error.

State Change threshold

NOTE
This threshold is only available for Fabric OS devices running 6.3 or later.

Use this type of threshold to block a port when a state change violation type meets the Fabric OS switch threshold.

For 4 Gbps Router, Extension Switches and Blades only, when you apply this threshold on an E Port, the threshold is also applied to the VE Ports (internally by Fabric OS).

Adding thresholds

NOTE
Only available for Fabric OS products.

NOTE
This feature requires a Trial or Licensed version.

The Management application allows you to create Invalid CRCs, Invalid words, Link, Link Reset, Protocol Error, Security, and Sync Loss thresholds.

Adding a C3 Discard Frames threshold

NOTE
This threshold is only available for Fabric OS devices running 6.3 or later.

Use to block a port when a **C3 Discard Frames** violation type meets the Fabric OS switch threshold. For default threshold values for Fabric OS devices, refer to Chapter 7 of the *Fabric Watch Administrator's Guide*.

To add an C3 Discard Frames threshold, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays (Figure 243).

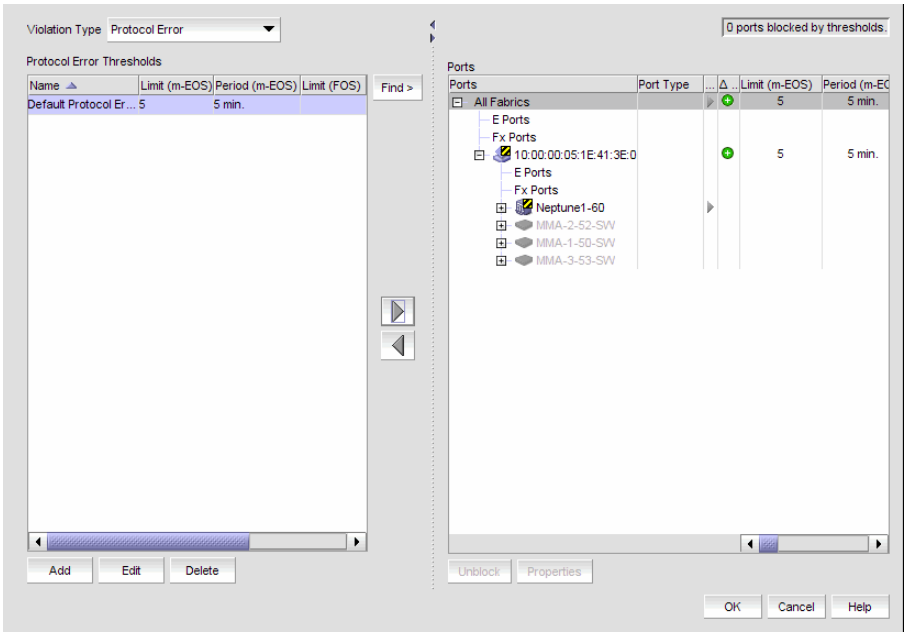


FIGURE 243 Port Fencing dialog box

2. Select **C3 Discard Frames (Fabric OS only)** from the **Violation Type** list.
3. Click **Add**.

   The **Add C3 Discard Frames Threshold** dialog box displays.

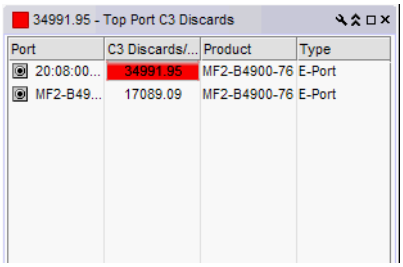


FIGURE 244 Add C3 Discard Frames Threshold dialog box

4. Enter a name for the threshold in the **Name** field.
5. Select one of the following options:
   - Default — Uses device defaults. Go to step 8.
   - Custom — Uses your selections. Continue with step 6.
6. Enter the number of C3 discarded frames allowed for the threshold in the **Threshold** errors field.
7. Select the time period for the threshold from the **errors per** list. The following choices are available:
   - None — the port is blocked as soon as the specified number of C3 discarded frames allowed is met.

- Second — the port is blocked as soon as the specified number of C3 discarded frames allowed is reached within a second.
- Minute — the port is blocked as soon as the specified number of C3 discarded frames allowed is reached within a minute.
- Hour — the port is blocked as soon as the specified number of C3 discarded frames allowed is reached within a hour.
- Day — the port is blocked as soon as the specified number of C3 discarded frames allowed is reached within a day.

8. Click **OK** to add the C3 discarded frames threshold to the table and close the **Add C3 Discard Frames Threshold** dialog box.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 685.

9. Click **OK** on the **Port Fencing** dialog box.

Adding an Invalid CRCs threshold

NOTE
This threshold is only available for Fabric OS devices.

NOTE
This feature requires a Trial or Licensed version.

Use to block a port when an **Invalid CRC** violation type meets the Fabric OS switch threshold. For default threshold values for Fabric OS devices, refer to Chapter 7 of the *Fabric Watch Administrator's Guide*.

To add an Invalid CRCs threshold, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **Invalid CRCs (Fabric OS only)** from the **Violation Type** list.
3. Click **Add**.

   The **Add Invalid CRCs Threshold** dialog box displays.

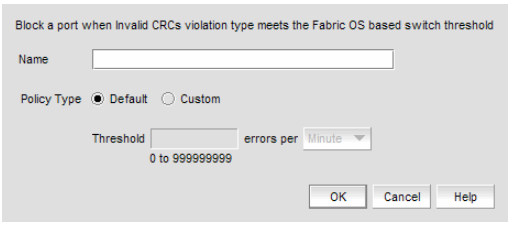


FIGURE 245 Add Invalid CRCs Threshold dialog box

4. Enter a name for the threshold in the **Name** field.
5. Select one of the following options:
   - Default — Uses device defaults. Go to step 8.

- Custom — Uses your selections. Continue with step 6.

6. Enter the number of invalid CRCs allowed for the threshold in the **Threshold** errors field.
7. Select the time period for the threshold from the **errors per** list. The following choices are available:
   - None — the port is blocked as soon as the specified number of invalid CRCs allowed is met.
   - Second — the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a second.
   - Minute — the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a minute.
   - Hour — the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a hour.
   - Day — the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a day.
8. Click **OK** to add the Invalid CRCs threshold to the table and close the **Add Invalid CRCs Threshold** dialog box.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 685.
9. Click **OK** on the **Port Fencing** dialog box.

Adding an Invalid Words threshold

NOTE
This threshold is only available for Fabric OS devices.

NOTE
This feature requires a Trial or Licensed version.

Use to block a port when the **Invalid Words** violation type meets the Fabric OS switch threshold. For default threshold values for Fabric OS devices, refer to Chapter 7 of the *Fabric Watch Administrator's Guide*.

To add an Invalid Words threshold, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.
2. Select **Invalid Words (Fabric OS only)** from the **Violation Type** list.
3. Click **Add**.

   The **Add Invalid Words Threshold** dialog box displays.

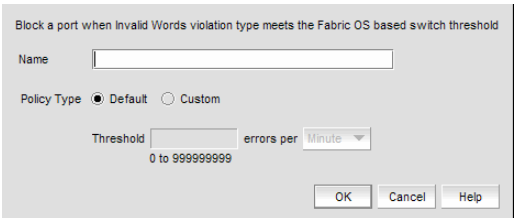


FIGURE 246 Add Invalid Words Threshold dialog box

4. Enter a name for the threshold in the **Name** field.
5. Select one of the following options:
   - Default — Uses device defaults. Go to step 8.
   - Custom — Uses your selections. Continue with step 6.
6. Enter the number of invalid words allowed for the threshold in the **Threshold** errors field.
7. Select the time period for the threshold from the **errors per** list. The following choices are available:
   - None — the port is blocked as soon as the specified number of invalid words allowed is met.
   - Second — the port is blocked as soon as the specified number of invalid words allowed is reached within a second.
   - Minute — the port is blocked as soon as the specified number of invalid words allowed is reached within a minute.
   - Hour — the port is blocked as soon as the specified number of invalid words allowed is reached within a hour.
   - Day — the port is blocked as soon as the specified number of invalid words allowed is reached within a day.
8. Click **OK** to add the Invalid Words threshold to the table and close the **Add Invalid Words Threshold** dialog box.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 685.
9. Click **OK** on the **Port Fencing** dialog box.

Adding a Link Reset threshold

NOTE
This threshold is only available for Fabric OS devices.

NOTE
This feature requires a Trial or Licensed version.

Use to block a port when the **Link Reset** violation type meets the Fabric OS switch threshold. For default threshold values for Fabric OS devices, refer to Chapter 7 of the *Fabric Watch Administrator's Guide*.

To add a Link Reset threshold, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **Link Reset (Fabric OS only)** from the **Violation Type** list.
3. Click **Add**.

   The **Add Link Reset Threshold** dialog box displays.

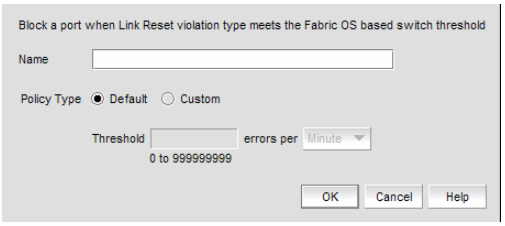


FIGURE 247 Add Link Reset Threshold dialog box

4. Enter a name for the threshold in the **Name** field.
5. Select one of the following options:
   - Default — Uses device defaults. Go to step 8.
   - Custom — Uses your selections. Continue with step 6.
6. Enter the number of link resets allowed for the threshold in the **Threshold** errors field.
7. Select the time period for the threshold from the **errors per** list. The following choices are available:
   - None — the port is blocked as soon as the specified number of link resets allowed is met.
   - Second — the port is blocked as soon as the specified number of link resets allowed is reached within a second.
   - Minute — the port is blocked as soon as the specified number of link resets allowed is reached within a minute.
   - Hour — the port is blocked as soon as the specified number of link resets allowed is reached within a hour.
   - Day — the port is blocked as soon as the specified number of link resets allowed is reached within a day.

8. Click **OK** to add the Link Resets threshold to the table and close the **Add Link Reset Threshold** dialog box.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 685.

9. Click **OK** on the **Port Fencing** dialog box.

Adding a Protocol Error threshold

NOTE
Only available for Fabric OS products.

NOTE
This feature requires a Trial or Licensed version.

Use this type of threshold to block a port when one of the following ISL protocol errors meet the threshold:

- ISL Bouncing–ISL has repeatedly become unavailable due to link down events.
- ISL Segmentation–ISL has repeatedly become segmented.
- ISL Protocol Mismatch–ISL has been repeatedly put into the Invalid Attachment state due to a protocol error.

To add a Protocol Error threshold, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **Protocol Error** from the **Violation Type** list.
3. Click **Add**.

   The **Add Protocol Error Threshold** dialog box displays.

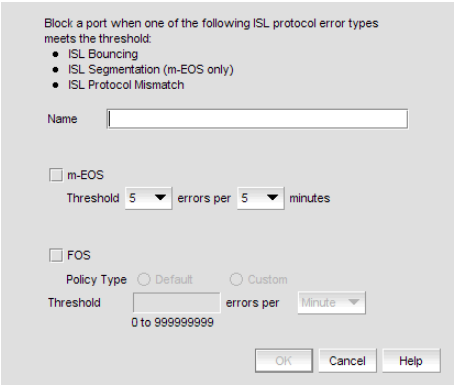


FIGURE 248 Add Protocol Error Threshold dialog box

4. Enter a name for the threshold in the **Name** field.
5. Select the **Fabric OS** check box.

a. Select one of the following options:

- Default — Uses device defaults. Go to step 6.
- Custom — Uses your selections. Continue with step b.

b. Enter the number of protocol errors allowed for the threshold from the **Threshold** errors field.

c. Select the time period for the threshold from the **errors per** list. The following choices are available:

- None — the port is blocked as soon as the specified number of protocol errors allowed is met.
- Second — the port is blocked as soon as the specified number of protocol errors allowed is reached within a second.
- Minute — the port is blocked as soon as the specified number of protocol errors allowed is reached within a minute.
- Hour — the port is blocked as soon as the specified number of protocol errors allowed is reached within a hour.
- Day — the port is blocked as soon as the specified number of protocol errors allowed is reached within a day.

6. Click **OK** to add the protocol errors threshold to the table and close the **Add Protocol Error Threshold** dialog box.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 685.

7. Click **OK** on the **Port Fencing** dialog box.

Adding a State Change threshold

NOTE
This threshold is only available for Fabric OS devices running 6.3 or later.

NOTE
This feature requires a Trial or Licensed version.

Use to block a port when a state change violation type meets the Fabric OS switch threshold. For 4 Gbps Router, Extension Switches and Blades only, when you apply this threshold on an E Port, the threshold is also applied to the VE Ports (internally by Fabric OS). For default threshold values for Fabric OS devices, refer to Chapter 7 of the *Fabric Watch Administrator's Guide*.

To add an State Change threshold, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **State Change (Fabric OS only)** from the **Violation Type** list.

3. Click **Add**.

   The **Add State Change Threshold** dialog box displays.

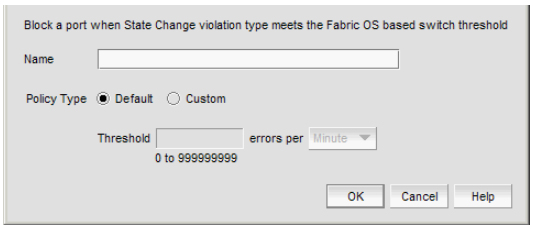


FIGURE 249 Add State Change Threshold dialog box

4. Enter a name for the threshold in the **Name** field.
5. Select one of the following options from the Policy Type field:
   - Default — Uses device defaults. Go to step 8.
   - Custom — Uses your selections. Continue with step 6.
6. Enter the number of state changes allowed for the threshold in the **Threshold** errors field.
7. Select the time period for the threshold from the **errors per** list. The following choices are available:
   - None — the port is blocked as soon as the specified number of state changes allowed is met.
   - Second — the port is blocked as soon as the specified number of state changes allowed is reached within a second.
   - Minute — the port is blocked as soon as the specified number of state changes allowed is reached within a minute.
   - Hour — the port is blocked as soon as the specified number of state changes allowed is reached within a hour.
   - Day — the port is blocked as soon as the specified number of state changes allowed is reached within a day.
8. Click **OK** to add the state changes threshold to the table and close the **Add State Change Threshold** dialog box.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 685.
9. Click **OK** on the **Port Fencing** dialog box.

Assigning thresholds

You can assign thresholds to any active object in the **Ports** table. You can only assign one threshold to an object at a time. If you assign a threshold to a switch, director, or fabric object, or to the All Fabrics object, the threshold is assigned to all subordinate objects (which do not have a directly assigned threshold) in the tree.

However, if an object inherits a threshold from another object above it in the hierarchy, you cannot remove that inherited threshold directly from the subordinate object. You must either remove the threshold from the higher object to which it was directly assigned or directly assign a different threshold to the subordinate object.

To assign an existing threshold to fabric, director, switch, port type, and port objects, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select a threshold type from the **Violation Type** list.
3. Select the threshold you want to assign from the **Thresholds** table.
4. Select the objects (All Fabrics, Fabric, Director, Switch, Port Type, and/or Port) to which you want to assign the threshold from the **Ports** table.
5. Click the right arrow.

   A directly assigned icon ( ) displays next to the objects you selected in the **Ports** table to show that the threshold was applied at this level and was inherited by every subordinate object below it in the tree (if not affected by lower level direct assignments).

   An added icon ( ) appears next to every object in the tree to which the new threshold is applied.

6. Click **OK** on the **Port Fencing** dialog box.

Unblocking a port

The Management application allows you to unblock a port (only if it was blocked by Port Fencing) once the problem that triggered the threshold is fixed. When a port is blocked an Attention icon ( ) displays next to the port node.

To unblock a port, complete the following steps.

1. Select Monitor > Fabric Watch > Port Fencing.

   The Port Fencing dialog box displays.

2. Right-click anywhere in the Ports table and select Expand.
3. Select a blocked port from the Ports table.
4. Click Unblock.
5. Click OK on the message.

   If you did not solve the root problem, the threshold will trigger again.

6. Click OK on the Port Fencing dialog box.

Avoiding port fencing inheritance

When you directly assign a threshold to an object, the threshold is inherited by all subordinate objects in the tree (unless they already have directly assigned thresholds). You cannot remove an inherited threshold from a subordinate object. However, the Management application allows you to effectively avoid inheritance for individual subordinate objects while maintaining inheritance for other subordinate objects. To avoid inheritance for an individual subordinate object, you must create a new threshold with a maximum limit of events allowed and a minimum time period, then assign the new threshold to the subordinate object.

To turn off port fencing inheritance, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select a threshold type from the **Violation Type** list.
3. Click **Add**.

   The **Add** *Type* **Threshold** dialog box displays.
4. Type a name for the new threshold (for example, AvoidProtocolError) in the **Name** field.
5. Select or enter the maximum number of errors or violations allowed in the **Threshold errors/violations** field.
6. Select the minimum time period available from the **Threshold minutes/seconds** list.
7. Click **OK** on the **Add** *Type* **Threshold** dialog box.
8. Click **OK** on the **Port Fencing** dialog box.

Editing thresholds

The Management application allows you to edit the name, number of events needed, and time period of ISL Protocol, Link, and Security thresholds.

Editing a C3 Discard Frames threshold

NOTE
This threshold is only available for Fabric OS devices.

NOTE
This feature requires a Trial or Licensed version.

Use to block a port when a **C3 Discard Frames** violation type meets the Fabric OS switch threshold.

To edit a C3 Discard Frames threshold, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.
2. Select **C3 Discard Frames (Fabric OS only)** from the **Violation Type** list.
3. Select the threshold you want to change and click **Edit**.

   The **Edit C3 Discard Frames** dialog box displays.
4. Complete step 4 through step 7 in "Adding a C3 Discard Frames threshold" on page 677.
5. Click **OK** on the **Edit C3 Discard Frames Threshold** dialog box.

   If the threshold has already been assigned to ports, an "Are you sure you want to make the requested changes to this threshold on "X" ports?" message displays. Click **OK** to close.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 685.
6. Click **OK** on the **Port Fencing** dialog box.

Editing an Invalid CRCs threshold

NOTE
This threshold is only available for Fabric OS devices.

NOTE
This feature requires a Trial or Licensed version.

Use to block a port when the **Invalid CRCs Threshold** violation type meets the Fabric OS switch threshold.

To edit an Invalid CRCs threshold, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **Invalid CRCs (Fabric OS only)** from the **Violation Type** list.
3. Select the threshold you want to change and click **Edit**.

   The **Edit Invalid CRCs Threshold** dialog box displays.

4. Complete step 4 through step 7 in "Adding an Invalid CRCs threshold" on page 679.
5. Click **OK** on the **Edit Invalid CRCs Threshold** dialog box.

   If the threshold has already been assigned to ports, an "Are you sure you want to make the requested changes to this threshold on "X" ports?" message displays. Click **OK** to close.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 685.

6. Click **OK** on the **Port Fencing** dialog box.

Editing an Invalid Words threshold

NOTE
This threshold is only available for Fabric OS devices.

NOTE
This feature requires a Trial or Licensed version.

Use to block a port when the **Invalid Word Threshold** violation type meets the Fabric OS switch threshold.

To edit an Invalid Words threshold, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **Invalid Words (Fabric OS only)** from the **Violation Type** list.
3. Select the threshold you want to change and click **Edit**.

   The **Edit Invalid Words Threshold** dialog box displays.

4. Complete step 4 through step 7 in "Adding an Invalid Words threshold" on page 680.

5. Click **OK** on the **Edit Invalid Words Threshold** dialog box.

   If the threshold has already been assigned to ports, an "Are you sure you want to make the requested changes to this threshold on "X" ports?" message displays. Click **OK** to close.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 685.

6. Click **OK** on the **Port Fencing** dialog box.

Editing a Link Reset threshold

NOTE
This threshold is only available for Fabric OS devices.

NOTE
This feature requires a Trial or Licensed version.

Use to block a port when the **Link Reset** violation type meets the Fabric OS switch threshold.

To edit a Link Reset threshold, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **Link Reset (Fabric OS only)** from the **Violation Type** list.

3. Select the threshold you want to change and click **Edit**.

   The **Edit Link Reset Threshold** dialog box displays.

4. Complete step 4 through step 7 in "Adding a Link Reset threshold" on page 681.

5. Click **OK** on the **Edit Link Reset Threshold** dialog box.

   If the threshold has already been assigned to ports, an "Are you sure you want to make the requested changes to this threshold on "X" ports?" message displays. Click **OK** to close.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 685.

6. Click **OK** on the **Port Fencing** dialog box.

Editing a Protocol Error threshold

NOTE
This threshold is only available for Fabric OS devices.

NOTE
This feature requires a Trial or Licensed version.

Use to block a port when one of the following ISL protocol errors meet the threshold:

- ISL Bouncing–ISL has repeatedly become unavailable due to link down events.
- ISL Segmentation–ISL has repeatedly become segmented.

- ISL Protocol Mismatch–ISL has been repeatedly put into the Invalid Attachment state due to a protocol error.

To edit a Protocol Error threshold, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **Protocol Error** from the **Violation Type** list.
3. Select the threshold you want to change and click **Edit**.

   The **Edit Protocol Error Threshold** dialog box displays.

4. Complete step 4 through step 5 in "Adding a Protocol Error threshold" on page 683.
5. Click **OK** on the **Edit Protocol Error Threshold** dialog box.

   If the threshold has already been assigned to ports, an "Are you sure you want to make the requested changes to this threshold on "X" ports?" message displays. Click **OK** to close.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 685.

6. Click **OK** on the **Port Fencing** dialog box.

Editing a State Change threshold

NOTE
This threshold is only available for Fabric OS devices running 6.3 or later.

NOTE
This feature requires a Trial or Licensed version.

Use to block a port when a state change violation type meets the Fabric OS switch threshold. For 4 Gbps Router, Extension Switches and Blades only, when you apply this threshold on an E Port, the threshold is also applied to the VE Ports (internally by Fabric OS).

To edit an State Change threshold, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **State Change (Fabric OS only)** from the **Violation Type** list.
3. Select the threshold you want to change and click **Edit**.

   The **Edit State Change Threshold** dialog box displays.

4. Complete step 4 through step 7 in "Adding a State Change threshold" on page 684.
5. Click **OK** to add the state change threshold to the table and close the **Edit State Change Threshold** dialog box.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 685.

6. Click **OK** on the **Port Fencing** dialog box.

Finding assigned thresholds

The Management application allows you to find all ports with a specific threshold applied.

NOTE
This search is performed on the threshold name. Since Fabric OS devices do not retain the threshold name, the ability to search for a threshold on a Fabric OS device is not available in most cases.

To find assigned thresholds, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select a threshold type from the **Violation Type** list.
3. Select a threshold from the **Threshold** table.
4. Click **Find**.
5. Every port which uses the selected threshold is highlighted in the **Ports** table.
6. Click **OK** on the **Port Fencing** dialog box.

Viewing thresholds

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select a threshold type from the **Violation Type** list.
3. Review the **Thresholds** and **Ports** tables.
4. Repeat step 2 and step 3, as necessary.
5. Click **OK** on the **Port Fencing** dialog box.

Viewing all thresholds on a specific Fabric OS device

NOTE
This threshold is only available for Fabric OS devices.

NOTE
This feature requires a Trial or Licensed version.

To view all thresholds assigned to a specific switch, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Right-click anywhere in the **Ports** table and select **Expand**.
3. Right-click the device for which you want to view threshold information and select **Switch Thresholds**.

   The **Switch Thresholds** dialog box displays with a list of all thresholds assigned to the selected switch.

4. Review the **Thresholds** table.
    - **#** (Number) — The line number for each threshold in the table.
    - **Status** — The threshold status.
    - **Directly Assigned Indicator** — Whether or not the threshold was directly assigned.
    - **Name** — The threshold name.
    - **Limit** — The number of events required to trigger the threshold.
    - **Period** — The time limit required (for the number of events) to trigger a port blocking action.
    - **Area** — The threshold type.
    - **Class** — The port type.
    - **Disabled on Ports** — The port numbers on which the threshold is disabled.
5. Click **Close** on the **Switch Thresholds** dialog box.
6. Click **OK** on the **Port Fencing** dialog box.

Removing thresholds

When you assign a new threshold to an object, the threshold that was active on that object is automatically removed. The Management application also allows you to remove thresholds from an individual Fabric, Switch, or Switch Port, from all Fabrics, Switches, and Switch Ports at once, as well as from the **Threshold** table.

Removing thresholds from individual objects

To remove thresholds from the All Fabrics object, an individual Fabric, Chassis group, Switch, or Switch Port, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

    The **Port Fencing** dialog box displays.
2. Select a threshold type from the **Violation Type** list.
3. Select the object with the threshold you want to remove in the **Ports** table.
4. Click the left arrow.

NOTE
If the selected object inherits a threshold assignment from an object higher in the tree, you cannot remove the threshold. However, you may assign a different threshold directly to the selected subordinate objects or change the assignment on the higher object.

A removed icon ( ) displays next to every instance where the threshold was removed from a selected object and it does not inherits a threshold from higher in the tree.

If an inherited threshold replaces the removed threshold, an added icon ( ) displays next to every instance where the threshold was replaced.

A directly assigned icon ( ) displays next to each object with an assigned threshold which does not inherit a threshold from higher in the tree.

NOTE
If you remove a threshold from All Fabrics, it removes the threshold from individual Fabrics, switches, and switch ports in all Fabrics except for a Chassis group. You must remove repeat the procedure for the Chassis group.

5. Click **OK** on the **Port Fencing** dialog box.

Removing thresholds from the thresholds table

To remove thresholds from all Fabrics, Switches, and Switch Ports as well as the **Threshold** table, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select a threshold type from the **Violation Type** list.
3. Select the threshold you want to remove in the **Thresholds** table.
4. Click **Delete**.

   A removed icon ( ) displays next to the selected threshold in the **Thresholds** table when you click **Delete**.

5. Click **OK** on the **Port Fencing** dialog box.

Chapter

21

FICON Environments

In this chapter

FICON configurations

NOTE
FICON configurations are available only for Fabric OS products.

IBM Fibre Connection (FICON) is a protocol used between IBM (and compatible) mainframes and storage. FICON configurations can be categorized into three types, based on complexity:

- Point-to-point configurations that do not use a switch.
- Switched point-to-point configurations, also called single switch configurations, connect a host channel to a storage control unit using a single switch. In this type of configuration, the channel is configured to use single-byte addressing.
- Cascaded configurations, also called high integrity fabrics, connect host channels and storage control units that reside in different domains. Cascaded FICON fabrics must be configured as high integrity fabrics. In this type of configuration, the channel is configured to use two-byte link addressing. Figure 250 and Figure 251 are examples of cascaded FICON configurations. IBM does not support configurations that have more than two domains in a path from a FICON Channel interface to a FICON Control Unit interface to Channel-to-Channel (CTC) except under special circumstances.

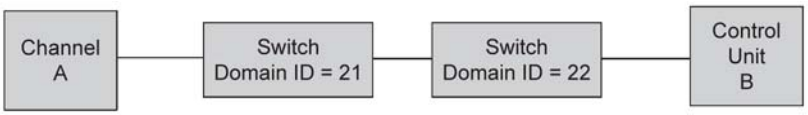


FIGURE 250 Cascaded configuration, two domains

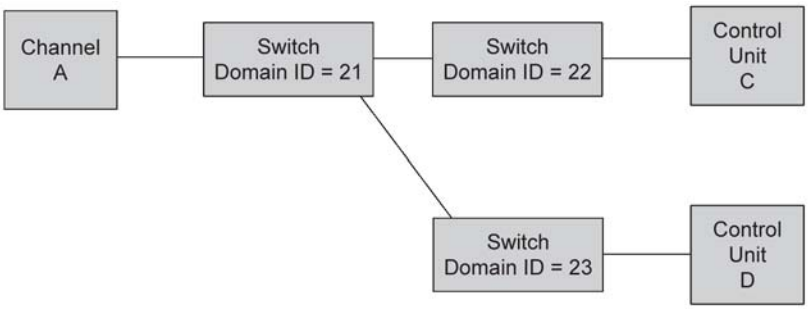


FIGURE 251 Cascaded configuration, three domains, but only two in a path

Configuring a switch for FICON operation

This section provides a basic guide for configuring a switch for FICON operation. Procedures assume that the switch is installed and IP addresses are assigned to the switch for discovery and access by the Management application. These procedures may refer to additional sections in this chapter or chapters in this manual for more detailed information.

Planning the configuration

Perform the following tasks to plan your configuration:

1. Obtain a high-level drawing of the intended fabric configuration.
2. Obtain all required license keys for the switch and Management application features.

   Licenses must be converted from transaction codes delivered with the switch. Access to a public internet connection is required. It is highly recommended that you obtain license keys before the scheduled configuration.
3. Obtain all versions of firmware for switches that the will be managed by the Management application so that you can add them to the firmware **Repository** in step 13.

   Although switches are loaded with the latest firmware at the time of manufacture, firmware may be out of date due to switch storage and transit times. If adding a switch to an existing fabric, you may need to upgrade the existing fabric, downgrade the new switch, or use a mixture of firmware in the fabric. Note that using firmware versions for switches in the same fabric that vary by one release is not recommended.

Observe the following best practices:

- Always check the version of firmware on a switch
- Unless otherwise advised by a certified Fabric OS support professional, always load the most recently qualified firmware.
- Before upgrading or downgrading firmware read the upgrade and downgrade considerations in the firmware release notes.

4. If incorporating more than one switch into a fabric, refer to planning steps in "Cascaded FICON fabric" on page 709.
5. Make a record of the following information for the switch:
    - Fabric name.
    - Switch name.
    - Domain ID (DID).

      Domain IDs are entered in either decimal or hexadecimal. If you enter the domain ID in decimal, ensure you use the correct hexadecimal equivalent. For example, if the first byte of the link address is 33, then the domain ID in decimal is 51. Also, use a domain ID that is the hexadecimal equivalent of the Switch ID in the IOCP. For example, for Switch ID 1F, set Domain ID to 31 in decimal or 1F in hexadecimal.

      The recommended best practice is the make the hexadecimal equivalent of the domain ID match the switch ID in HCD or IOCP. Also, use a unique domain ID for every switch, although this is obviously not possible in very large data centers.

    - Fabric ID (FID).

      Configure a FID if you are enabling a virtual fabric. A FID can be any number between 1-128, and all switches in the same fabric must have the same FID. Note that FMS cannot be enabled in the default switch on the 8-slot Backbone Chassis or 16 Gbps 8-slot Backbone Chassis. Therefore, the recommended best practice is leave the default switch FID at 128 and create a new logical switch for all FICON ports. A simple FID numbering scheme starting from 1 is recommended. There is no correlation between the FID and the DID.

    - Management IP address.
    - Administrator password.

      Although the Management application is typically configured for managing the switch as an admin user, root will also work. The default admin password is "password." You do not need to change the password during installation; however if the password is changed, the password for device discovery must be changed also. Although launched from the Management application, Element Manager (Web Tools) passwords do not propagate the Management application.

      The recommended best practice is to create identical passwords for all switches in the same fabric. This not only simplifies discovery, but in most cases since users are given access to a fabric, not an individual switch, there are fewer passwords to remember and maintain.

    - Call home number.

      This may not apply. If using a call home service you will need the phone number for the service and an understanding of what is being covered in the service agreement.

- Required firmware for the switch. Refer to step 3.
- Port addressing.

  The port address is important because it is implemented in HCD or IOCP. The easiest port addressing scheme is to start from 0x00 at the bottom left of the port card, increment on ports going up the card, then continue starting numbering from the bottom right of the next column of ports. Any port addressing scheme is possible however.

6. If you are considering creating a cascaded switch configuration, consider connecting all ISLs between switches first. This will help simplify cascaded configuration. If this is not possible, you can merge cascaded fabrics later using steps in "Cascaded FICON fabric merge" on page 712.
7. If you are considering connecting cascaded switches over IP networks, refer to the planning considerations in the "Connecting cascaded FICON fabrics over FCIP" in Chapter 22, "Fibre Channel over IP".

Configuring the switch

Perform the following steps to configure a switch for FICON operation.

1. Launch the Management application and select the **SAN** tab.

   NOTE
   The recommended best practice is to run the application client from a server other than the Management application server itself. Sometimes during installation this is not practical. To start a client on the Management application server, double click on the application icon. To open a client from a system other than the Management application server, open a browser and enter the IP address of the Management application server.

2. Configure the Management application display for FICON. Refer to the "Setting your FICON display" section of Chapter 5, "Application Configuration".
3. Select the Decimal-Hex drop down selector on the tool bar at the top of the **SAN** tab to display domain IDs and port numbers in hex format.
4. Select **Discover > Fabrics**.

   The **Discover Fabrics** dialog box displays. If the switch is already in a fabric, it is automatically added and should display under the discovered fabric. If the switch does not display, perform step 5 and step 6.

5. Select **Add** on the **Discover Fabrics** dialog box.

   The **Add Fabric Discovery** dialog box displays.

6. Perform one of the following tasks to configure a switch for discovery:

   - Add information for the switch in the **IP Address** tab and click **OK**.

     FIGURE 252 Add Fabric Discovery dialog box (IP Address tab)

     NOTE
     Selecting **Automatic** to use the SNMPv3 profile is recommended.

- To manually configure SNMP for discovery, select **Manual** to activate the **SNMP** tab, then select the **SNMP** tab. Fill out the fields as required.

FIGURE 253 Add Fabric Discovery dialog box (SNMP tab)

Refer to the "SAN discovery overview" section in Chapter 3, "Discovery" for more information on using these dialog boxes.

7. Add all required licenses to the switch using the following steps:
   a. Select a discovered switch from the Product List panel, and then select **Element Manager > Admin**.

      The Web Works **Switch Administration** window displays.

   b. Select the **License** tab and click **Add**.

      The **Add License** dialog box displays.

   c. Past or enter the license key in the **License Key** field.

   d. Click **Add License**.

   e. Repeat steps b through d for additional licenses.

   f. Click **Refresh** to display new licenses in the **License** tab.

8. As an optional step, manage switch users by selecting the **User** tab on the Web Works **Switch Administration** window. Use this tab to add users, change passwords, or perform other steps to manage switch users.

NOTE
If you change the password for a user that was used for Management application discovery, you must delete the switch from the **Discover Fabrics** dialog box, and then discover the switch again with the new login credentials.

9. To download firmware to the switch, select **Configure > Firmware Management** from the **SAN** tab on the Management application window as shown in Figure 254 on page 700.

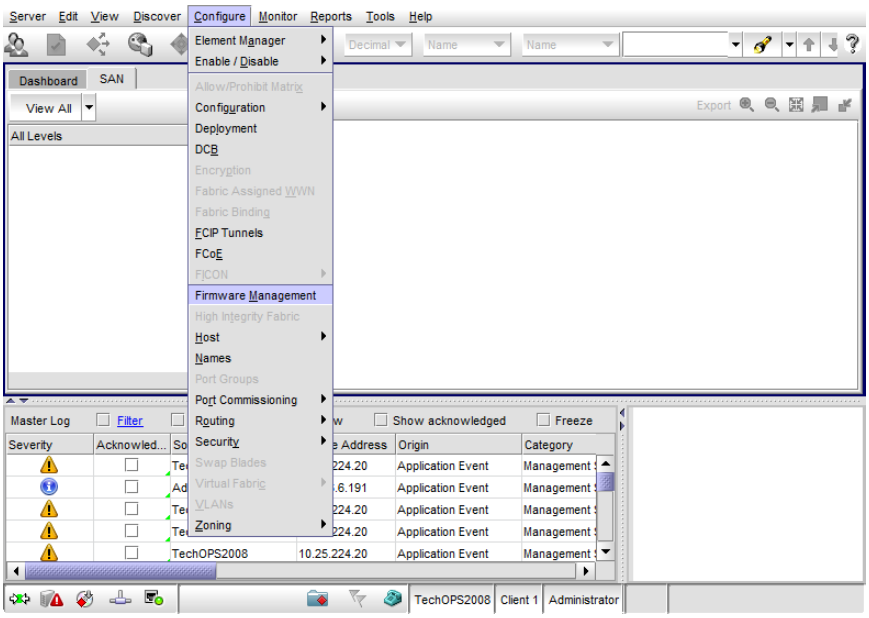


FIGURE 254 Selecting Firmware Management from Configure menu

The **Firmware Management** dialog box displays.

10. Select the **Download** tab (Figure 255).

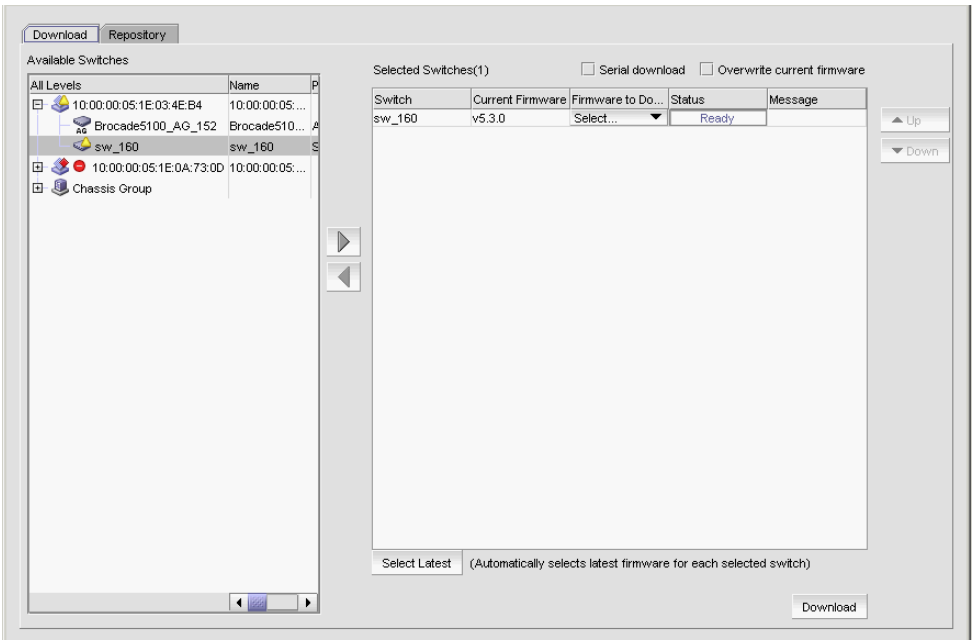


FIGURE 255 Firmware download

11. Select the switches in the **Available Switches** panel where you want to download firmware, and then click the right arrow to move them under **Selected Switches**.
12. Click **Download**.

13. Select the **Repository** tab to import new firmware files for downloads. Refer to the "Firmware management" section in Chapter 12, "SAN Device Configuration" for more information on importing firmware.
14. If you are not using virtual fabrics or you do not plan to enable virtual fabrics and only use the default switch, skip to step 15. As an option at this point, you can configure virtual fabrics by referring to procedures in the following sections under "Configuring Virtual Fabrics" in the "Virtual Fabrics" chapter, then return to step 15.
    - "Enabling Virtual Fabrics"
    - "Creating a logical switch or base switch"
    - "Assigning ports to a logical switch"

    For best practices for configuring virtual fabrics, refer to "FICON best practices for Virtual Fabrics" on page 551.
15. To configure the switch as part of a fabric, follow procedures under "Configuring a cascaded FICON fabric" on page 710, then return to step 16.
16. If a name does not display for the switch after configuring the fabric, right click the switch icon in topology of the SAN tab and select **Properties**.

    The switch **Properties** dialog box displays.
17. Edit the switch name.
18. Define port fencing parameters for the switch using the following steps (optional):

    NOTE
    Although this is an optional step, best practice is to configure port fencing.

    a. Configure thresholds that you require for the switch using steps under the "Adding thresholds" in Chapter 20, "Port Fencing".

       Following are recommend parameters for the various thresholds:
       - C3 Discard Frames = 2 per minute.
       - Invalid Words = 25 per minute.
       - Invalid CRCs = 3 per minute. Note that it is not uncommon for an ISL to travel through a path that is more prone to noise than internal data center connections to control units and channels. Therefore, a slightly higher CRC threshold may be better for E-Port connections. In most cases the CRC is set to 3.
       - Link Reset = 2 per minute.
       - Protocol Error = 2 per minute.
       - State Change = 7 per minute.

    b. Assign a threshold to the switch using steps under "Assigning thresholds" in Chapter 20, "Port Fencing".
19. Set the zoning policy for the switch by referring to steps under "Enabling or disabling the default zone for fabrics" in Chapter 19, "Zoning".

The recommended policy is to disable the default zone (No Access). Although enabling the default zone (All Access) can be used for FICON environments, prohibiting connection between ports using the **Configure Allow/Prohibit Matrix** dialog box requires activating at least one zone. Even if you do not want to prohibit connections using the matrix, configuring a single zone containing all ports provides the same benefits as All Access, while providing flexibility to configure "prohibits" or more restrictive zoning in the future. In addition, when moving an ISL in the future, there will not need to modify zoning.

20. Configure zoning using steps under "Configuring zoning" in Chapter 19, "Zoning".

    Be sure to reference the "Zoning and FICON" section of Chapter 19, "Zoning" for more information on FICON environments.

21. Configure the Allow/Prohibit Matrix for the switch using steps under "Configuring an Allow/Prohibit Matrix" on page 702.

22. Configure Call Home by referring to procedures in Chapter 10, "Call Home".

    NOTE
    The call home number and the events to trigger a call home depend on your service contract and service provider. Contact your service provider for additional information.

23. Enable bottleneck detection using the following Fabric OS **bottlneckmon** commands:

    - **bottleneckmon –cfgcredittools -intport -recover onLrOnly** - This command monitors for lost credits on links. This is necessary because occasional errors on links can cause lost credits that can result in IFCCs and poor performance over time.
    - **bottleneckmon –enable -alert** - This command causes AN-1004 RAS log messages to generate whenever congestion occurs and AN-1010 RAS log messages to generate whenever severe congestion occurs. The recommended best practice is to enable alerts now so that you don't forget when you merging the fabrics.

    The **bottlneckmon** command operates the entire chassis, regardless of the FID where it is executed.

24. Clear error counters (common during switch configuration) by right-clicking the switch in the Connectivity Map or Product List and selecting **Performance > Clear Counters**.

Configuring FICON display

You can set display settings for FICON display so that the columns of any table that contains end device descriptions to move the following eight columns to be the first columns: FC Address, Serial #, Tag, Device Type, Model, Vendor, Port Type, and WWN.

Configuring an Allow/Prohibit Matrix

The Allow/Prohibit Matrix is a FICON port attribute that can be used to prohibit communication between specific ports. Allow/Prohibit Matrix are not recommended on E_Ports (inter-switch links).

The Allow/Prohibit Matrix can be manipulated by host-based management programs using FICON Control Unit Port (CUP), or from a Management application program to create policies and determine paths for data and command flows. Up to eight Allow/Prohibit matrices can be modified at the same time. Allow/Prohibit Matrix settings apply per switch rather than per fabric, and only work when an active zone configuration is present in the fabric.

Multiple configurations can be defined, edited, copied, or removed. Only one configuration can be active per switch.

Configuring the Allow/Prohibit matrix requires that a zone configuration be activated on the fabric. Prohibits can be configured without an active zone configuration, but they cannot be enforced until an effective zone is configured.

1. Select **Configure > Allow/Prohibit Matrix**.

   The **Configure Allow/Prohibit Matrix** dialog box displays.

2. Select a switch from **Available Switches**.

   Two default configurations (Active and IPL) are displayed in a tree structure under the switch. Existing configurations are also displayed.

3. Choose one of the following options:

   - Double-click a configuration file.
   - Select a configuration file and click the right arrow.

   A matrix displays in the **Allow/Prohibit Matrix** panel. The switch ports are displayed on both the vertical axis and horizontal axis. An Allow icon ( ) indicates communication is allowed between the ports, as shown in Figure 256 on page 703.

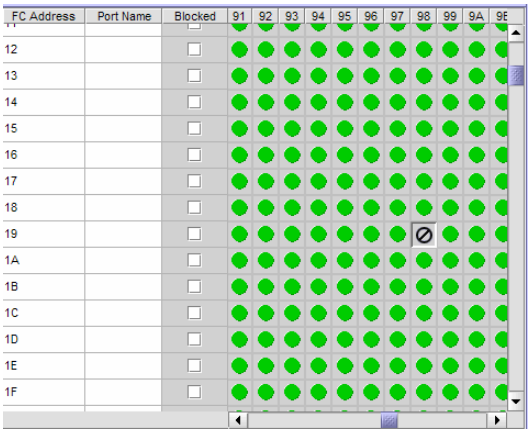


FIGURE 256 Active Configuration in Allow/Prohibit Matrix panel

4. Prohibit a connection between two ports by clicking the intersection point between the ports.

   A prohibit icon ( ) displays at the intersection point. If you know the port addresses of the ports for which you want to prohibit or allow communication and do not want to search the matrix for the exact port intersection point, use the procedure in "Configuring an Allow/Prohibit Matrix manually" on page 704.

5. Repeat step 4 as needed to create the matrix you want to apply. If you want to change a selection from prohibit to allow, click the intersection point to clear the prohibit icon.

6. When you have completed the matrix, click **Save** if you started with a new matrix, or **Save As** to save a copy of an existing matrix.
7. Click **Analyze Zone Conflicts**.

   This operation can be done before or after a configuration is saved. This operation checks the current zoning settings for conflicts with settings in the Allow/Prohibit Matrix. Zone conflict is analyzed against the switch for port zoning only. The table cells display in the red background if the two ports are not in the same zone in an active zone configuration.
8. Click **Close** on the **Configure Allow/Prohibit Matrix** dialog box.

Configuring an Allow/Prohibit Matrix manually

To configure to allow or prohibit communication between specific ports manually, complete the following steps.

1. Select **Configure > Allow/Prohibit Matrix**.

   The **Configure Allow/Prohibit Matrix** dialog box displays.
2. Select a switch from **Available Switches**.

   Two default configurations (Active and IPL) are displayed in a tree structure under the switch. Existing configurations are also displayed.
3. Choose one of the following options:
   - Double-click a configuration file.
   - Select a configuration file and click the right arrow.

   A matrix displays. The switch ports are displayed on both the vertical axis and horizontal axis. An Allow icon ( ) indicates communication is allowed between the ports.
4. Click **Manual Allow/Prohibit**.

   The **Manual Allow/Prohibit** dialog box displays, as shown in Figure 257 on page 704.

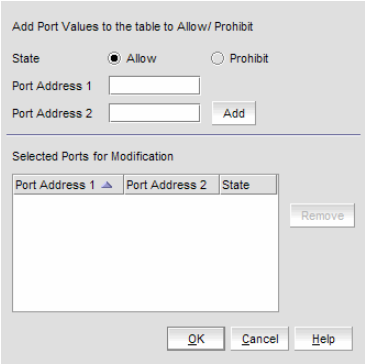


FIGURE 257 Manual Allow/Prohibit dialog box

NOTE
The **Manual Allow/Prohibit** dialog box is only available for Fabric OS products.

5. Select one of the following options:

- Select **Allow** to allow communication between two specific ports.
- Select **Prohibit** to prohibit communication between two specific ports.

6. Enter the port number of the first port for which you want to allow or prohibit communication in the **Port Address 1** field.
7. Enter the port number of the second port for which you want to allow or prohibit communication in the **Port Address 2** field.
8. Click **Add**.

   The information displays in the **Selected Ports for Modification** list.

   To delete any of these manual configurations, select the configuration you want to delete in the **Selected Ports for Modification** list and click **Remove**.

   The **Selected Ports for Modification** list displays the following information:

   - **Port Address 1** column — The port number of the first port for which you want to allow or prohibit communication.
   - **Port Address 2** column — The port number of the second port for which you want to allow or prohibit communication.
   - **State** column — Whether you want to allow or prohibit communication.

9. Repeat step 5 through step 8 for each allow or prohibit configuration.
10. Click **OK** on the **Manual Allow/Prohibit** dialog box.
11. When you have completed the matrix, click **Save** if you started with a new matrix, or **Save As** if you edited a copy of an existing matrix.
12. Click **Analyze Zone Conflicts**.

    This operation can be done before or after a configuration is saved. This operation checks the current zoning settings for conflicts with settings in the Allow/Prohibit Matrix. Zone conflict is analyzed against the switch for port zoning only. The table cells display in the red background if the two ports are not in the same zone in an active zone configuration.
13. Click **Close** on the **Configure Allow/Prohibit Matrix** dialog box.

Saving or copying Allow/Prohibit Matrix configurations to another device

When copying or saving a configuration from a small switch (source switch with fewer ports; for example, 64 ports) to a larger switch (destination switch with a larger number of ports; for example, 256 ports) only the port address range of the smaller switch will be affected on the larger switch. All additional port addresses will display the default settings (port state defaults to “Allow” and the **Blocked** check box defaults to cleared).

Copying or saving a configuration from a larger switch to a smaller device only copies or saves the port address range that matches the smaller switch. Additionally a message displays that the additional port addresses from the larger switch are discarded.

When copying or saving a configuration from or to logical switches, the only ports affected are the port addresses defined in the logical switch. The FICONd CUP Daemon retains the full compliment of records regardless of the size of the logical switch. Therefore, copying or saving a configuration from or to logical switches should work the same as copying or saving between standard switches.

Copying an Allow/Prohibit Matrix configuration

To duplicate an existing Allow/Prohibit Matrix configuration, complete the following steps.

1. Select **Configure > Allow/Prohibit Matrix**.

   The **Configure Allow/Prohibit Matrix** dialog box displays.

2. Select the Allow/Prohibit Matrix configuration you want to copy.

   You can do this by expanding the view for the switch under **Available Switches** and selecting a configuration, or you can select the matrix under **Allow/Prohibit Matrix**.

3. Click **Duplicate**.

   The **Save As/Duplicate** dialog box displays, as shown in Figure 258 on page 706.

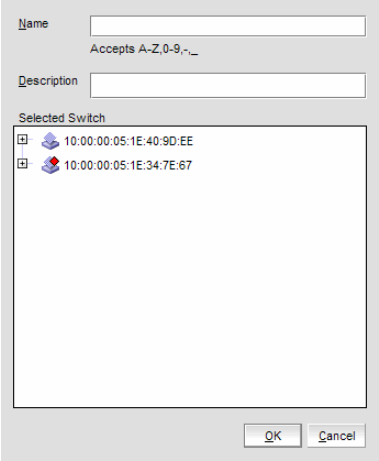


FIGURE 258 Save As/Duplicate dialog box

4. Enter a name for the configuration.
5. Enter a description for the configuration.
6. Select the check box for the switch to which you want to save the configuration in the **Selected Switch** list.
7. Click **OK**.

   A message displays stating that the outstanding port configuration is discarded when copying a configuration from the switch with more ports to a switch with fewer ports and vice versa. Click **OK** to close the message.

   The copied configuration displays in the **Available Switches** list under the selected switch. To edit this configuration, refer to "Configuring an Allow/Prohibit Matrix" on page 702 or "Configuring an Allow/Prohibit Matrix manually" on page 704.

Saving an Allow/Prohibit Matrix configuration to another device

To save an existing Allow/Prohibit Matrix configuration to another device, complete the following steps.

1. Select **Configure > Allow/Prohibit Matrix**.

   The **Configure Allow/Prohibit Matrix** dialog box displays.

2. Select the Allow/Prohibit Matrix configuration you want to save.

   You can do this by expanding the view for the switch under **Available Switches** and selecting a configuration, or you can select the matrix under **Allow/Prohibit Matrix**.

3. Click **Save As**.

   The **Save As/Duplicate** dialog box displays, as shown in Figure 259 on page 707.

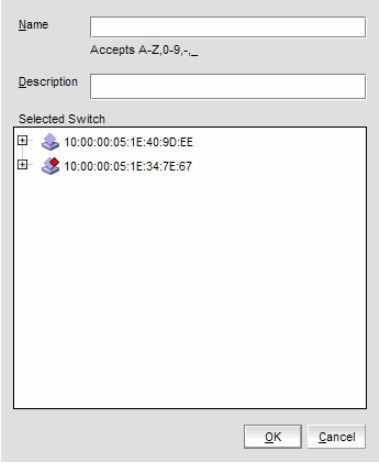


FIGURE 259 Save As/Duplicate dialog box

4. Enter a name for the configuration.
5. Enter a description for the configuration.
6. Select the check box for the device to which you want to save the configuration in the **Selected Switch** list.
7. Click **OK**.

   A message displays stating that the outstanding port configuration is discarded when copying a configuration from the switch with more ports to a switch with fewer ports and vice versa. Click **OK** to close the message.

   The saved configuration displays in the **Available Switches** table under the selected switch. To edit this configuration, refer to "Configuring an Allow/Prohibit Matrix" on page 702 or "Configuring an Allow/Prohibit Matrix manually" on page 704.

Activating an Allow/Prohibit Matrix configuration

You must have an active zone configuration before you can activate an Allow/Prohibit Matrix configuration.

1. Select **Configure > Allow/Prohibit Matrix**.

   The **Configure Allow/Prohibit Matrix** dialog box displays.

2. Select the Allow/Prohibit Matrix configuration you want to activate.
   You can do this by expanding the view for the switch under **Available Switches** and selecting a configuration, or you may select the matrix under **Allow/Prohibit Matrix**.

3. Click **Activate**.

   A confirmation message displays, as shown in Figure 260 on page 708.

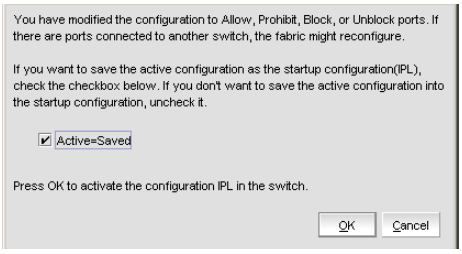


FIGURE 260 Activate Matrix Confirmation message

4. Select the **Active=Saved** check box to save the active configuration as the startup configuration (IPL).

5. Click **OK** to confirm.

   If you select the **Active=Saved** check box, the text [=Active] is appended to the IPL file in the **Configure Allow/Prohibit Matrix** dialog box.

   The **Active=Saved** check box and the IPL filename represent the current state of the Active=Saved Mode (ASM) bit on the switch. However, this is limited to changes done to the ASM configuration through the Management application. If changes occur through external means (such as, Webtools or the CLI) the changes are not reflected in the Management application until the **Configure Allow/Prohibit Matrix** dialog box is re-launched.

NOTE
Active=Saved" means the matrix configuration will survive a power failure. If not selected, all ports can access each other after power is restored.

Deleting an Allow/Prohibit Matrix configuration

You cannot delete the active configuration, the IPL configuration, or a configuration that is marked as having uncommitted changes.

1. Select **Configure > Allow/Prohibit Matrix**.

   The **Configure Allow/Prohibit Matrix** dialog box displays.

2. Select the Allow/Prohibit Matrix configuration you want to delete.
   You can do this by expanding the view for the switch under **Available Switches** and selecting a configuration, or you can select the matrix under **Allow/Prohibit Matrix**.
3. Click **Delete**.

   A confirmation message displays.
4. Click **Yes** to confirm.

Changing the Allow/Prohibit Matrix display

You can modify the matrix display on the **Configure Allow/Prohibit Matrix** dialog box using the **Window Arrangement** list above the matrix display or the **Clear all port names** option below the display.

Changing window arrangement

There are three options for the **Allow/Prohibit Matrix** display on the **Configure Allow/Prohibit Matrix** dialog box located in the **Window Arrangement** list above the display.

- The matrix definitions may be cascaded (this is the default view).
- The matrix definitions may be tiled horizontally.
- The matrix definitions may be tiled vertically.

Perform the following steps to change the display to the desired format.

1. Select **Configure > Allow/Prohibit Matrix**.

   The **Configure Allow/Prohibit Matrix** dialog box displays.
2. Select **Cascade**, **Tile Horizontally**, or **Tile Vertically** from the **Window Arrangement** list.

Clearing port names

Use the following steps to clear all port names from the selected matrix.

1. Select **Clear Port Names** below the matrix display.

   A warning displays asking you to confirm the operation.
2. Select **Yes** to clear all port names from the matrix or select **No** to cancel the operation.

Cascaded FICON fabric

NOTE
You must have FICON Management privileges to configure a fabric for cascaded FICON.

The Management application enables you to easily configure a fabric for cascaded FICON. Note that configuring a fabric for cascaded FICON may be disruptive to current I/O operations in the fabric, as this involves disabling and enabling the switches in the fabric.

FICON configuration performs the following operations on the selected fabric:

- Turns on the insistent domain ID flag (IDID) on all switches.
- Sets High Integrity Fabric Configuration (HIFC) on the seed switch.
  - Fabric-wide consistency policy (FWCP) is configured to include SCC in strict mode.
  - SCC policy is created or modified to limit connectivity to only the switches in the selected fabric.
- Enables port-based routing on all switches.
- Enables In-Order Delivery (IOD) on all switches.
- Enables Dynamic Load Sharing (DLS) based on user selection and the firmware level.

NOTE
To enable DLS, all switches in the fabric must be 8 Gbps or faster and running Fabric OS 6.4 or later.

- (Optional) Turns on FICON Management Server (FMS) mode on all switches.

  Consider the following information when enabling FMS mode.

  - If switches are running Fabric OS 7.0 and later, FMS will not be enabled unless the switches have an active CUP license.
  - If switches are running Fabric OS earlier than version 7.0 and do not have a CUP license, after successful configuration, you can access the Port Connectivity (Allow/Prohibit) matrix, but the host system cannot communicate with the FICON Management Server unless you install a CUP license. If a CUP license is later installed on these switches, then FMS mode must be re-enabled on these switches.
  - For logical fabrics running Fabric OS v7.1 or later, you can enable FMS mode when logical switches are configured to allow XISL use.

Configuring a cascaded FICON fabric

The FICON wizard automatically creates HIFC settings that support a cascaded FICON fabric.

1. Select **Configure > FICON > Configure Fabric** or right-click a fabric in the product tree and select **FICON > Configure Fabric**.

   The **Configure Cascaded FICON Fabric** screen of the **FICON Configuration** dialog displays, as shown in Figure 261 on page 711.

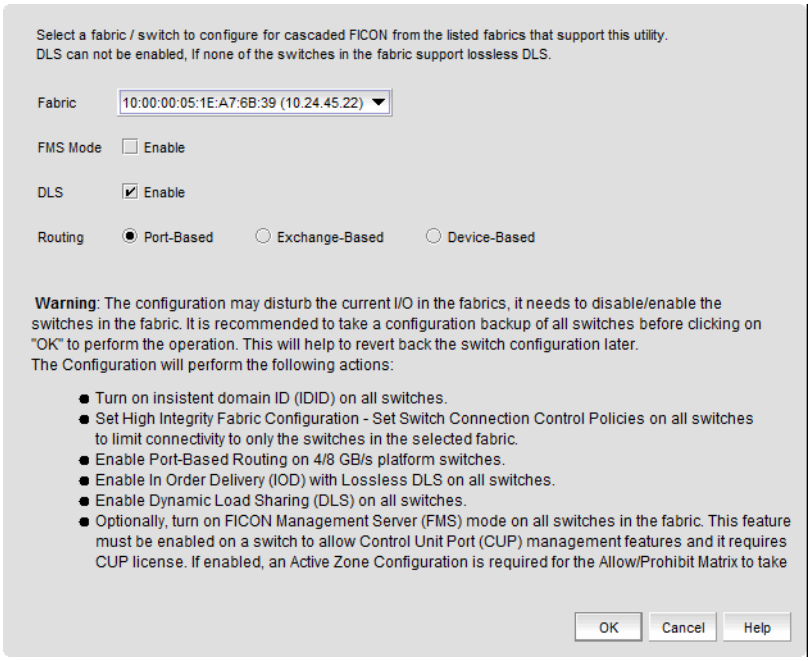


FIGURE 261 Configure Cascaded FICON Fabric / Switch dialog box

2. Use the **Fabric** list to select the fabric you want to configure.

NOTE
(Fabric OS switches only) All switches in a fabric must be running Fabric OS version 5.3 or later. If a Fabric OS version earlier than version 5.3 is present in the topology, the fabric is not listed.

3. Select the **FMS Mode** check box to manage the fabric by a host-based management program using FICON CUP protocol.

   If you select **FMS Mode**, each switch is checked for a CUP license. Any switches that do not have a CUP license are listed, with a reminder that a CUP license is necessary to communicate with the FICON Management Server.

4. Select the **DLS** check box to enable Dynamic Load Sharing (DLS) or Lossless DLS only on switches that support lossless DLS. For more information, refer to "Enabling DLS" on page 712. You must enable DLS to select routing policies.

5. Select one of the following options to enable port-based, exchange-based, or device-based routing on switches:

   - **Port-Based**, enables port-based routing on 4 Gbps platform switches.
   - **Exchange-Based**, enables exchange-based routing for the fabric if all switches are 8 Gbps or greater platforms running Fabric OS 6.4 or later. If these requirements are not met, an error message displays.
   - **Device-Based**, enables device-based routing for the fabric if all switches in the fabric are 8 Gbps or greater platforms running Fabric OS 7.1 or later. If these requirements are not met, an error message displays.

NOTE
Either exchange based routing, port based routing, or device-based routing is enabled on all switches of the selected fabric. You cannot enable a mixed routing policy.

6. Click **OK** if you want to proceed.

   A warning message displays listing the switches of the selected fabric that are to be disabled and re-enabled in order to enable the desired routing policy and IDID.

7. Click **Yes** to continue.

   If configuration is successful, a confirmation message displays.

   If **FMS Mode** was selected, each switch is checked for a CUP license. Any switches that do not have a CUP license are listed, with a reminder that a CUP license is necessary to communicate with the S/B FICON Management Server.

NOTE
FMS mode cannot be enabled on switches running Fabric OS 7.0 and later unless the switches have an active CUP license.

Enabling DLS

Consider the following when enabling Dynamic Load Sharing (DLS) in step 4:

- DLS requires DLS support on the switch. Lossless DLS requires Lossless DLS support on the switch.
- Enabling DLS will enable IOD without Lossless DLS on all other switches, enable DLS on switches that support DLS, and disable DLS on all other switches.
- DLS is only supported on the 40-port, 8 Gbps FC Switch, 80-port, 8 Gbps FC Switch, 512-port Backbone Chassis, and 4-slot Backbone Chassis.
- Enabling DLS may result in dropped frames when paths fail over. It is recommended that you set the preferred IOD delay time to minimize frame drops.
- To enable DLS, all switches in the fabric must be 8 Gbps or faster and running Fabric OS 6.4 or later.

Cascaded FICON fabric merge

The Management application provides a wizard to help you merge two fabrics for cascaded FICON. Note that merging two cascaded FICON fabrics may be disruptive to current I/O operations in both fabrics as this involves disabling and enabling the switches in both fabrics. The merge process will not make any configuration changes on the primary (production) fabric that are disruptive.

NOTE
It is recommended that you run a configuration backup on all switches before performing the fabric merge. This helps you to revert back the switch configurations later.

The cascaded FICON fabrics merge wizard performs the following operations:

- Checks the primary and secondary fabrics for any merge issues.

- Configures High Integrity Fabric Configuration (HIFC) on the seed switch of the primary and secondary fabric.
  - SCC policy will be created or modified to limit connectivity to switches from both fabrics.
  - Configures Fabric-Wide Consistency Policy (FWCP) on both fabrics.
  - FWCP is configured in tolerant mode for SCC for an Fibre Channel Routing (FCR) fabric.
- Enables Port-Based Routing (PBR) on all switches in the secondary fabric if all the switches in the primary fabric are found to be enabled for PBR. Note that a mixed policy of Exchanged-Based Routing (EBR), Device-Based Routing (DBR) and PBR cannot be enabled on a fabric.
- Enables Exchange-Based Routing (EBR) on all switches in the secondary fabric if all switches in the primary fabric are enabled for EBR. Note that EBR requires that switches operate at 8 Gbps or greater with Fabric OS 6.4 or later. If all the EBR-enabled switches in the primary fabric are found to meet these requirements and a switch in the secondary fabric does not meet these requirements, an error message displays. Note that a mixed policy of EBR and PBR cannot be enabled on a fabric.
- Enables Device-Based Routing (DBR) on all switches in the secondary fabric if all switches in the primary fabric are enabled for DBR. Note that DBR requires that switches operate at 8 Gbps or greater with Fabric OS 7.1 or later. If all the DBR-enabled switches in the primary fabric are found to meet these requirements and a switch in the secondary fabric does not meet these requirements, an error message displays. Note that a mixed policy of PBR, EBR, and DBR cannot be enabled on a fabric.
- (Optional) Turns on FICON Management Server (FMS) mode on all switches. If some switches already have FMS mode enabled, it is re-enabled.

  Consider the following information when enabling FMS mode.
  - If switches are running Fabric OS 7.0 and later, FMS will not be enabled unless the switches have an active CUP license.
  - If switches are running Fabric OS earlier than version 7.0 and do not have a CUP license, after successful configuration, you can access the Port Connectivity (Allow/Prohibit) matrix, but the host system cannot communicate with the FICON Management Server unless you install a CUP license. If a CUP license is later installed on these switches, then FMS mode must be re-enabled on these switches.
  - For logical fabrics running Fabric OS v7.1 or later, you can enable FMS mode when logical switches are configured to allow XISL use.
- (Optional) Configures long distance settings on selected ports of primary and secondary fabrics (requires an Extended Fabric license).

NOTE
If the distance between the merged fabrics is 10 km or greater, you must configure the connection as a long distance connection.

Note that the merge wizard does not enable primary fabric switches for DLS, In-Order Delivery (IOD), insistent domain ID flag (IDID), and Advanced Performance Tuning (APT).

- In-Order Delivery (IOD) will be enabled on all switches in the secondary fabric.
- Dynamic Load Sharing (DLS) will be enabled on switches in the secondary fabric that are operating at 8 Gbps or greater and are running Fabric OS 6.3 or later.

NOTE
To enable DLS, all switches in the fabric must be 8 Gbps or faster and running Fabric OS 6.3 or later.

- Primary fabric switches will not be disturbed for disruptive operations, such as IDID and APT. Instead, all primary fabric switches will be validated for current routing policies and the same policies will be enabled on all the secondary fabric switches.

The cascaded FICON fabrics merge wizard performs the following operations to avoid Active Directory (AD), Access Control List (ACL), and zone database merge conflicts between the two fabrics:

- Clears Admin Domain, Access Control Lists (ACLs), and zone databases, if they exist, from the secondary fabric that you select within the wizard.

NOTE
Clearing the ACL database in a large fabric can take a long time; for example, in a 50-switch fabric, this operation can take from 30 minutes to 1 hour.

- Sets the default zoning configuration on the secondary fabric to match the default zoning status of the primary fabric.
- Modifies ACL policy on the secondary fabric to match the primary fabric parameters, including Accept Distribution and FWCP.
- Sets FWCP in strict mode for SCC for the primary fabric.
- Sets FWCP in tolerant mode for the Fibre Channel Routing (FCR) fabric.

Merging two cascaded FICON fabrics

If you want to join two cascaded FICON fabrics, they must be merged. If the distance between fabrics is 10 km or more, an Extended Fabrics license is required, and an extra step is required to configure the connection as a long distance connection. To successfully configure a long distance connection, use the same E_Ports and cable distance values used when configuring Extended Fabrics. For long distance connections, it is recommended that you create the Extended Fabrics configuration first, have an active connection, and have the E_Port and cable distances values ready before you merge the fabrics.

1. Select **Configure > FICON > Merge Fabrics** or right-click a fabric in the product tree and select **FICON > Merge Fabrics**.

   The **Overview** screen of the cascade FICON fabrics merge wizard displays.

   NOTE
   Cascade FICON fabrics merge wizard is only available for Fabric OS products.

2. Click **Next**.

   The **Select fabrics** screen displays.

3. Select the two fabrics you want to merge under **Available Fabrics**, and click the right arrow to move them to **Selected Fabrics**. You may do this one fabric at a time, or select both by pressing **CTRL** and then clicking each fabric.

NOTE
All switches in a fabric must be running Fabric OS version 5.3 or later and must be reachable. If a Fabric OS version earlier than version 5.3 is present in the fabric, the fabric is not listed.

NOTE
Switches running Fabric OS 6.3 or earlier cannot be merged with switches running Fabric OS 6.4 or later.

NOTE
For 8 Gbps switches, all switches in the fabric must be 8 Gbps or faster. 8 Gbps switches cannot be merged with switches that have SFP transceivers with a speed less than 8 Gbps.

4. Click **Next**.

   The **Set up merge options** screen displays.

5. Select **FMS Mode** to manage the fabric by a host-based management program using FICON CUP protocol. Note that you cannot enable FMS mode on switches running Fabric OS 7.0 or later unless they have an active CUP license.

6. Select a secondary fabric where AD, ACL, and zone databases, if defined, will be cleared.

7. Read the bulleted list of actions so you understand the actions that are taken to avoid conflicts when the fabrics are merged.

8. Click **Next**.

   The **Check merge** screen displays.

   A **Status details** table shows progress through merge check points. A rotating arrow under **Status** indicates a **Merge check** step is in progress. A blue check mark indicates successful completion of that **Merge check**. A red stop sign indicates a failed step. If the configuration is successful, all configuration items have blue check marks.

9. If the merge fails, but is recoverable, click **Resolve**.

10. If desired, click **Check Merge Again** to run the merge check test again.

11. Click **Next** to continue.

    The **Configure long distance (optional)** dialog box displays. If the distance between the merged fabrics is 10 km or greater, you must configure the connection as a long distance connection. Selecting a distance invokes an algorithm to compute the required number of BB credits available to the port. The longer the link, the greater latency, resulting in the potential for more outstanding frames in the link, and the need for more BB credits. FICON may require more BB credits than the algorithm provides, and it is a good practice to specify a distance that is longer than the actual distance to be sure enough BB credits are allocated.

12. Perform the appropriate following action based on whether the connection is a long distance connection:

    - If it is not a long distance connection, click **Next** to view the **Configure merge** screen. Proceed to step 13.
    - If it is a long distance connection, expand the fabrics under **Selected Fabrics** to the switch port level.

a. Select the E_Ports used for the connection on the local switch and on the remote switch, and click the right arrow.
The selected E_Ports are moved to **Selected Ports**.
If there is no E_Port in the selected fabrics, a warning message displays.

b. Specify the **Cable length between switch ports**.
The range is form 10 through 500 km. The default is 50 km.

c. Select **ARBs** or **IDLEs** to configure the **Fibre Channel Primitive Signal Fill Words**.
For Fabric OS version 6.1.0b or earlier, the setting is always **ARBs**. You cannot change to **IDLEs**.
For Fabric OS version 6.1.0c or later, the default setting is **IDLEs**, however, you can change it to **ARBs**.

d. Click **Next**.
The **Configure merge** screen displays.

13. Read and review the information on the **Configure merge** screen. If you understand and agree, click **Next** to confirm the information.

    A **Summary** screen displays.

14. Read the information, and click **Finish** to close the wizard.

Resolving merge conflicts

You can resolve the following types of switch configuration conflicts:

- Domain ID
- TOV
- Buffer To Buffer Credit
- Disable Device Probe

NOTE
This test will be skipped if all primary and secondary fabric switches are found to be Fabric OS 7.0 and later.

- Route Priority Per Frame
- Sequence Level Switching
- Suppress Class F
- Long Distance Setting
- Data Field Size
- VC Priority

Note that not all tests support resolution. If a test supports resolution, the **Description** column contains the text “Resolvable”.

To resolve merge conflicts, complete the following steps.

1. Select the failed test where the **Description** column contains the text “Resolvable”.
2. Click **Resolve**.

A “The switches in fabric *Name* will be disabled prior to making the configuration change. The switches will be reenabled after the configuration changes are applied. Please confirm to proceed.” warning message displays.

3. Click **OK** on the warning message.

   The values of the fabric chosen on the **Set up merge options** screen are applied to all devices in the second fabric. Once the settings are applied, the test is run again and the merge results are updated.

   If the test passes, go to step 4.

   If an error occurs, an error message displays. You must use Web Tools or the CLI to resolve this conflict. Click **OK** on the error message and go to step 4.

   If you are resolving a domain ID error, there may be multiple switches involved. If multiple switches have the domain ID error, the **Configure Domain IDs** dialog box displays listing all devices that have the domain ID conflict.

   a. Select the device for which you want to resolve the domain ID in the **Available Switches** list and click the right arrow button.

   b. Select a new domain ID for the device from the **Domain ID** list.

   c. Repeat steps a and step b for each device in the **Available Switches** list.

   d. Click **OK** on the **Configure Domain IDs** dialog box.

4. Repeat step 1 through step 3 until all resolvable tests pass.

5. Perform step 11 through step 14 of the procedure “Merging two cascaded FICON fabrics” on page 714 to finish resolving a merge conflict.

Port groups

A port group is a group of FC ports from one or more switches within the same fabric. Port groups are user-specific; you can only view and manage port groups that you create.

The ports display in the order in which you add them to the port group. The order in which you add ports to a port group is persisted in both the port group and the Allow/Prohibit Matrix. While port groups can be at the fabric level (ports from multiple switches within the same fabric), the Allow/Prohibit Matrix is at the switch level. Therefore, when you view the Allow/Prohibit Matrix for a port group with ports from multiple switches, the matrix only shows the ports for the selected switch.

To reorder the ports, you must remove the ports, save your changes, then open the **Port Groups** dialog box and add the ports back to the port group in the new order.

Once you create a port group, you can view and edit the Allow/Prohibit Matrix for the port group. Allow/Prohibit Matrix is a FICON port attribute that can be used to prohibit communication between specific ports. For more information about the Allow/Prohibit Matrix, refer to “Configuring an Allow/Prohibit Matrix” on page 702.

Creating a port group

NOTE
At least one switch must be reachable to create a port group.

To create a port group, complete the following steps.

1. Select **Configure > Port Groups**.

   The **Port Groups** dialog box displays, as shown in Figure 262 on page 718.

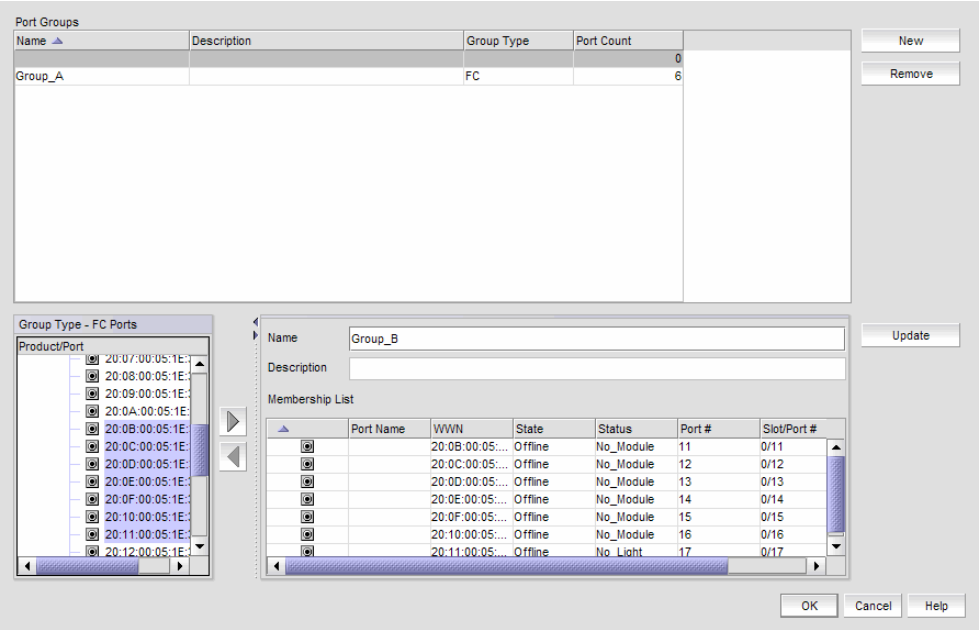


FIGURE 262 Port Groups dialog box

2. Click **New**.
3. Enter a name for the port group in the **Name** field.
4. Enter a description for the port group in the **Description** field.
5. Select one or more ports to add to the group in the **Group Type - FC Ports** list.

   A port group must have at least one port in the **Membership List**. All ports must be from switches in the same fabric.
6. Click the right arrow button.

   The selected ports display in the **Membership List**.
7. Click **Update**.

   The new port group displays in the **Port Groups** list.
8. Click **OK** to close the **Port Groups** dialog box.

Viewing port groups

To view port groups, complete the following steps.

1. Select **Configure > Port Groups**.

   The **Port Groups** dialog box displays only port groups defined by you.

   If a fabric becomes un-monitored, any port groups associated with that fabric do not display in the **Port Groups** list. Once the fabric becomes monitored again, the associated port groups display in the **Port Groups** list.

   If a fabric is removed from discovery, any port groups associated with that fabric are removed permanently from the **Port Groups** dialog box.

   If a device is removed from a fabric, then all ports associated with that device are automatically removed permanently from the port group. If the port group only contains ports from the removed device, then the port group is removed permanently from the **Port Groups** dialog box.

   If a fabric or device is added to the topology while the **Port Groups** dialog box is open, it does not display in the **Group Type - FC Ports** tree until you close and reopen the **Port Groups** dialog box.

2. Edit the port group, as needed.

   To edit a port group, refer to "Editing a port group" on page 719.

3. Delete the port group, as needed.

   To delete a port group, refer to "Deleting a port group" on page 720.

4. Click **OK**.

Editing a port group

To edit a port group, complete the following steps.

1. Select **Configure > Port Groups**.

   The **Port Groups** dialog box displays.

2. Select the port group you want to edit in the **Port Groups** list.

   The information for the selected port group displays in the update information area.

3. Change the name for the port group in the **Name** field, if necessary.

   NOTE
   If you change the port group name, it is the same as copying the existing port group with a new name.

4. Change the description for the port group in the **Description** field, if necessary.
5. Select one or more ports to add to the group in the **Group Type - FC Ports** list.
6. Click the right arrow button.

   The selected ports display in the **Membership List**.

7. Select one or more ports to remove from the group in the **Membership List**.
8. Click the left arrow button.

   The selected ports are removed from the **Membership List**.

9. Click **Update**.

10. Click **OK**.

Deleting a port group

To delete a port group, complete the following steps.

1. Select **Configure > Port Groups**.

   The **Port Groups** dialog box displays.

2. Select the port group you want to delete in the **Port Groups** list.
3. Click **Remove**.

   The selected ports are removed from the **Port Groups** list.

4. Click **OK**.

Swapping blades

NOTE
Blade-based port swap is mainly used for FICON and is only applicable for port blades. However, the Management application does not block blade-based port swap for other application blades, including the 8 Gbps 24-port blade.

You can swap all of the ports from one blade to another blade. During this operation, all ports in the selected blades are swapped. This operation disrupts the traffic on all ports for the selected blades. If GE_Ports are present on the blade, only the non-GE_Ports are swapped.

To swap blades, you must meet the following requirements:

- The chassis must be running Fabric OS 6.3 or later.
- You must have read and write access for the Product Administration privilege.
- The chassis must have at least two blades of the same type present.

Example

The source blade has ports sp1 and sp2, and the destination blade has ports dp1 and dp2. During the swap operation, the address sp1 is swapped with dp1 and address sp2 is swapped with dp2.

NOTE
To perform the swap blades function, you must have read and write access for the Product Administration privilege.

To swap blades, complete the following steps.

1. Select a chassis that contains at least two of the same type of blades.
2. Select **Configure > Switch > Swap Blades**.

   The **Swap Blades** dialog box displays.

3. Select the blade you want to replace from the first **Swap Blades** list.

   Once you select a blade, the second list automatically filters out the selected blade and any blade types that do not match the selected blade.

4. Select the blade with which you want to replace the first blade from the second **Swap Blades** list.
5. Select the **Enable ports after swap is complete** check box to enable ports on the destination blade after the swap is complete.
6. Click **OK**.

NOTE
This operation disrupts the traffic on all ports for the selected blades.

7. Click **Yes** on the confirmation message.

   Once the swap blade operation is complete, a “success” or “failure” message displays.

Chapter

IP Element Manager

22

In this chapter

Element Manager overview

The Element Manager allows you to access a device by connecting to its graphical user interface (GUI), command line interface (CLI), or Web Management interface.

NOTE
You cannot connect to Application products (ServerIron) through the Element Manager.

Element Manager CLI

The Element Manager allows you to access a device by connecting to its command line interface (CLI) through Telnet (default) or SSH. For a procedure to change from Telnet to SSH, refer to "Configuring IP communication" on page 171.

NOTE
You must have the Element Manager Read/Write privileges to change the device configuration through the Element Manager CLI.

NOTE
You must have the Element Manager - Port Config Read/Write privileges to manage specific ports through the Element Manager CLI.

NOTE
Telnet or SSH access to the device CLI must be enabled on the device.

Accessing the IP Element Manager CLI

The Element Manager CLI uses SNMP to query the login authentication type (for example, Telnet Login or Enable Password Login) that the device uses to create the Telnet session token. If SNMP fails, the Element Manager CLI will not work for that device.

To display the Element Manager CLI, complete the following steps.

1. Right-click a device on the Network Objects list or the IP or L2 Topology views and select **CLI through Server**.

   The Element Manager CLI displays and an attempt is made to establish a Telnet session with the credentials configured in your user profile (refer to "Configuring CLI credentials" on page 209). If the user profile credentials are no longer valid, the **User Account for Login to** *Device_IP_Address* dialog box displays.

2. Enter the user name and password for login in the appropriate fields.

   NOTE
   These credentials are only used for the Element Manager CLI login. You should also update these credentials in your user profile. Refer to "Configuring CLI credentials" on page 209.

3. Click **OK**. The Element Manager CLI displays (Figure 263).

   If successful, the **Connect** button is disabled and the **Disconnect** button is enabled.

   When an active CLI session exists and the device goes offline, the connection terminates and a message "Disconnected *IP_Address*" displays.

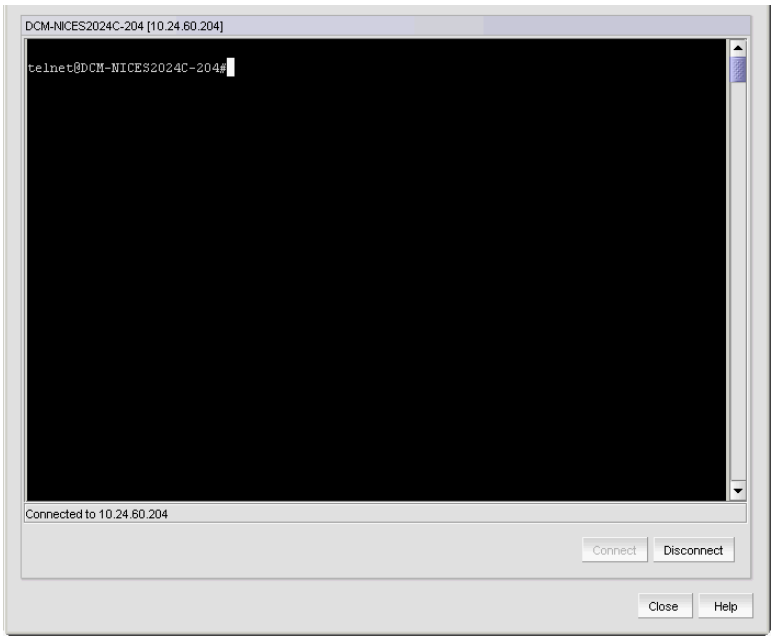


FIGURE 263 Element Manager CLI

Element Manager interface overview

The Element Manager interface provides management and monitoring functions to troubleshoot issues on the Ethernet router series switch running firmware version 5.4 or later.

Element Manager is accessible from the Management application and provides the details of the switch and its ports.

Accessing the Element Manager interface

To launch the Element Manager interface, choose one of the following options:

- Select **Configure** > **Element Manager** > **GUI**.
- Right-click a Ethernet router device on the Network Objects list or VLAN or the IP or L2 Topology views and select **Element Manager** > **GUI**.

  The Element Manager interface displays (Figure 264).

NOTE
You can launch a maximum of six Element Managers from the Management application. For more information, refer to "Configuring IP device manager preferences" on page 162.

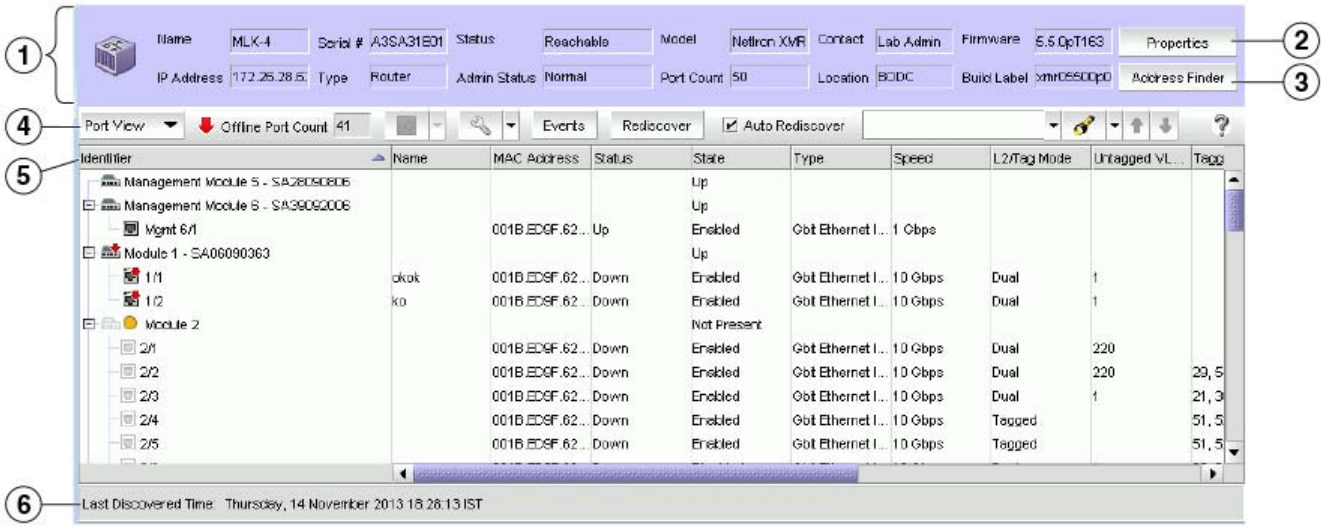


FIGURE 264 Element Manager - main window

The Element Manager interface consists of the following components:

1. Switch properties area - Displays the switch properties. For more information, refer to "Switch properties" on page 726.
2. **Properties** button - Click to launch the **Properties** dialog box. For more information, refer to "Viewing IP device and port properties" on page 1314.
3. **Address Finder** button - Locates where hosts are connected to your network from traffic on the network. For more information, refer to "Address Finder" on page 301.

4. Element Manager toolbar - Provides quick access to dialog boxes and functions. For more information, refer to "Element Manager toolbar" on page 728.
5. Port properties list - Displays the port properties for the selected view (Port, Table, or VLAN). For more information, refer to "Displaying port properties" on page 729.
6. Status bar - Displays the Auto Rediscover progress and last discovered details of the switch.

NOTE
The User Administrator has control over what functions individual users can see and use in the Element Manager. For information on user privileges, refer to "User Privileges" on page 1283.

Switch properties

The switch properties area in the Element Manager displays details of the selected switch. The fields in Table 73 are non-editable.

TABLE 73 Top panel components

Field	Description
Name	Displays the name of the product.
Serial #	Displays the serial number of the product.
Status	Displays the status of the product; whether it is reachable, not reachable, or degraded.
Model	Displays the model number of the product.
Contact	Displays the name or contact number of the person or group you must contact about the product.
Firmware	Displays the firmware version of the product.
IP Address	Displays the IP address (IPv4 or IPv6 format) of the product.
Type	Displays the type of the product.
Admin Status	Displays the administrative status of the product.
Port Count	Displays the number of ports on the product.
Location	Displays the physical location of the product.
Build Label	Displays the firmware build number.

To view more switch properties, cluster information, and the related port properties, click **Properties**. The **Properties** dialog box displays (Figure 265). For more information on the listed switch properties and cluster information, refer to "Viewing IP device and port properties" on page 1314.

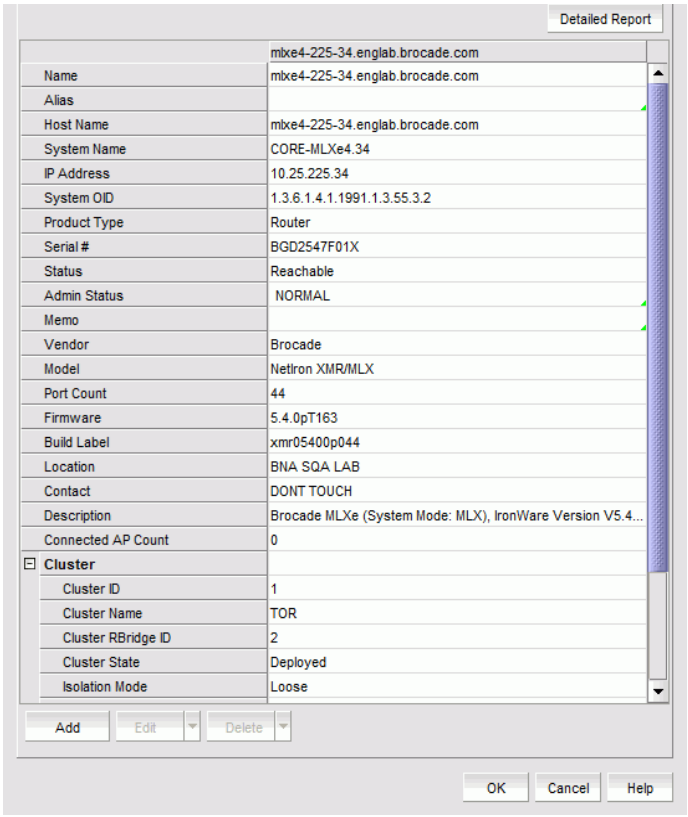


FIGURE 265 Properties dialog box

You can enable and disable port actions as well as access performance monitoring from the **Ports** tab of the **Properties** dialog box (Figure 266). Refer to "Port actions" on page 327 for more information.

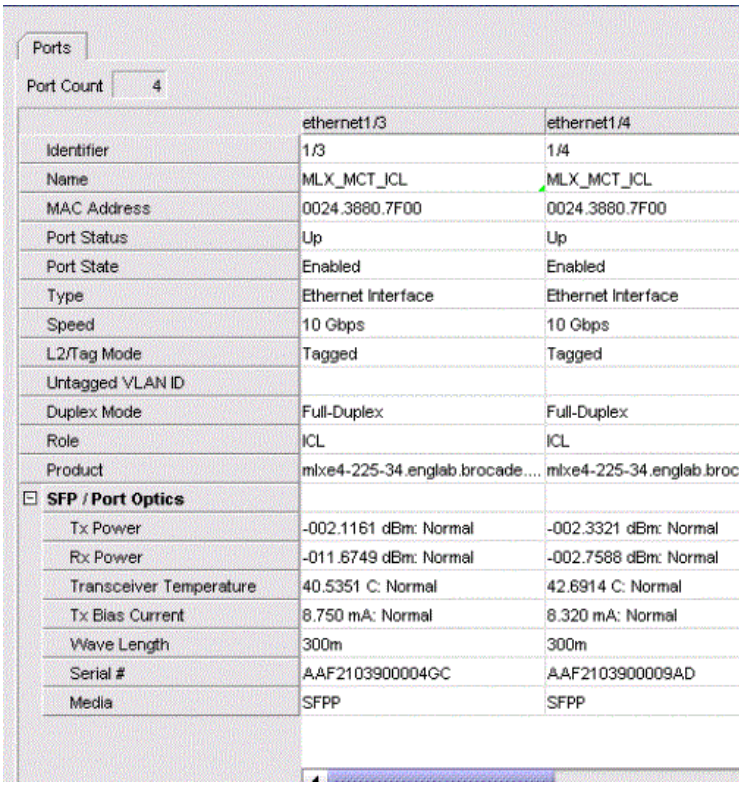


FIGURE 266 Properties dialog box - Ports tab

Element Manager toolbar

The Element Manager toolbar (Figure 267) is located beneath the switch properties.

FIGURE 267 Element Manager - toolbar

The Element Manager toolbar provides the following icons and buttons:

1. View list — Select a view (Port, Table, or VLAN) from the list. For more information, refer to "Displaying port properties" on page 729.
2. **Offline Port Count** — Displays the total number of ports on the switch that are in the offline or down state.
3. **Performance** button — Select to access real-time graphs and historical graphs. For more information, refer to "Performance data" on page 734.
4. **Configure** button — Click to launch the **Configure VLAN**, **Port Actions**, **Port Mirroring, sFlow**, and **MR Switch Over** dialog boxes. For more information, refer to "Configure dialog box" on page 735.
5. **Events** button - Click to view events that have occurred on the selected switch.

6. **Rediscover** button — Click to manually refresh the Element Manager and display the latest information from the switch.
7. **Auto Rediscover** check box — Select the check box to automatically refresh the Element Manager in five-minute intervals. Clear the check box to stop auto-rediscovery.
8. **Product List Search —** Use to search for a port in the port list. For detailed instructions, refer to "Search" on page 299.
9. **Help —** Click to display the online help.

Displaying port properties

You can select any of the following views from the view list on the Element Manager toolbar to view the port properties:

- **Port View**: Select this view for a hierarchical view of the slots and trunks listing their respective ports.
- **Table View**: Select this view for a sequential list of the ports in the *slot #/port #* format.
- **VLAN View**: Select this view for a hierarchical view of the VLANs listing their respective ports.

Table 74 describes the properties of the **Port View** and **Table View**.

TABLE 74 Port View and Table View port properties

Field/Component	Description
Identifier	The identifier of the port. Displays a chronological order of the ports in chassis/slot/port format.
Name	The name of the port.
MAC Address	The MAC address of the port.
Status	The operational status (Up or Down) of the port.
State	The management state (Enabled or DIsabled) of the port. **NOTE:** To enable or disable a port, right-click a slot (or slots), trunk (or trunks), or port (or ports) and select **Enable** or **Disable**.
Type	The type of the port.
Speed	The speed of the port.
L2/Tag Mode	Whether the port is tagged or untagged or dual.
Untagged VLAN ID	The untagged VLAN identifier of the port.
Tagged VLAN ID	The tagged VLAN identifier of the port. **NOTE:** To wrap the VLAN IDs displayed in the column, right-click the **Tagged VLAN ID** column and select **Wrap**. By default, the VLAN IDs are not wrapped in the column.
Duplex Mode	The duplex mode of the port.
MCT Client Name	The MCT client name.
Role	The role of the port. Possible values include the following roles: • MCT • ICL
Module	The name of the module to which the port belongs. **NOTE:** This property is displayed only in **Table View**.

TABLE 74 Port View and Table View port properties (Continued)

Field/Component	Description
SFP / Port Optics tab	Select to display the details of all the SFP and port optics. **NOTE:** To export SFP details, click the link under the **Physical Ports - SFP Details** section of **Detailed Report**.
Tx Power	The power transmitted by the port in a device.
Rx Power	The power received by the port in a device.
Transceiver Temperature	The temperature of the port, in Celsius.
Tx Bias Current	The current supplied to the SFP transceiver. **NOTE:** To export power supply details, click the link under the **Chassis - Power Supply** section of **Detailed Report**.
Wavelength	The wavelength of the port.
Serial #	The number to identify the port.
Media	The type in which the port is present.

Table 75 describes the properties of the **VLAN View.**

TABLE 75 VLAN View port properties

Field/Component	Description
Identifier	The identifier of the port.
Name	The name of the VLAN or port.
Type	The type of the port.
Port Mode	Indicates the tag mode of the port. • Tagged represents the port is in dual mode but is in the tagged state for that particular VLAN. • Untagged represents the port is untagged for that particular VLAN. • The third port mode is Dual mode.
QoS	The Quality of Service (QoS) to assign traffic priority (high, medium, or low) for a given source and destination traffic flow.
STP Type	The type of Spanning Tree Protocol (STP) - STP, RSTP, and None.
STP Status	Indicates whether STP is enabled or disabled.
Virtual/Routing Interface	The virtual routing interface number. You can add an IP address to the virtual routing interface once the VLAN is deployed.
Path Cost	The STP cost of using the port to reach the root bridge.
Transparent VLAN Flooding	The enabled or disabled status of transparent VLAN flooding. Enabled status allows the packets to be forwarded without any form of CPU intervention including MAC learning and MAC destination lookups.
Port Priority	The preference that STP gives this port relative to other ports for forwarding traffic out of the spanning tree.
Role	The role of the port. Possible values include the following roles: • MCT • ICL

Comparing physical port properties

You can compare multiple physical port properties, for example, a healthy port with an offline port.

1. From **Port View** or **Table View**, select two or more ports (press **Ctrl** and click each port).
2. Right-click one of the selected ports, and select **Properties**.

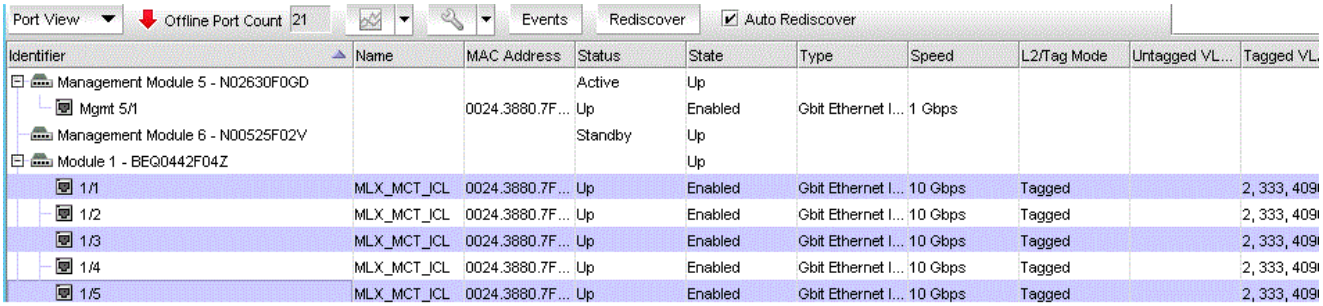


FIGURE 268 Physical port properties

For example, in Figure 268, ports 1/1, 1/3, and 1/5 are selected. The selected port properties display in the **Port Properties** dialog box and the order of port selection is also retained, as shown in Figure 269.

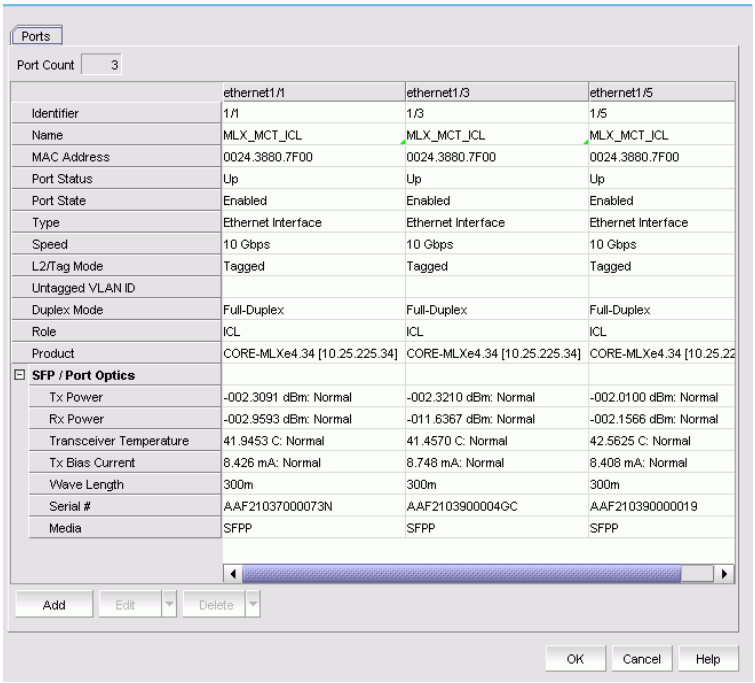


FIGURE 269 Comparing physical port properties

Comparing physical and virtual port properties

You can compare physical and virtual port properties.

1. From **VLAN View**, select one or more virtual ports and physical ports.
2. Right-click one of the selected ports, and select **Properties** (Figure 270).

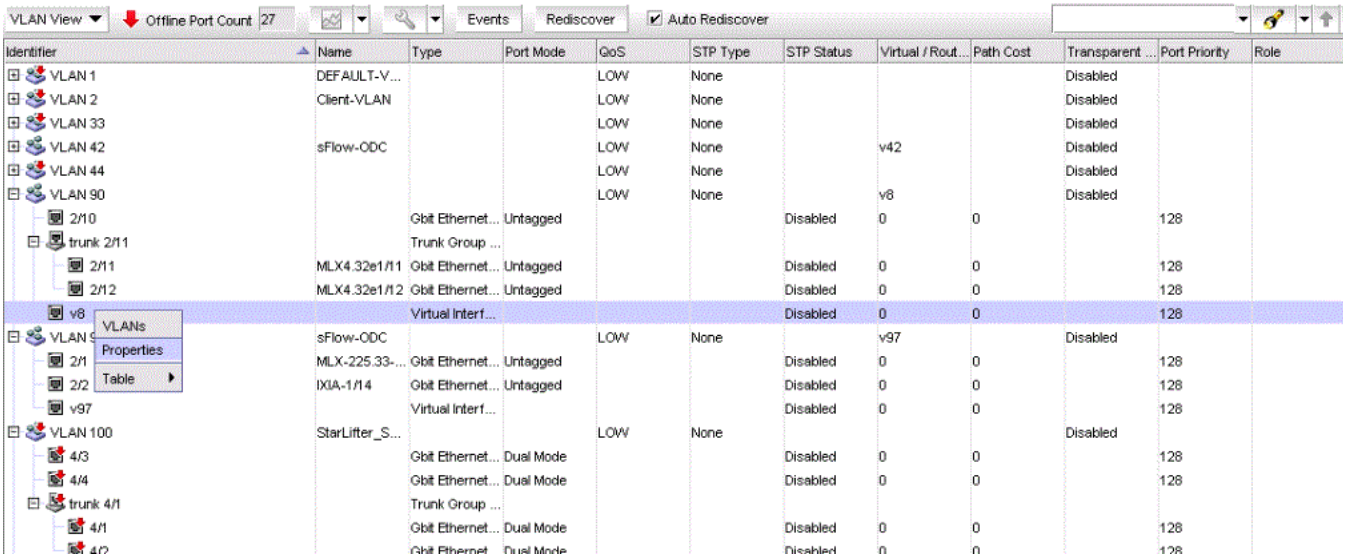


FIGURE 270 Physical and virtual port properties

The selected port properties are displayed in the **Port Properties** dialog box, where the selected physical port properties are displayed under the **Ports** tab and the selected virtual port properties are displayed under the **Virtual Interfaces** tab, as shown in Figure 271.

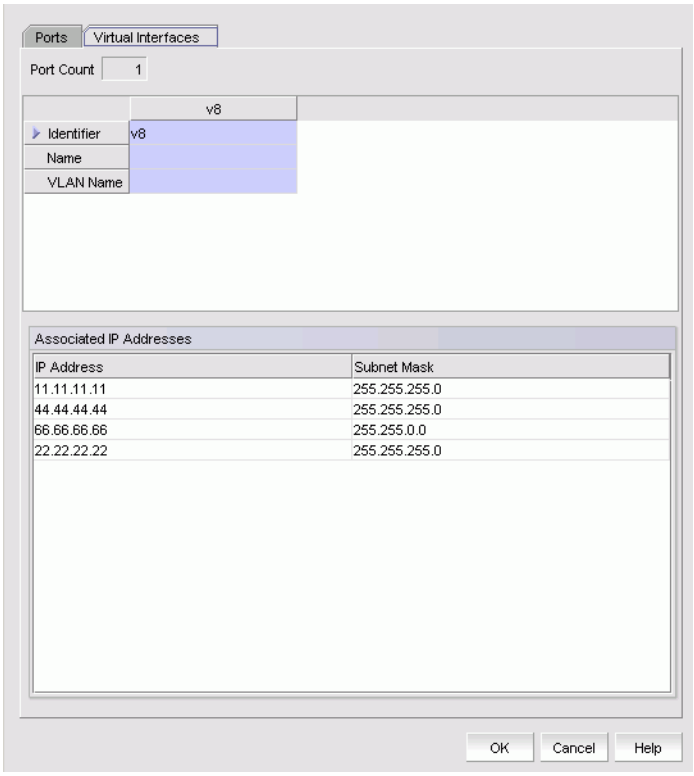


FIGURE 271 Comparing physical and virtual port properties

Status indicator icons

Table 76 describes the icons that are used to indicate the status of a switch, slot, or port.

TABLE 76 Status indicator icons

Status icon	Description
	Indicates the port is down.
	Indicates the switch is not reachable.
	Indicates a degraded link (the switch is reachable but cannot receive SNMP).
	Indicates an IP slot containing a line card.
	Indicates an IP slot containing no line card.
	Indicates a port in an IP slot containing no line card.
	Indicates that the module or line card is blocked or down.
	Indicates that the module or line card is booting, initializing, interactive, LP synchronizing, not present, powered off, rebooting, recovering, strip synchronizing, loading software, or FID synchronizing.

If a port or multiple ports in a slot are down, the status rolls up to the slot level to display a down icon on the slot.

Search

You can search for a objects by text or regular expression.

NOTE
The **Search** function retains your last 10 search criteria.

Refer to "Search" on page 299 for more information.

Table capabilities

You can customize any table in the Management application main interface (for example, the Master Log or the Product List) or in individual dialog boxes in the following ways:

- Display only specific columns
- Display columns in a specific order
- Resize the columns to fit the contents
- Sort the table by a specific column or multiple columns
- Copy information from the table to another application
- Export information from the table
- Search for information
- Expand the table to view all information

- Collapse the table.

Refer to "Customizing application tables" on page 294 for information on table functions.

Performance data

You can use the following options to monitor the performance data of a switch:

- **Real Time Graph/Table**
- **Historical Graph/Table**

Real-time performance monitoring

Real-time performance monitoring allows you to view a snapshot of the current performance data. To monitor the real-time performance of the switch, complete the following steps.

NOTE
You can monitor real-time graphs for a slot, multiple slots, a trunk, multiple trunks, a port, or multiple ports.

1. In the Element Manager, right-click a slot (or slots), trunk (or trunks), or port (or ports) and select **Performance** > **Real Time Graph/Table**.

   Or

   Select a slot (or slots), trunk (or trunks), or port (or ports), and select **Real Time Graph/Table** from the **Performance** button on the Element Manager toolbar, as shown in Figure 272.

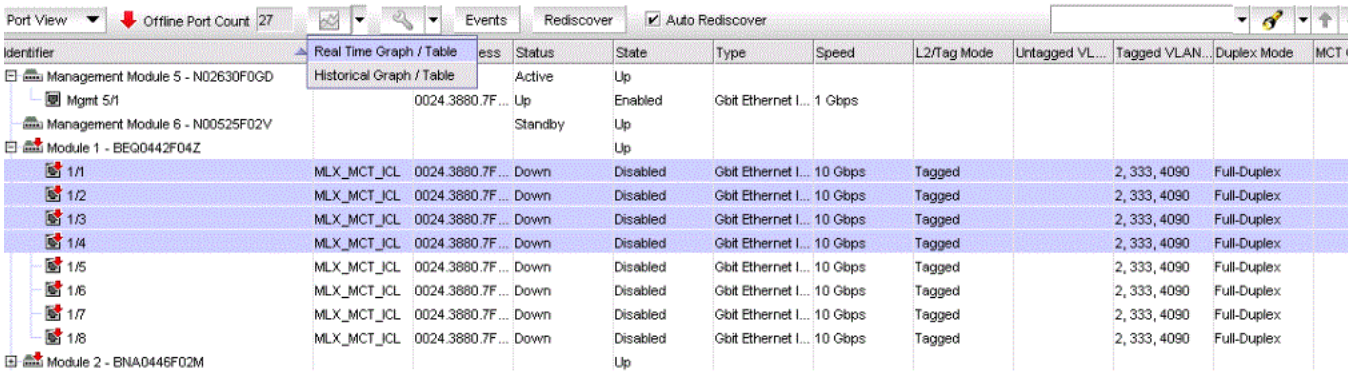


FIGURE 272 Real Time Graph/Table performance data

The performance data for the selected slots, trunks, or ports is displayed in the **Real Time Graphs/Tables** window. Refer to "IP real-time performance monitoring" on page 983 for more information.

Historical performance monitoring

Historical performance monitoring allows you create data collectors by choosing MIB object and by choosing or creating mathematical expressions. You can also configure a historical data graph or table to display data.

1. In the Element Manager, right-click a slot (or slots), trunk (or trunks), or port (or ports) and select **Performance** > **Historical Graph/Table**.

   Or

   Select a slot (or slots), trunk (or trunks), or port (or ports), and select **Historical Graph/Table** from the **Performance** button on the Element Manager toolbar, as shown in Figure 273.

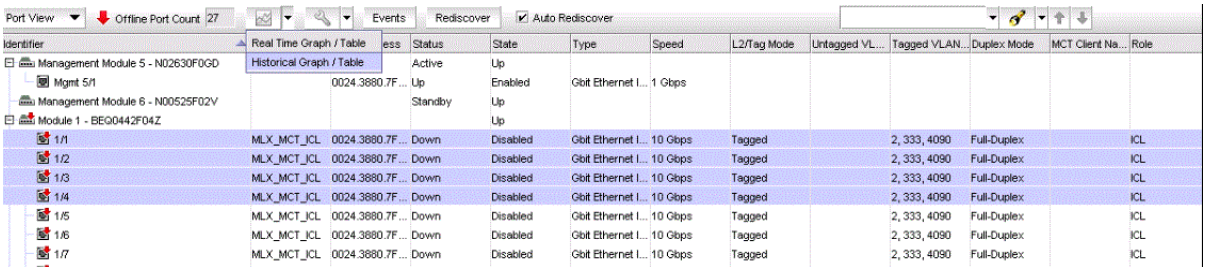


FIGURE 273 Historical Graph/Table performance data

The performance data for the selected slots, trunks, or ports is displayed in the **Historical Graphs/Tables** window. Refer to "IP historical performance monitoring" on page 995 for more information.

Configure dialog box

The **Configure** button allows you to manage the Virtual Local Area Network (VLAN), the associations for the selected ports.

Configuring VLAN

To access the **Configure VLAN** dialog box from Element Manager, right-click a module (or modules), trunk (or trunks), or port (or ports) and select VLANs.

Or

Select a module (or modules), trunk (or trunks), or port (or ports), and click the **Launch VLAN** button on the Element Manager toolbar.

The **Configure VLAN** dialog box displays. For more information, refer to "Adding or modifying port VLANs" on page 827.

Resetting port counters

Resetting port counters allows you to clear the statistics of a module (or modules), trunk (or trunks), or port (or ports).

1. In the Element Manager, select a module (or modules), trunk (or trunks), or port (or ports).
2. Click the **Configure** icon and select **Port Actions** > **Reset Counter** on the toolbar (as shown in Figure 274).

   To access the Resetting port counters dialog box from Element Manager, right-click a module (or modules), trunk (or trunks), or port (or ports) and select Reset port counter.

A warning message displays:
You want to reset the selected interface statistics. Do you want to continue?

Click **Yes** to clear all the statistics of the port.

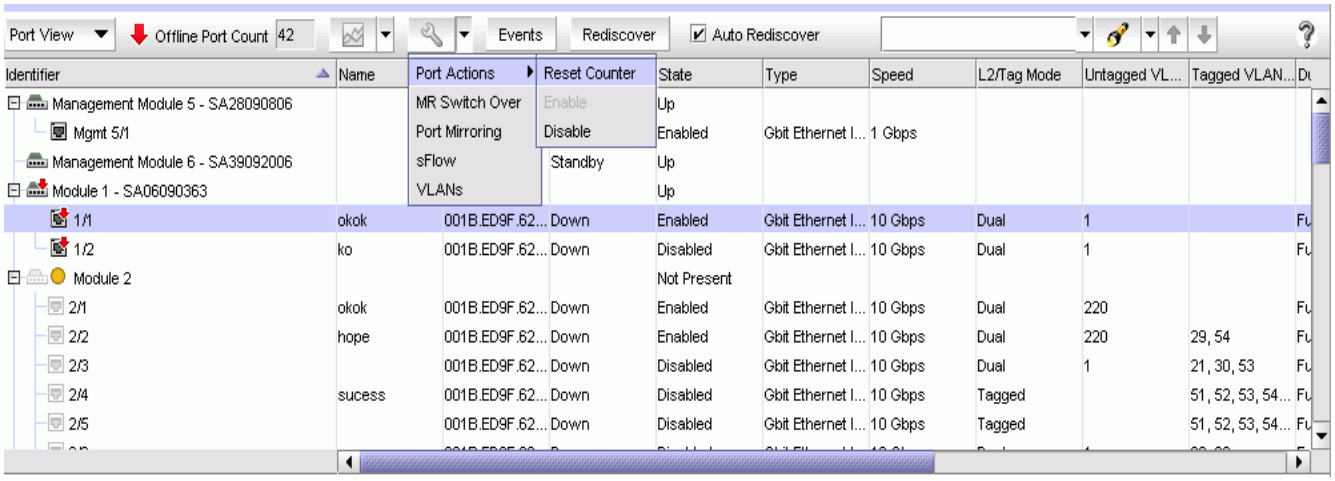


FIGURE 274 Resetting port counters

Enable or Disable

Enable or disable on a module will perform module power on or off. It is applicable only to the configuration module.

To enable or disable a port, right-click a slot (or slots), trunk (or trunks), or port (or ports) and select **Enable** or **Disable**.

NOTE
After performing the enable or disable operation on ports or at module level, the changes will be reflected only after the discovery of the product.

Management Module switchover

The Management Module allows you to manage all of the routing actions of a device. If there is more than one Management Module you can make one of the modules the active module and the other module the standby module.

NOTE
If the active Management Module fails, you must switch to the the standby module.

Changing the standby Management Module to active

To change the standby Management Module to active, click Configure > MR Switch Over (as shown in Figure 275).

Or

To access the MR switch over dialog box from Element Manager, right-click a module (or modules), trunk (or trunks), or port (or ports) and select MR Switch Over.

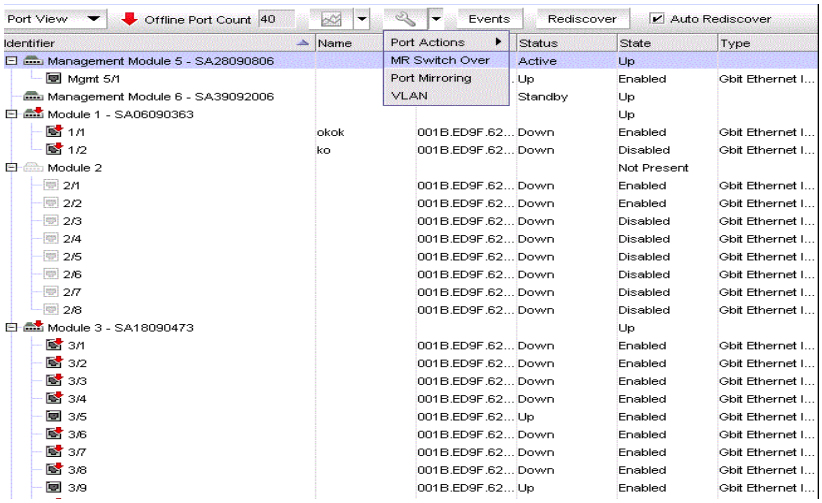


FIGURE 275 MR Switch Over

The **MR Switch Over Status** dialog box is displayed and confirms if the Management Module is active (as shown in Figure 276).

NOTE
MR Switch Over option will be disabled for single Management Module switch.

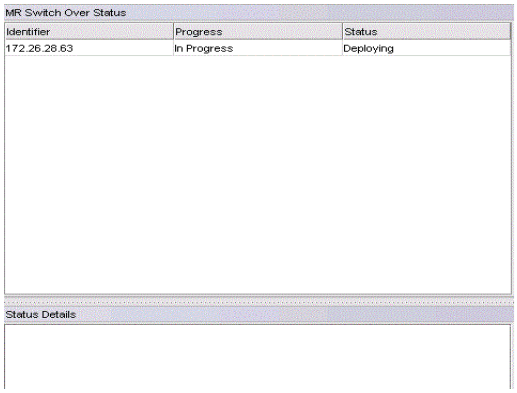


FIGURE 276 MR Switch Over Status dialog box

Switch Fabric Module

Switch Fabric Modules switch packets from one interface module to another. The Switch Fabric Module displays the serial number, state, and the status of the switch (as shown in Figure 277).

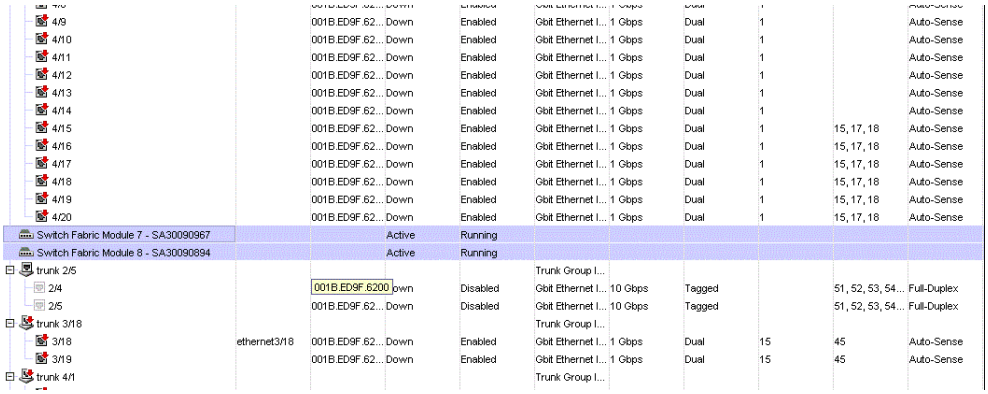


FIGURE 277 Switch Fabric Module

Port mirroring

Port mirroring analyzes the traffic flowing in a port by monitoring the particular port. Port mirroring helps to monitor the inbound traffic, outbound traffic, or both.

Configuring port mirroring

1. Click the **Configure** icon in the Element Manager toolbar.
2. Select **Port Mirroring** (as shown in Figure 278).

   The **Port Mirroring** dialog box is displayed (as shown in Figure 279).

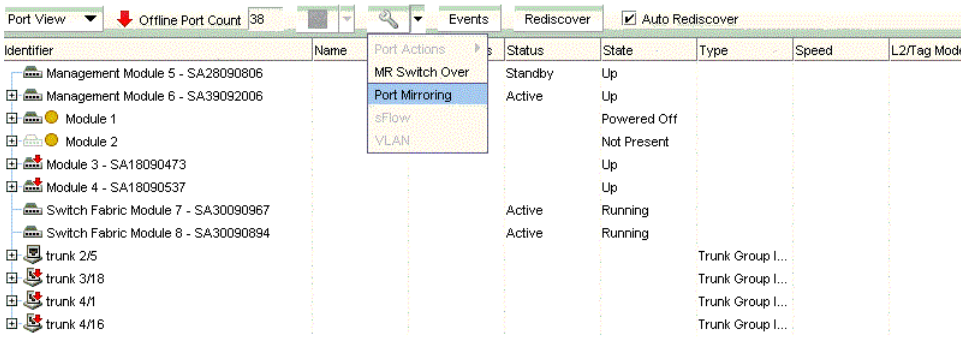


FIGURE 278 Port Mirroring

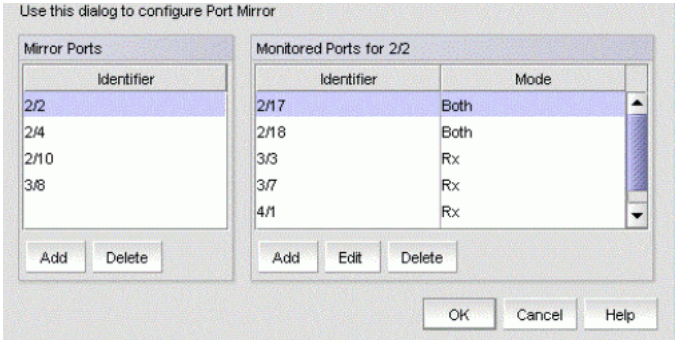


FIGURE 279 Port Mirroring dialog box

The **Port Mirroring** dialog box provides the following buttons to perform various functions.

- Left pane (**Mirror Ports**) — Displays the mirror ports of a device.
  - **Add** — Adds mirror ports.
  - **Delete** — Deletes the mirror ports.
- Right pane (**Monitored Ports**) — Displays the monitored ports of a device.
  - **Identifier** — Displays the ports where traffic must be monitored.
  - **Mode** — Displays if the traffic is inbound (TX), outbound (RX), or both.
  - **Add** — Adds monitored ports.
  - **Edit** — Edits the monitored ports.
  - **Delete** — Deletes the monitored ports.

Adding a port to port mirroring

To add mirror ports in a device, perform the following steps.

1. Select **Configure** > **Port Mirroring**.

   The **Port Mirroring** dialog box is displayed.

2. In the Mirror Ports pane, click **Add (Mirror Port).** Select a port from the list to act as a mirror port. You can configure multiple monitoring ports to a specific mirror port to monitor traffic.

   NOTE
   An error message is displayed if the monitored port is being mirrored in Rx and Tx.

3. Select **Mode** from the list based on whether to monitor inbound traffic, outbound traffic, or both.

Editing a port in port mirroring

To edit monitored ports in a device, perform the following steps.

1. Select **Configure** > **Port Mirroring**.

   The **Port Mirroring** dialog box is displayed.

2. Select a port in the **Mirror Ports** pane.

3. In the **Monitored Ports** pane, click **Edit.** Select a port from the list to edit the monitor port.

NOTE
An error message is displayed if the monitored port is being mirrored by some other mirror port.

4. Select **Mode** from the list based on whether to monitor inbound traffic, outbound traffic, or both.

Deleting a port from port mirroring

To delete mirror ports in a device, perform the following steps.

1. Select **Configure** > **Port Mirroring**.

   The **Port Mirroring** dialog box is displayed.

2. Select a port in the **Mirror Ports** pane.
3. In the **Monitored Ports** pane, click **Delete.** Select a port from the list to delete the monitor port.

sFlow

The IP Element Manager supports sFlow to capture traffic data and configure sFlow collector.

Configuring sFlow in Element Manager

1. Click the **Configure** icon in the Element Manager toolbar..
2. Select **sFlow** (as shown in Figure 280).

   or

   To access the sFlow from Element Manager, right-click a module (or modules), trunk (or trunks), or port (or ports) and select sFlow.

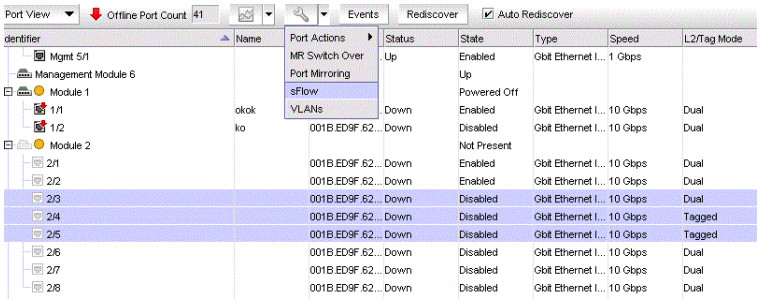


FIGURE 280 sFlow dialog box

3. To configure sFlow, refer to "Configuring sFlow" on page 1020.

Web Management interface

The Element Manager allows you to access a device by connecting to its Web Management interface.

NOTE
You must have the Element Manager Read/Write privilege to change the device configuration through the Web Management interface.

NOTE
Web Management interface access must be enabled on the device.

Accessing the Web Management interface

To launch the Web Management interface, choose one of the following options:

- Select **Configure > Element Manager > Web**.
- Right-click a device on the Network Objects list or the IP or L2 Topology views and select **Element Manager > Web.**
- From the Wired Product Report, IP Subnet Report, or IP Address Report, click the IP address of the product.

  If you select a Fabric OS DCB device, Web Tools displays. For information about Web Tools, refer to the *Web Tools Administrator's Guide*.

  The Web Management interface displays (Figure 281). You can use the Web Management interface to manage the device configuration.

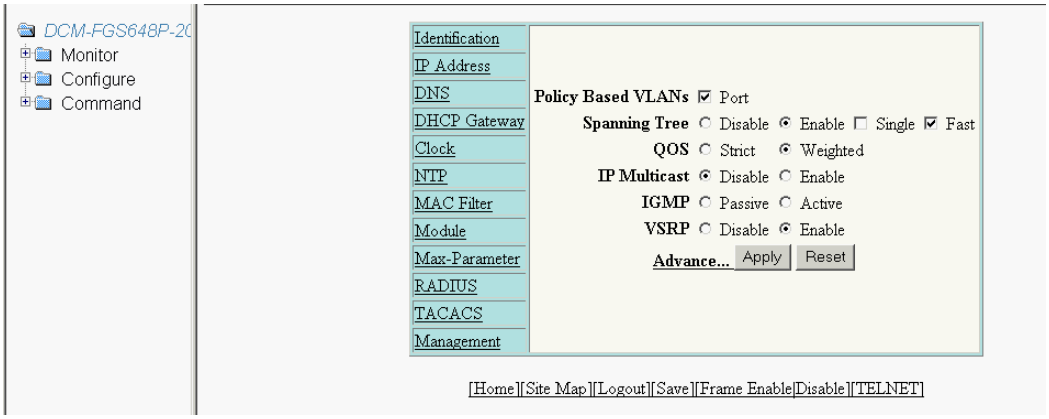


FIGURE 281 Web Management interface

If the device does not have a supported web interface, an error message displays: "Failed to connect to the web management interface. The product might not support web interface."

Accessing the IP device front panel

To display the Element Manager front panel, choose one of the following options:

- Select **Configure > Element Manager > Front Panel**.
- Right-click a device on the Network Objects list or the IP or L2 Topology views and select **Element Manager > Front Panel.**

The Web Management interface - Front Panel displays (Figure 282). You can use the Front Panel to manage port configuration.

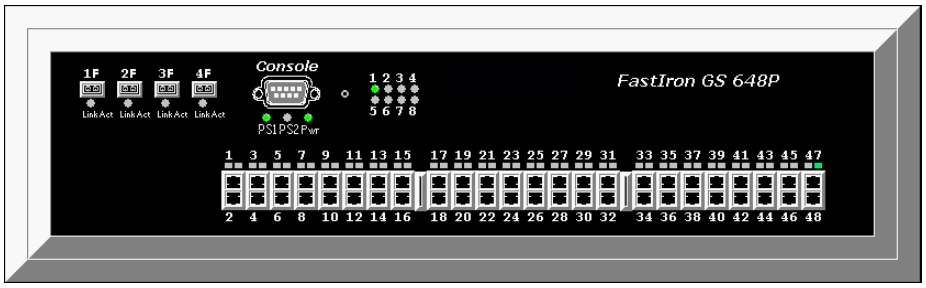


FIGURE 282 Web Management Interface - Front Panel

If the device does not have a supported web interface, an error message displays: “Failed to connect to the web management interface. The product might not support web interface.”

Web Management interface troubleshooting

Table 77 lists a possible issue and the recommended solution for launching the Web Management interface.

TABLE 77 Troubleshooting

Problem	Resolution

The Web Management interface does not launch even when you configure both the IronWare OS products and the Management application server to use HTTPS to launch the Web Management interface. You should still be able to launch the product Web Management interface directly by entering the URL in a web browser.
Failure is due to insecure SSL certificates (MD2, MD5, DES, 3DES, and RC2) deployed in the IronWare OS products.
To configure IronWare OS products to use HTTPS, use the **web-management https** command to enable HTTPS in the device for web-based communication.
To configure the Management server to use HTTPS, refer to “Configuring IP communication” on page 171.
	Workaround 1 — Editing the Java security file
	1 Open the java.security file located in the *Install_Home*\jre\lib\security\ directory in a text editor.
	Install_Home is the directory where the Management application is installed.
	2 Comment out the following attributes:
	`#jdk.certpath.disabledAlgorithms=MD2`
	`#jdk.tls.disabledAlgorithms=MD5, DES, 3DES, RC2`
	3 Save and close the file.
	4 Restart the Management application service (“Stopping all services” on page 377).
	Workaround 2 — Removing and replacing SSL certificates
	Remove the insecure certificates using the MD2, MD5, DES, 3DES, or RC2 signature algorithms from the IronWare OS products and replace with more secure ciphers such as SHA1.

Chapter

Configuration Repository and Backup 23

In this chapter

Configuration repository

The **Product Configurations** tab of the **Configuration Repository** dialog box allows you to display each product configuration, including the name of the product, the version number of the configuration, the software release the product is running, and the product type. To open the configuration repository, complete the following steps.

1. Click the **IP** tab.
2. Select **Configure > Configuration > Configuration Repository**.
3. Click the **Product Configurations** tab.

   The **Product Configurations** tab of the **Configuration Repository** dialog box displays, as shown in Figure 283.

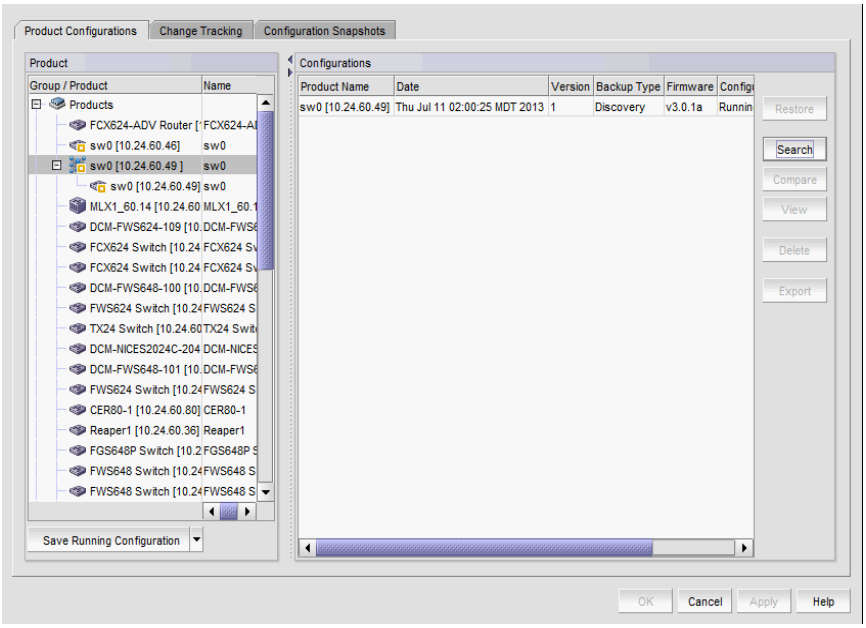


FIGURE 283 Configuration Repository dialog box — Product Configurations tab

The **Configuration Repository** dialog box displays the following information:

- **Product Name** — The name of the backed-up product
- **Date** — The date when the configuration file was stored in the server and the time when the last backup attempt occurred.
- **Version** — The version of the configuration file. The version number is incremented by one for each new version
- **Backup Type** — The type of backup used to obtain the configuration files from the device. Backup options include the following types:
  - Discovery — The discovery backup is obtained after the discovery process
  - Pre-deployment — Occurs before a configuration change is deployed to the device
  - Post-deployment — Occurs after a configuration change is deployed to the device
  - Re-sync — Occurs when a trap is generated by the device during a startup or running configuration change, or when a user performs a manual resynchronization of the device
    For Network OS devices, Re-sync backup occurs after manual rediscovery of the VCS cluster member device and when a CLI configuration deployment occurs on the product.
  - Manual — Occurs when a user clicks the **Save Running/Startup Configuration** button
  - Scheduled — Occurs when backups are regularly scheduled
  - Startup Config Change Trap — When startup configuration is changed for a device, the startup config change trap is triggered and the configuration backup is captured.

- Running Config Change Trap — When a running configuration is changed for a device, the running config change trap is triggered and the configuration backup is captured. For Startup Config Change Trap and Running Config Change Trap, make the following configurations:
  - Enable DoBackupOnStartupConfigChangeTrap and DoBackupOnRunningConfigChangeTrap on the OPtions dialog box (refer to "Configuring change manager preferences" on page 160).
  - Disable event triggered polling in discovery (refer to "Defining global setting preferences" on page 60).
  - Register the server with the product for SNMP traps (refer to "Adding a trap recipient to one or more switches" on page 1148

- **Firmware —** The version of the release on the backed-up device
- **Configuration Type** — The type of configuration (running or startup) taken
- **Baseline** — Enabled when you select a configuration as the baseline. By default, the first version configuration is the baseline. You can change the baseline configuration at any time.

4. Click the **Baseline** check box (if enabled) to designate the configuration as the base configuration. The Change Tracking feature uses the base configuration to compare the latest backup configuration file with the configuration that is designated as the baseline and to update the Configuration Deviation Status icon on the Status Bar (refer to "Viewing configuration deviation status" on page 753).
5. Select two configurations for the same product to view the Master Log events that occurred between the two selected configurations in the **Events Associated with Differences** table.

NOTE
The **Events Associated with Differences** table is blank for configuration files triggered on a Fabric OS DCB device.

NOTE
The **Events Associated with Differences** table is blank when you select configuration files from different products.

The **Events Associated with Differences** table is only available when you select two configuration backup files for the same product. List of events (up to 100) associated with the configurations. Right-click an event and select properties to view the **Event Properties** dialog box (refer to "Displaying event properties from the Master Log" on page 1207). This table contains the following data:

- **Acknowledge** check box — Select to acknowledge the event and remove it from the Master Log. The event is not removed from the **Events Associated with Differences** table.
- **Source Address** — IP address of the product on which a change occurred.
- **Category** — Audit log event category. Options include application, product audit, and user action events.
- **Description** — Description of the event.
- **Last Event Server Time** — Time and date the event last occurred on the server.
- **Message ID** — Message ID of the event.

- **Relative Time (mins)** — Relative time from the selected backup time to the event occurred time.
- **User** — Name of the user responsible for triggering the event.

6. Click the following buttons to access the corresponding dialog boxes:
   - **Restore** button — Select one or more configuration files from the **Configurations** list and click to restore to that configuration. To restore a configuration, refer to "Restoring a configuration" on page 750.
   - **Search** button — Click to launch the **Search Configuration Repository** dialog box, which allows you to search the contents of configurations in the repository of the management server. Refer to "Searching the configuration repository" on page 751 for more information.
   - **Compare** button — Select two configurations (same product or two different products) and click to launch the **Compare** dialog box with the differences between the two configurations are highlighted.
   - **View** button — Select a row in the **Configurations** list and click to display the contents of the selected configuration.
   - **Delete** button — Select one or more configurations from the **Configurations** list and click to manually delete the configuration from the repository of the management server.

     NOTE
     You cannot delete the baseline or latest configuration.

     NOTE
     When a configuration backup is added to the server, it is assigned a version number in sequential order. Deleting a configuration backup does not renumber the remaining versions.

   - **Export** button — Select one or more configurations and click to launch the **Export Configuration** dialog box, which allows you to export the configurations to a text file. Refer to "Exporting a configuration to a text file" on page 752 for more information.

Saving the configuration status

Use the **Save Configuration Status** dialog box to show the progress of the configuration retrieval for the product you select. If the product is a new version, it is saved in the management server with the server time captured as the date parameter.

1. Click the **IP** tab.
2. Select **Configure > Configuration > Configuration Repository**.
3. Click the **Product Configurations** tab.
4. Select the product from the **Product** list.

   Press **Ctrl** or **Shift** and then click each product to select more than one product.

   If you select a product group, the save configuration is run against all products in the selected group.

   If you select a VCS fabric, the save configuration is run against all members in the VCS fabric.

5. Select one of the following save options from the list:

   - **Save Running Configuration** — Select to retrieve the running configuration from the device. If there is no change in the running configuration since the latest running configuration (available in the repository), then the retrieval is skipped.
   - **Save Startup Configuration** — Select to retrieve the startup configuration from the device. If there is no change in the startup configuration since the latest startup configuration (available in the repository), then the retrieval is skipped.

   Either of these options launches the **Save Configuration Status** dialog box, shown in Figure 284.

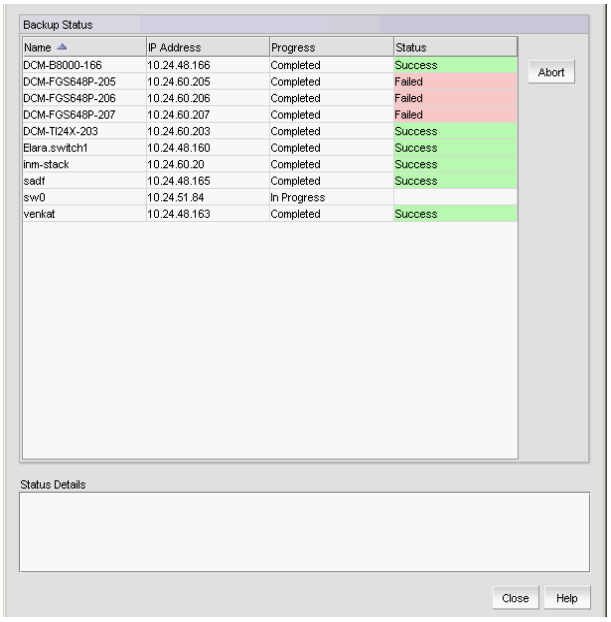


FIGURE 284 Save Configuration Status dialog box

6. Review the progress and status of the configuration retrieval for the products you selected in the **Status** column and the **Status Details** field.
7. Click **Close** to close the dialog box, or click **Abort** to cancel the operation.

Viewing the configuration

1. Click the **IP** tab.
2. Select **Configure > Configuration > Configuration Repository**.
3. Click the **Product Configurations** tab.
4. Select a configuration and click **View** to display configuration information.

   The **View Configuration** dialog box displays details of the selected configuration.

NOTE
You can view only one configuration at a time.

- **Description** — Displays a description of the device configuration.
- **Configuration** list — Displays details of the backed up configuration.
- **Find** — Enter a text string and perform one of the following actions:
  - Click **Find Next —** Searches the next matching string in the configuration.
  - Click **Find Previous —** Searches the previous matching string in the configuration.
- **Reached bottom of the page** icon — Displays when there are no more entries to display.
- **Highlight** grid — Click to highlight the text string.
- **Match Case** check box — Click to render the search case-sensitive.
- **Repeats** check box — Click to continue the search at the top when the bottom is reached.
- **Previous** button — Click to display the previous configuration (from current choice) in the **Configurations** list.
- **Next** button — Click to display the next configuration (from current choice) in the **Configurations** list.
- **Export** button — Click to export the currently viewed configuration to a text file.

Comparing product configurations

The **Comparison** dialog box allows you to display the contents of two configurations side-by-side. To compare two configurations, perform the following steps.

1. Click the **IP** tab.
2. Select **Configure > Configuration > Configuration Repository**.
3. Click the **Product Configurations** tab.
4. Select a product to view the configurations.
5. Select two configurations and click **Compare**.

   The **Compare** dialog box displays, as shown in Figure 285.

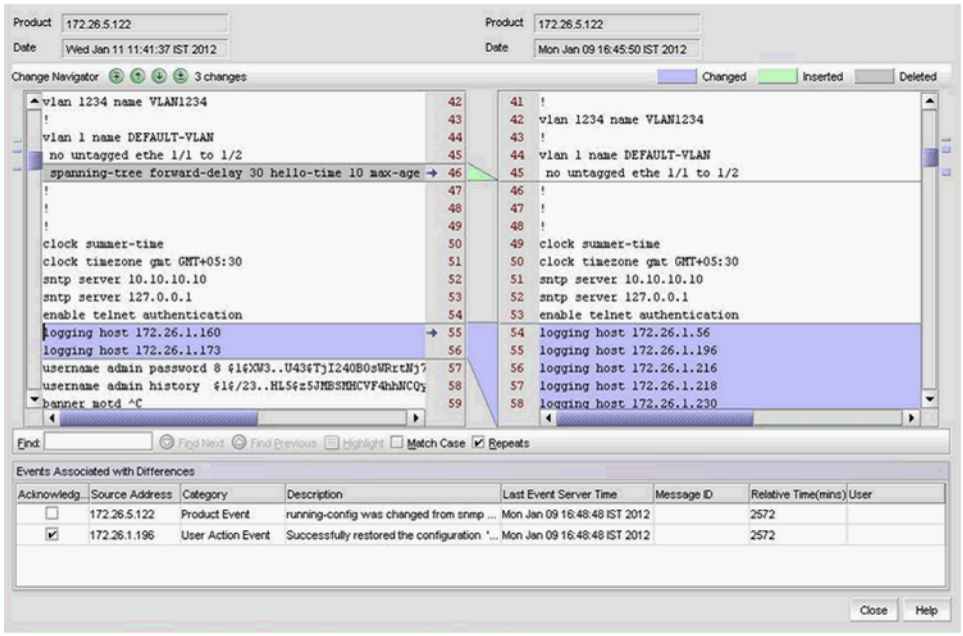


FIGURE 285 Compare dialog box

The **Compare** dialog box displays the following information:

- **Product** — The IP address of the device.
- **Date** — The Displays the date the device configuration was taken.
- **Change Navigator** buttons/legend — The Enabled when there is at least one change between to two compared files.
  - Go to first change button ( ) — Click to move to the first change.
  - Go to previous change button ( ) — Click to move to the previous change.
  - Go to next change button ( ) — Click to move to the next change.
  - Go to last change button ( ) — Click to move to the last change.
  - Number of changes label — Indicates the number of changes. If there are no differences, displays “No change”.
  - Differences legend — Displays the color legend for differences:
    - Changed status displays in blue.
    - Inserted status displays in green.
    - Deleted status displays in grey.
- **Phrase not found** icon — Displays when the search text string is not found.
- Configuration contents areas — Displays the contents of the selected configurations.
- **Find** — Enter a text string and take one of the following actions:
  - Click **Find Next** — Searches the next matching string in the configuration.
  - Click **Find Previous** — Searches the previous matching string in the configuration.
- **Highlight** grid — Click to highlight the text string.
- **Match Case** check box — Click to render the search case-sensitive.
- **Repeats** check box — Click to continue the search at the top when the bottom is reached.

- **Events Associated with Differences** table — Only available when you select two configuration backup files for the same product. List of events (up to 100) associated with the configurations. Right-click an event and select properties to view the **Event Properties** dialog box (refer to "Displaying event properties from the Master Log" on page 1207). This table contains the following data:

  NOTE
  The **Events Associated with Differences** table is blank for configuration files triggered on a Fabric OS DCB device.

  NOTE
  The **Events Associated with Differences** table is blank when you select configuration files from different products.

  - **Acknowledge** check box — Select to acknowledge the event and remove it from the Master Log. The event is not removed from the **Events Associated with Differences** table.
  - **Source Address** — IP address of the product on which a change occurred.
  - **Category** — Audit log event category. Options include application, product audit, and user action events.
  - **Description** — Description of the event.
  - **Last Event Server Time** — Time and date the event last occurred on the server.
  - **Message ID** — Message ID of the event.
  - **Relative Time (mins)** — Relative time from the selected backup time to the event occurred time.
  - **User** — Name of the user responsible for triggering the event.

6. Click **Close**.

Restoring a configuration

1. Click the **IP** tab.
2. Select **Configure > Configuration > Configuration Repository**.
3. Click the **Product Configurations** tab.
4. Select the configuration you want to restore from the **Configurations** list.

   To restore configurations for multiple products, select one configuration for each product.

5. Click **Restore**.

   If you select to restore a VCS configuration, a message displays. Select one of the following options on the message and click **OK**.

   - Running
   - Startup
   - Startup and Reload

   If you select to restore a IronWare product configuration, a message displays. Select one of the following options on the message and click **OK**.

   - Startup

- Startup and Reload

6. Review the status details for accuracy.

Searching the configuration repository

The **Search Configuration Repository** dialog box allows searching for products that have a particular configuration in the management server's repository. Use the search feature to refine the configuration repository based on the filter criteria described in this section.

1. Click the **IP** tab.
2. Select **Configure > Configuration > Configuration Repository**.
3. Click the **Product Configurations** tab.

   The **Configuration Repository** dialog box displays.

4. Click the **Search** button.

   The **Search Configuration Repository** dialog box, as shown in Figure 286, displays.

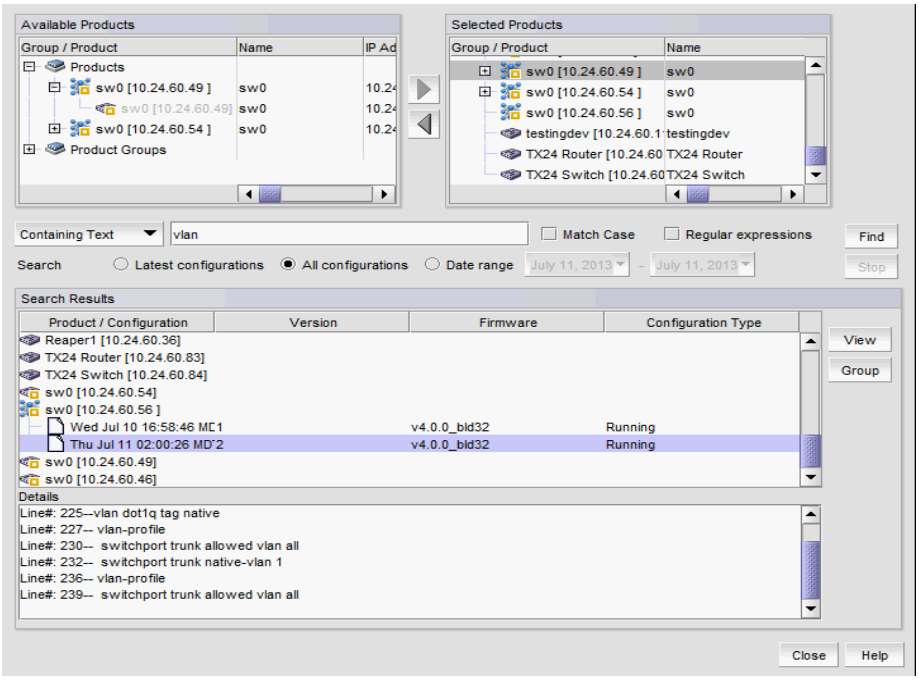


FIGURE 286 Search Configuration Repository dialog box

5. Select a product from the **Available Products** list and click the right arrow button to move one or more products to the **Selected Products** list.

   Press **Ctrl** or **Shift** and then click each product to select more than one product.

6. Enter a search text string, with a limit of 255 characters, into the **Containing Text** field. This text string is used to search on configurations of the selected products.
7. Enable the following options, as required:

   - **Match Case** check box - Select the check box to make the search case-sensitive.

- **Regular expressions** check box - Select the check box to use unicode regular expressions in your search.
- **Search** options — Specify the following types of available searches:
  - **Latest configurations** — Searches the text in the most recent configurations of the selected products.
  - **All configurations** — Searches the text in all configurations of the selected products.
  - **Date range** — Searches the configuration files of the selected products within the specified date range.

8. Click the **Find** button to find the text string and display the search results in the **Search Results** list.
9. Click the **Stop** button to stop the search in progress.
10. Click the **View** button to display the contents of the selected configuration file. The configuration entry that matches the search criteria is displayed in red.
11. Click the **Group** button to create product groups.

NOTE
You can only use the Product Group feature if you have the Configuration Management privilege and the **Search Configuration Repository** dialog box has search results.

12. Click **Close** to close the **Search Configuration Repository** dialog box.

Exporting a configuration to a text file

The **Export** button on the **Configuration Repository** dialog box allows you to export the configuration of the selected product to a text file. You must have the Configuration Management privilege in your Management application user account to perform this task.

Follow these steps to export a configuration to a text file. You can export a maximum of 25 configurations simultaneously.

1. Click the **IP** tab.
2. Select **Configure > Configuration > Configuration Repository**.
3. Click the **Product Configurations** tab.
4. Select one or more products from the **Product** list.
5. Select one or more configurations from the **Configurations** list.
6. Click **Export**.

   The **Export Configuration** dialog box displays.
7. Browse to the location to which you want export the configuration and click **Export**.

   The default locations for the product configuration are as follows:

   - Windows: Desktop\My Documents
   - Linux: \root

   If you select configurations from the same product, the default text file name is *IP_Address*_config.txt. IPv6 addresses use dashes (-) instead of colons (:) in file naming.

If you select configurations from multiple products, the default text file name is MultiProduct_config.txt.

Configuration deviation

The Management application backs up the product configuration after a change is detected in the product configuration. The initial copy of a product configuration backup becomes the baseline configuration. Once the baseline configuration is established, the Management application compares all additional product configuration backup files to the baseline configuration for deviation. You can view configuration deviation status on the Status Bar of the Management application window.

Viewing configuration deviation status

The Management application enables you to view the configuration deviation status at a glance by providing a configuration deviation status icon on the Status Bar.

Point to the configuration deviation status icon on the Status Bar. Depending on the status, one of the following status icons displays.

TABLE 78 Configuration Status Icons

Icon	Description
	No deviation in the baseline configuration — None of the product configurations are deviated from baseline configuration.
	Deviation in the baseline configuration — <*N*> products configurations are deviated from their baseline configuration.

To view the configuration changed details, click the configuration deviation status icon on the Status Bar. The **Change Tracking** tab of the **Configuration Repository** dialog box displays with the list of product configurations that have deviated from the baseline configuration. For more information, refer to "Change tracking" on page 753.

Change tracking

Use the change tracking feature to compare the latest backup configuration file with the configuration that is designated as the baseline.

1. Click the **IP** tab.
2. Select **Configure > Configuration > Configuration Repository**.
3. Click the **Change Tracking** tab.

   The **Change Tracking** tab of the **Configuration Repository** dialog box displays, as shown in Figure 287.

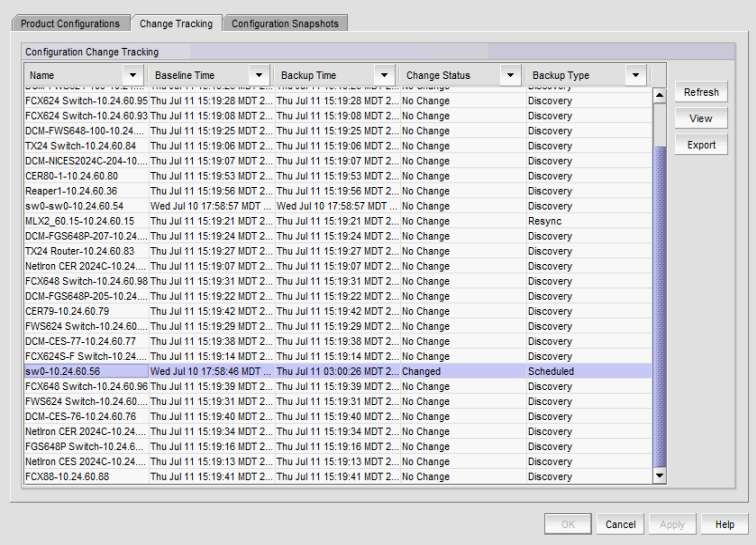


FIGURE 287 Configuration Repository dialog box - Change Tracking tab

The **Configuration Change Tracking** list displays the following information:

- **Name —** The product name and IP address
- **Baseline Time** — The date and time when the baseline configuration for the device was copied into the repository of the management server
- **Backup Time —** The time when the last backup attempt occurred for the selected device
- **Change Status** — The change status of the latest device backup
- **Backup Type** — How the backup was obtained. Backup options include the following types:
  - Discovery — Obtained after the discovery process
  - Pre-deployment — Occurs before a configuration change is deployed to the device
  - Post-deployment — Occurs after a configuration change is deployed to the device
  - Running Config Change Trap — Occurs when a running configuration is changed
  - Startup Config Change Trap — Occurs when a startup configuration is changed
  - Re-sync — Occurs when a trap is generated by the device during a startup or running configuration change, or when a user performs a manual resynchronization of the device
    For Network OS devices, Re-sync backup occurs after manual rediscovery of the VCS cluster member device and when a CLI configuration deployment occurs on the product.
  - Manual — Occurs when a user clicks the **Save Running/Startup Configuration** button
  - Scheduled — Occurs when obtained backup at the scheduled time

4. Perform one of the following actions:
   - Click the **Refresh** button to update the network and retrieve the latest data from the database.
   - Click the **View** button to compare the contents of the latest configuration and the baseline configuration. You can view only one configuration at a time.
   - Click the **Export** button to export the currently viewed change tracking records to a .csv file. The default file name is “Change_Tracking_Report.csv.”

5. Click **OK** to save the configuration.
6. Click **Close** to exit the dialog box.

Configuration snapshots

The **Configuration Repository** dialog box - **Configuration Snapshots** tab, shown in Figure 288, allows you to compare two configuration snapshots; for example, the pre-configuration and post-configuration snapshots.

1. Click the **IP** tab.
2. Select **Configure > Configuration > Configuration Repository**.
3. Click the **Configuration Snapshots** tab.

   The **Configuration Snapshots** tab displays, as shown in Figure 288.

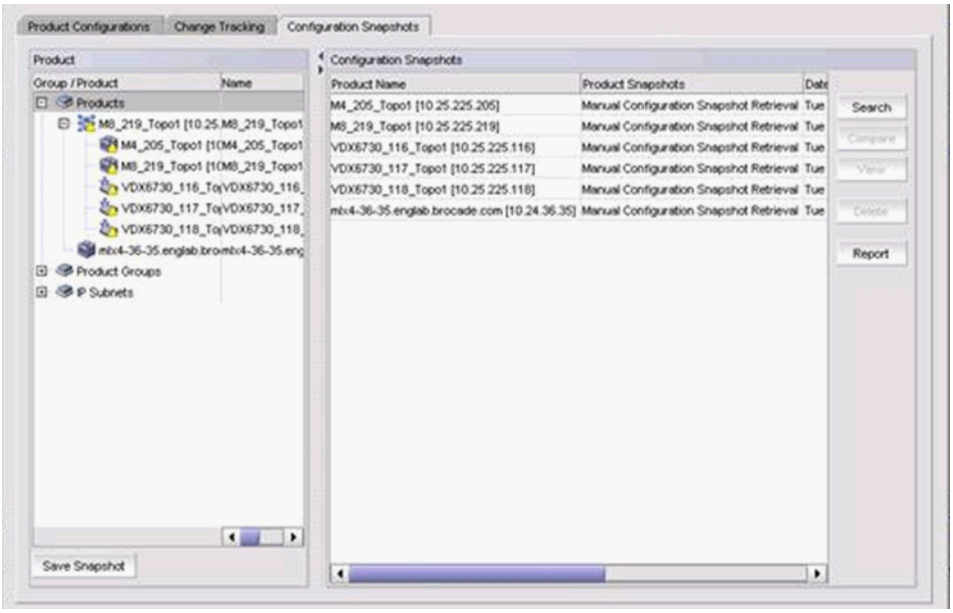


FIGURE 288 Configuration Repository dialog box - Configuration Snapshots tab

The **Configuration Snapshots** tab displays the following information:

- **Product Name** — The name of the product
- **Product Snapshots —** The product snapshots
- **Date** — The date when the snapshot file was stored in the server
- **Snapshot Type** — The type of snapshot generated. There are three types:
  - Manual: Generated manually by clicking the **Save Snapshot** button on the Backup Configuration Manager.
  - Pre-Snapshot: Generated before the new configuration was deployed to the device.
  - Post-Snapshot: Generated after the new configuration was deployed to the device.
- **CLI Template —** The name of the snapshot template used for the pre- or post-snapshot deployment.
- **Status —** The snapshot status

4. Click the following buttons to access the corresponding dialog boxes:
   - **Search** button — Click to launch the **Search Pre/Post Snapshots** dialog box, which allows you to search the contents of snapshots in the repository of the management server. Refer to "Searching the configuration repository" on page 751 for more information.
   - **Compare** button — Select two snapshots (same product or two different products) and click to launch the **Comparison** dialog box.

     If you select two snapshots from the **Configuration Snapshots** list and click **Compare**, the differences between the two configurations are highlighted.
   - **View** button — Select a row in the **Configuration Snapshots** list and click to display the contents of the selected snapshot.
   - **Delete** button — Select one or more snapshots from the **Configuration Snapshots** list and click to manually delete the snapshots from the repository of the management server.
   - **Report** button — Click to launch the **Configuration Snapshot Report** dialog box. Refer to "Generating a configuration snapshot report" on page 758 for more information.

Comparing configuration snapshots

The **Comparison** dialog box allows you to display the contents of two configurations side-by-side. To compare two configuration snapshots, perform the following steps.

1. Click the **IP** tab.
2. Select **Configure > Configuration > Configuration Repository**.
3. Click the **Configuration Snapshots** tab.
4. Select one or more products to view the snapshots.
5. Select two snapshots and click **Compare**.

   The **Compare** dialog box displays, as shown in Figure 289.

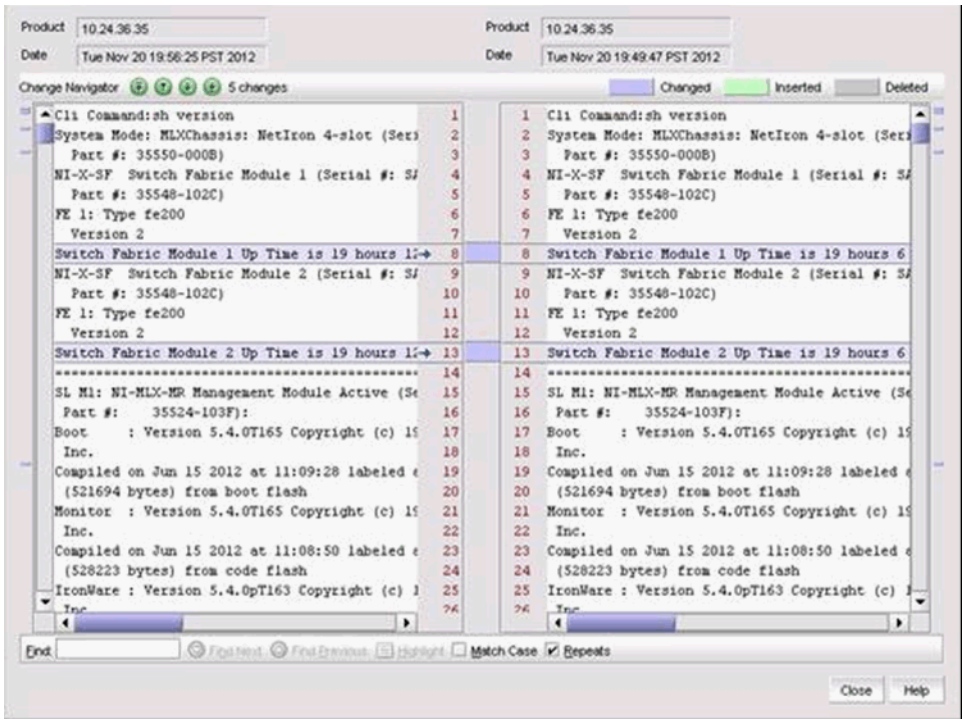


FIGURE 289 Compare dialog box

The **Compare** dialog box displays the following information:

- **Product** — The IP address of the device.
- **Date** — The Displays the date the device configuration was taken.
- **Change Navigator** buttons/legend — The Enabled when there is at least one change between to two compared files.
  - Go to first change button ( ) — Click to move to the first change.
  - Go to previous change button ( ) — Click to move to the previous change.
  - Go to next change button ( ) — Click to move to the next change.
  - Go to last change button ( ) — Click to move to the last change.
  - Number of changes label — Indicates the number of changes. If there are no differences, displays “No change”.
  - Differences legend — Displays the color legend for differences:
    - Changed status displays in blue.
    - Inserted status displays in green.
    - Deleted status displays in grey.
- **Phrase not found** icon — Displays when the search text string is not found.
- Configuration contents areas — Displays the contents of the selected configurations.
- **Find** — Enter a text string and take one of the following actions:
  - Click **Find Next** — Searches the next matching string in the configuration.
  - Click **Find Previous** — Searches the previous matching string in the configuration.
- **Highlight** grid — Click to highlight the text string.

- **Match Case** check box — Click to render the search case-sensitive.
- **Repeats** check box — Click to continue the search at the top when the bottom is reached.

6. Click **Close**.

Generating a configuration snapshot report

If the configuration snapshot list is too long, you can condense the list by running a report. To generate a configuration snapshot report, perform the following steps.

1. Click the **IP** tab.
2. Select **Configure > Configuration > Configuration Repository**.
3. Click the **Configuration Snapshots** tab.
4. Click the **Report** button.

   The **Configuration Snapshot Report** dialog box displays, as shown in Figure 290.

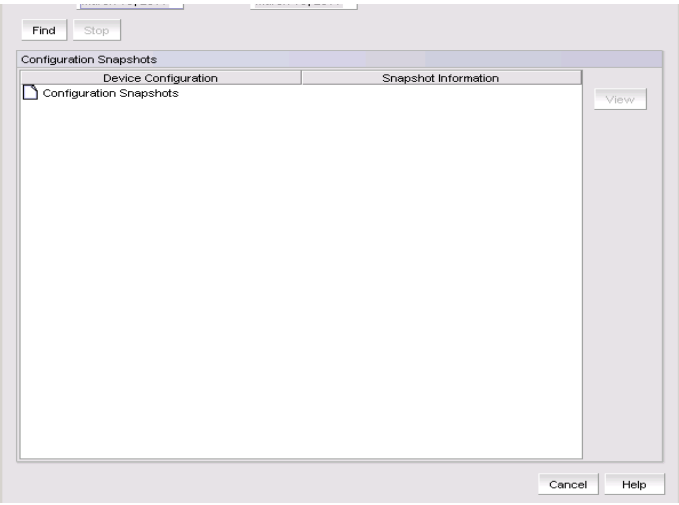


FIGURE 290 Configuration Snapshot Report dialog box

5. Select the start date and end date of the configuration snapshots you want to view.
6. Click **Find**.

   The Management application displays the list of snapshots that match the start date and end date you specified.

7. You can expand each tree node to view details about the configuration snapshot. Expand the configuration snapshot name under the **Device Configuration** column to display the list of configuration snapshots that have been recorded for that device configuration.
8. Expand a specific configuration snapshot folder to display the status of each record. Status can be one of the following:

   - Not Applicable
   - Change — The device configuration deployment included both pre- and post-configuration snapshot options. There is a difference between the pre-configuration snapshot and the post- configuration snapshot.

- No Change — The device configuration deployment included pre-configuration and post-configuration snapshots. There is no difference between the two snapshots.
- Error — An error was encountered in one or more devices during the deployment of the snapshots. The devices where the error occurred are listed under the Error status.

NOTE
Click the **Stop** button to stop running the configuration snapshot report.

Viewing the pre- and post-configuration snapshot

You can create a device configuration payload that issues device-monitoring commands to the devices when the payload is deployed. Device-monitoring commands can be issued before (pre-configuration snapshot), after (post-configuration snapshot), or before and after (pre-payload deployment and post-payload deployment).

Outputs of the device-monitoring commands are available as configuration snapshots. To view these snapshots, complete the following steps.

1. Click the **IP** tab.
2. Select **Configure > Configuration > Configuration Repository**.
3. Click the **Configuration Snapshots** tab.
4. Select a device from the **Product Name** column to display the configuration snapshots that are available for that device.
5. Click **View** to display information for that deployment.

   The **View Pre/Post Configuration Snapshot** dialog box displays details of the selected configuration.

NOTE
You can view only one snapshot at a time.

- **Device** — The IP address of the product.
- **Date** — The date and time when deployment was initiated.
- **Device Configuration** list — Displays the name of the deployed configuration, and can come from any one of the following:
  - Payload configuration name, saved using the Configuration Wizard.
  - MAC filter configuration name.
  - VLAN configuration name.
  - Manual Configuration Snapshot Retrieval, which identifies a configuration retrieved by clicking the **Save Snapshot** button.
  - INTERNAL:user-date&time, which indicates a payload deployment with pre- or post-snapshot properties, but the payload was not saved.
- **Snapshot Template** — The name of the snapshot template used for the pre- or post-snapshot deployment.

- **Snapshot Type** — The type of snapshot generated. There are three types:
  - Manual: Generated manually by clicking the **Save Snapshot** button on the Backup Configuration Manager.
  - Pre-Snapshot: Generated before the new configuration was deployed to the device.
  - Post-Snapshot: Generated after the new configuration was deployed to the device.
- **CLI Command** — The name of the device-monitoring template from the CLI Configuration Manager used for the pre- or post-snapshot deployment.
- **Configuration** list — Displays details of the snapshot.
- **Find** — Enter a text string and perform one of the following actions:
  - Click **Find Next** — Searches the next matching string in the configuration.
  - Click **Find Previous** — Searches the previous matching string in the configuration.
- **Reached bottom of the page** icon — Displays when there are no more entries to display.
- **Highlight** grid — Click to highlight the text string.
- **Match Case** check box — Click to render the search case-sensitive.
- **Repeats** check box — Click to continue the search at the top when the bottom is reached.

Saving a configuration snapshot

You can select a CLI template from the **Save Configuration Snapshot** dialog box. The CLI template is the product-monitoring template from the CLI Configuration Manager, used for pre- or post-configuration snapshot deployment.

To select and retrieve a CLI template, perform the following steps.

1. Click the **IP** tab.
2. Select **Configure > Configuration > Configuration Repository**.
3. Click the **Configuration Snapshots** tab.
4. Select a product from the **Group/Product** list.

   If no CLI product-monitoring templates exist, a message displays, prompting you to create a CLI product-monitoring template using CLI Configuration Manager.
5. Click **Save Snapshot**.

   The **Save Configuration Snapshot** dialog box displays, as shown in Figure 291.

FIGURE 291 Save Configuration Snapshot dialog box

6. Select a product-monitoring template that was previously created through the CLI Configuration Manager from the **CLI template** list.

   Make sure the template you select is configured for the selected products. You cannot apply an IronWare template to a Network OS product.

7. Click **OK** to save the configuration snapshot.

   The **Save Snapshot Status** dialog box displays details of the backup status.

   - **Backup Status** list — Displays the product name and IP address, as well as the progress and status of the configuration save.
   - **Status Details** — Displays details of a pending configuration save.

     Click **Abort** to abort a pending configuration save.

Searching the configuration snaphots

The **Search Pre/Post Snapshots** dialog box allows searching for products that have a particular snapshot in the management server's repository. Use the search feature to refine the snapshot repository based on the filter criteria described in this section.

1. Click the **IP** tab.
2. Select **Configure > Configuration > Configuration Repository**.
3. Click the **Configuration Snapshots** tab.
4. Click the **Search** button.

   The **Search Pre/Post Snapshots** dialog box, as shown in Figure 292, displays.

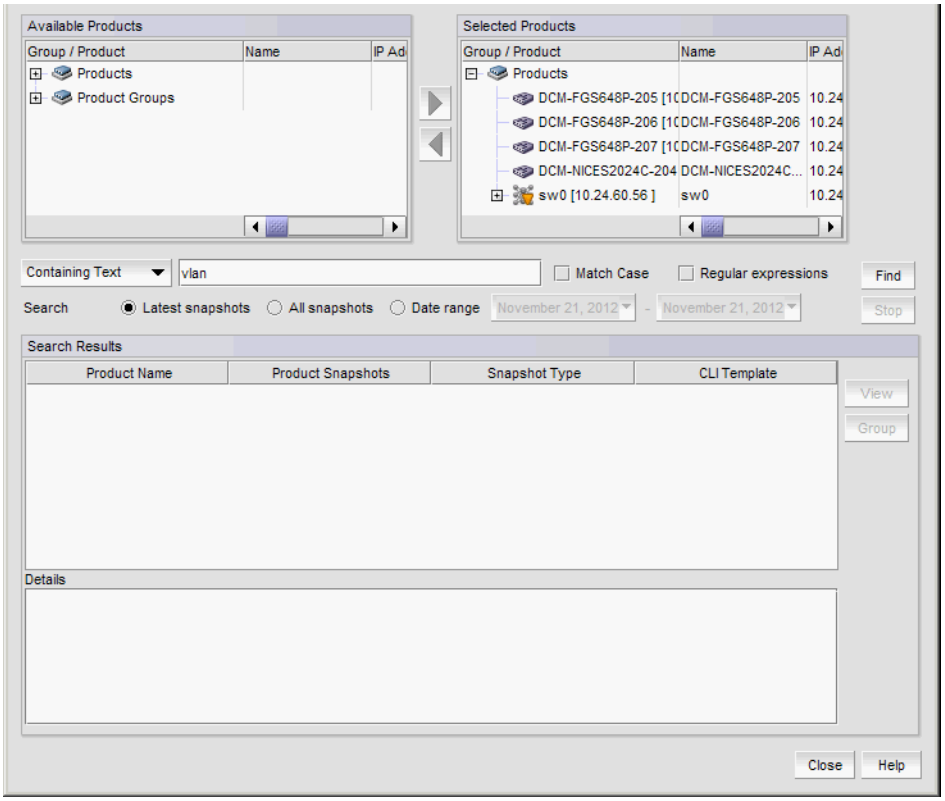


FIGURE 292 Search Pre/Post Snapshots dialog box

5. Select a product from the **Available Products** list and click the right arrow button to move one or more products to the **Selected Products** list.

Press **Ctrl** or **Shift** and then click each product to select more than one product.

6. Enter a search text string, with a limit of 255 characters, into the **Containing Text** field. This text string is used to search on snapshots of the selected products.

   Press **Ctrl** or **Shift** and then click each product to select more than one product.

7. Enable the following options, as required:
   - **Match Case** check box - Select the check box to make the search case-sensitive.
   - **Regular expressions** check box - Select the check box to use unicode regular expressions in your search.
   - **Search** options — Specify the following types of available searches:
     - **Latest configurations** — Searches the text in the most recent snapshots of the selected products.
     - **All configurations** — Searches the text in all snapshots of the selected products.
     - **Date range** — Searches the snapshot files of the selected products within the specified date range.
8. Click the **Find** button to find the text string and display the search results in the **Search Results** list.
9. Click the **Stop** button to stop the search in progress.
10. Click the **View** button to display the contents of the selected snapshot file. The snapshot entry that matches the search criteria is displayed in red.
11. Click the **Group** button to create product groups.

    NOTE
    You can only use the Product Group feature if you have the Configuration Management privilege and the **Search Pre/Post Snapshots** dialog box has search results.

12. Click **Close** to close the **Search Pre/Post Snapshots** dialog box.

Schedule backup

Using the **Schedule Backup** dialog box, you can poll the IronWare OS or Network OS product at regular intervals. You must have the Configuration Management privilege in your user account or role to access the Backup Scheduler.

NOTE
By default, the Backup Scheduler backs up configurations once a day, at 1:00 AM, and software images once a day, at 2:00 AM. Use the Backup Scheduler if you want to change the default.

Scheduling a configuration backup

The backup scheduler contains two types of scheduled backups: automatic configuration backup and automatic software image backup. This section presents a procedure for automatic configuration backup.

NOTE
The Management application enables you to save the same switch configuration to the repository using two methods: on demand (Configure > Configuration > Save) or by defining a schedule (Configuration > Schedule Backup).

To schedule a configuration backup, complete the following steps.

1. Click the **IP** tab.
2. Select **Configure > Configuration > Schedule Backup**.

   The **Schedule Backup** dialog box displays.

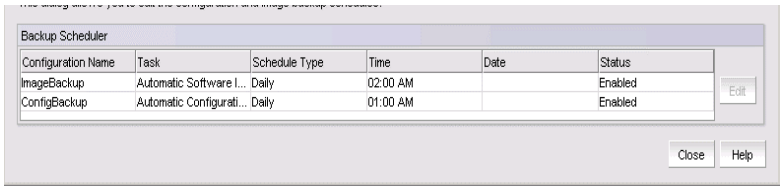


FIGURE 293 Schedule Backup dialog box

3. Select a backup configuration from the **Backup Scheduler** list.
4. Click the **Edit** button.

   The **Edit Automatic Configuration Backup** dialog box displays, as shown in Figure 294.

FIGURE 294 Edit Automatic Configuration Backup dialog box

5. Enter the following information:
   - Frequency - The interval at which scheduled tasks are to run. The following schedule types are available:
     - One Time
     - Hourly
     - Daily
     - Weekly
     - Monthly
     - Yearly
   - Time (hh:mm) - The time of day to run the backup. Options include hour, minute, and AM or PM.
   - Minutes past the hour - For hourly backups, select the number of minutes past the hour from the list.
   - Day of the week - If you selected Weekly as the frequency type, select the day from the list.

- Day of the month - If you selected Monthly as the frequency type, select the day of the month from the list.

6. Click **OK**.

   The new schedule appears in the **Backup Scheduler** list of the **Schedule Backup** dialog box.

   When scheduled backups begin, the Management application polls each product to check its current configuration.

NOTE
Software image backup is not initiated on VDX or VCS devices.

Disabling a backup schedule

To disable a scheduled backup, complete the following steps.

1. Select an entry in the **Backup Scheduler** list of the **Schedule Backup** dialog box.
2. Click **Edit**.

   The **Edit Automatic Configuration Backup** dialog box displays.

3. Select the **Disable Scheduling** check box.

   The Status column is updated as **Disabled**.

Chapter

24

IP Configuration Wizard

In this chapter

Configuration requirements

The Configuration Wizard allows you to create and deploy payloads of configurations to IOS devices on the network. A payload is a configuration of device properties, such as SNMP settings, user account information, software image, and others.

NOTE
You cannot use the Configuration Wizard to deploy configurations to non-IOS devices.

Before creating payload configurations, make sure the following prerequisites have been completed:

- The discovery process must be run to add devices to the Management application. Devices must be under the Management application before you can deploy configurations to them.
- The Configuration Management privilege must be in your Management application user account or role.
- You must configure the username and password required to log in to the device when using the Command Line Interface (CLI). Some payloads, such as image updates, banners, and SNMP community strings, are deployed to devices using the CLI instead of SNMP; therefore, the Management application must log in to the device with a CLI username and password.

Payloads

Payloads are defined as product payloads or interface payloads. Product payloads are deployed to the devices, whereas interface payloads are deployed to ports.

The available payloads are listed in Table 79.

TABLE 79 Payloads available for deployment

Payload name	Description
Product Payloads:	
802.1Q Tag Type	Sets the tag type, or tag ID, that identifies the aggregate VLAN.
Banners	Displays messages when a user logs in to a device at a Privileged EXEC CLI level, or when a user accesses a device using Telnet or Secure Shell.
Boot Sequence	Specifies the sources from which the device will boot.
CLI Configuration	Deploys CLI configuration definitions that have been created in the CLI Configuration Manager to wired devices.
CLI Product Monitoring	Deploys CLI product monitoring definitions that have been created in the CLI Configuration Manager to wired devices.
DNS	Defines a domain that serves as a gateway to the DNS (Domain Name Server).
DNS Name Search List	Creates a list of DNS names and adds, deletes, or replaces target products that match the names in the list.
Enable Passwords	Assigns passwords to management privilege levels on the IOS device.
FDP Settings	Enables IOS devices to advertise themselves to other IOS devices on the network.
Image Update: Boot	Deploys boot and monitor images to devices.
Image Update: Software	Updates the software image file on a device.
Firmware Image Update: Unified	Updates the unified firmware image file on a device.
LDP Settings	Configures LDP settings on a product.
Protocols	Enables or disables routing protocols on devices. This payload cannot be deployed to non-IP IOS devices.
RADIUS Parameters	Specifies the number of times an IOS device can resend an authentication request and wait for a response from the RADIUS server.
RADIUS Servers	Indicates which RADIUS servers are used for authentication.
Reload Products	Reloads selected products at one time.
SNMP Community Strings	Configures SNMP v1 and V2 community strings.
SNMP Identification	Sets the contact, location, and system name information about a product.
SNMP Trap Enable	Configures which standard traps are sent to trap receivers by the product.
SNMP Trap Receivers	Defines the trap receivers for a product.
SNMP V3 Settings	Defines the user accounts that can access the product using SNMP v3.
Syslog Receivers	Defines the systems that have been identified to receive system log events.
TACACS+ Parameters	Configures the TACACS/TACACS+ retransmit, timeout, and dead time authentication parameters.

TABLE 79 Payloads available for deployment (Continued)

Payload name	Description
TACACS+ Servers	Indicates which TACACS/TACACS+ servers are to be used for authentication.
Telnet	Sets Telnet password and idle timeout value, and enables Telnet authentication on devices for use with AAA authentication.
Time Zone/SNTP	Specifies the time zone and specifies whether the date and time are to be set by an SNTP server clock.
User Accounts	Configures accounts for users and administrators who are allowed to access the product.
Interface Payloads:	
LDP Settings	Configures LDP settings on an interface.
PoE Control	Powers up and powers down an interface that can be powered up over an Ethernet connection.
Port	Changes basic port parameters in VLAN Manager.
sFlow Configuration	Enables and configures sFlow on a device, globally or per interface
SNMP Trap for Port	Specifies whether a link-change trap is sent if the state of a port changes.

Creating a payload configuration

The Configuration Wizard facilitates the creation and deployment of payload configurations.

1. Select **Configure > Configuration Wizard**.
2. Click **Add**.

   The **Select Payload** pane displays, as shown in Figure 295. This pane displays all of the payloads you can deploy to wired devices.

   Payloads are grouped under **Product Payloads** or **Interface Payloads**. Product payloads are deployed to the devices, whereas interface payloads are deployed to ports.

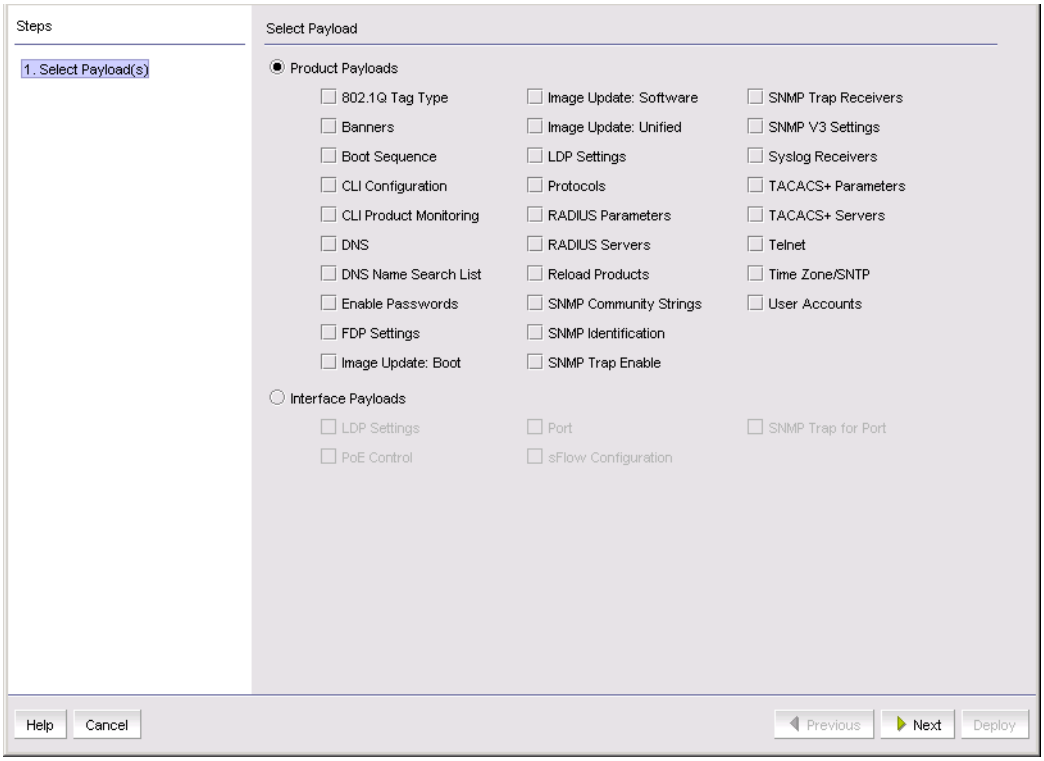


FIGURE 295 Configuration dialog box - Select Payload pane

3. Select **Product Payloads** or **Interface Payloads**, and select the payloads you want to configure.

   You can include more than one payload in a configuration. See Table 79 on page 766 for a brief description of the payloads.

4. Click **Next**.

   The next pane that displays depends on the payloads you are configuring. For example, Figure 296 shows the next pane for the SNMP Identification payload.

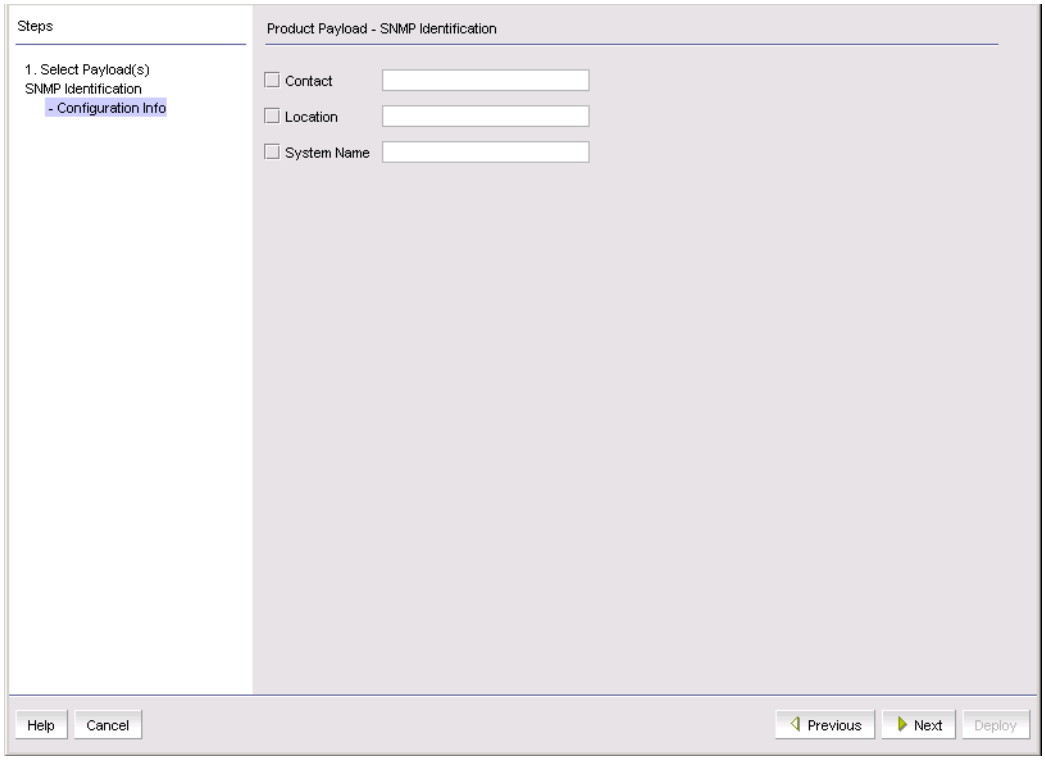


FIGURE 296 Configuration dialog box - Product Payload - SNMP Identification pane

5. Enter the required information for the payload and click **Next**. Click **Help** for detailed information on each payload you can define.

   After all of the payloads you have selected are configured, the **Deployment Targets** pane displays, as shown in Figure 297 on page 770.

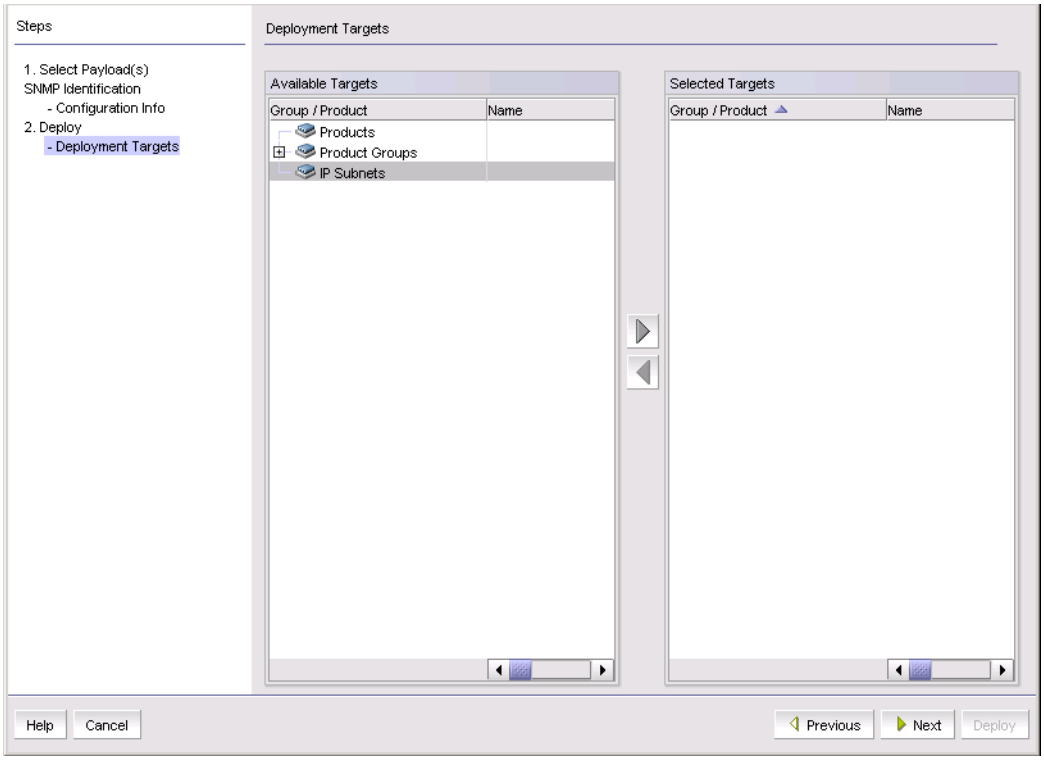


FIGURE 297 Configuration dialog box - Deployment Targets pane

6. In the **Available Targets** list, select the products, product groups, and IP subnets to which the payload configuration is to be deployed.

   - To select a target, expand the entry to display the entries under it, click the target in the **Available Targets** list, and click the right-arrow button to move it to the **Selected Targets** list.

     If the target is not on the list, run the discovery process.

     NOTE
     The **Deployment Targets** pane of the **Configuration** wizard does not include VCS devices when launched from the **Configuration Wizard** command on the **Configure** menu.

   - To remove a target, select it in the **Selected Targets** list and click the left arrow button to move it back to the **Available Targets** list.

7. Click **Next**.

   The **Deployment Properties** pane displays, as shown in Figure 298 on page 771.

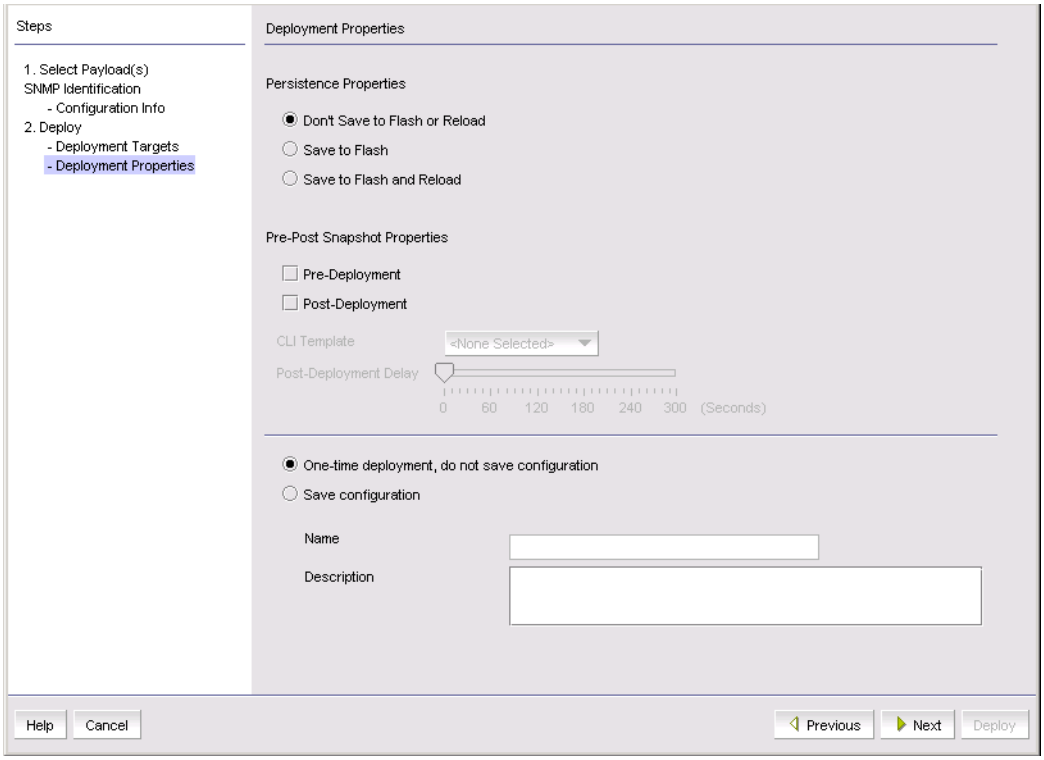


FIGURE 298 Configuration dialog box - Deployment Properties pane

8. Select one of the persistence properties.

- **Don't Save to Flash or Reload**

  Select this option if you just want to update the device running configuration. The payload configuration is not saved to the device flash memory, nor is the device rebooted when the payload configuration is deployed.

- **Save to Flash**

  Select this option if you want to make the payload configuration permanent in the device flash memory and saved to the running configuration. Selecting this option is the same as entering a **write memory** command on the device CLI. The payload configuration is applied to the device when the device reboots.

- **Save to Flash and Reload**

  Select this option if you want to save the payload configuration to the device flash memory and reboot the device. It is the same as entering the **write memory** and **reload** commands to the device CLI.

  NOTE
  This option is available only to Management application users who have the "Reload Device" privilege in their user account.

9. (*Optional*) Enter the following information if you want the Management application to run and save a report before or after this configuration is deployed to the device.
    a. Select the **Pre-Deployment** check box if you want the Management application to run and save a report *before* this configuration is deployed.
    b. Select the **Post-Deployment** check box if you want the Management application to run and save a report *after* this configuration is deployed.
    c. From the **CLI Template** list, select the template that contains the **show** commands that are executed before or after this configuration is deployed to the target.
    d. If you selected the **Post-Deployment** check box, and you want the Management application to wait a few seconds after this deployment before proceeding to the post-deployment, indicate the delay on the **Post-Deployment Delay** slider.
10. Select whether you want to save this configuration.
    - Select **One-time deployment, do not save configuration** if you want to deploy the configuration, but not save it.
    - Select **Save configuration** if you want the Management application to save the configuration.

      If you select this option, enter a name for the configuration and an optional description in the **Name** and **Description** fields.
11. Click **Next**.

    If you selected **Save configuration**, the **Deployment Schedule** pane displays, as shown in Figure 299. Continue with step 12.

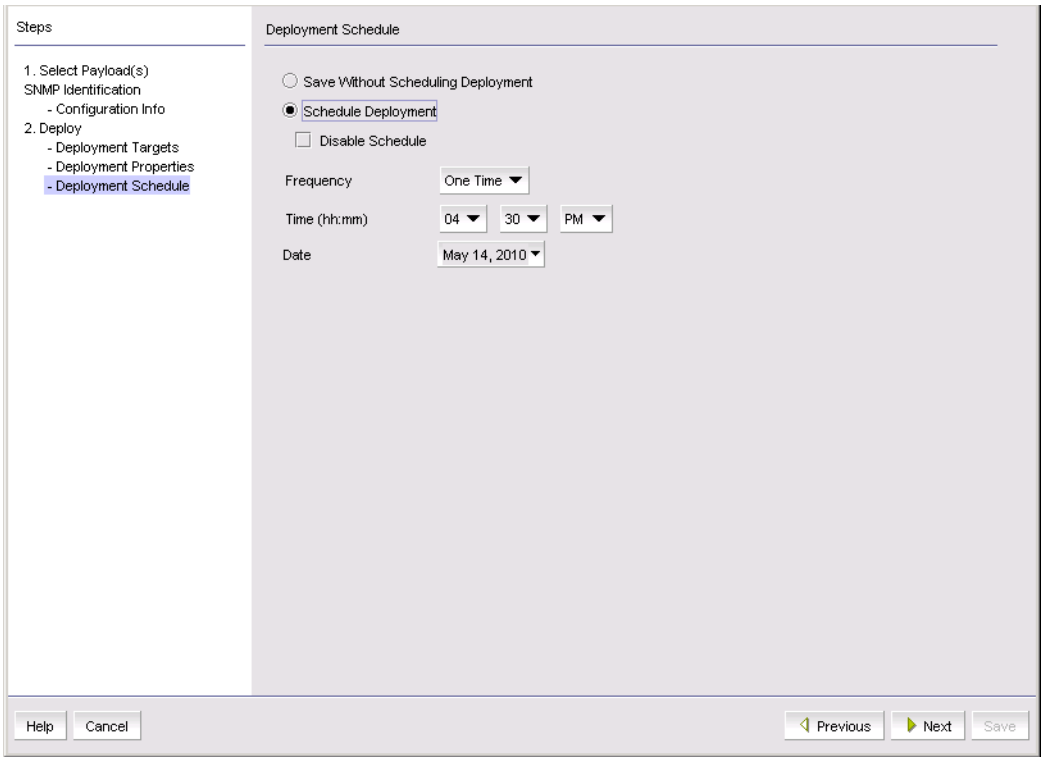


FIGURE 299 Configuration dialog box - Deployment Schedule pane

12. Select **Save Without Scheduling Deployment** or **Schedule Deployment**.

    If you select **Schedule Deployment**, select the frequency, time, and date parameters for the deployment.

13. Click **Next**.

    The **Summary Page** pane displays, as shown in Figure 300.

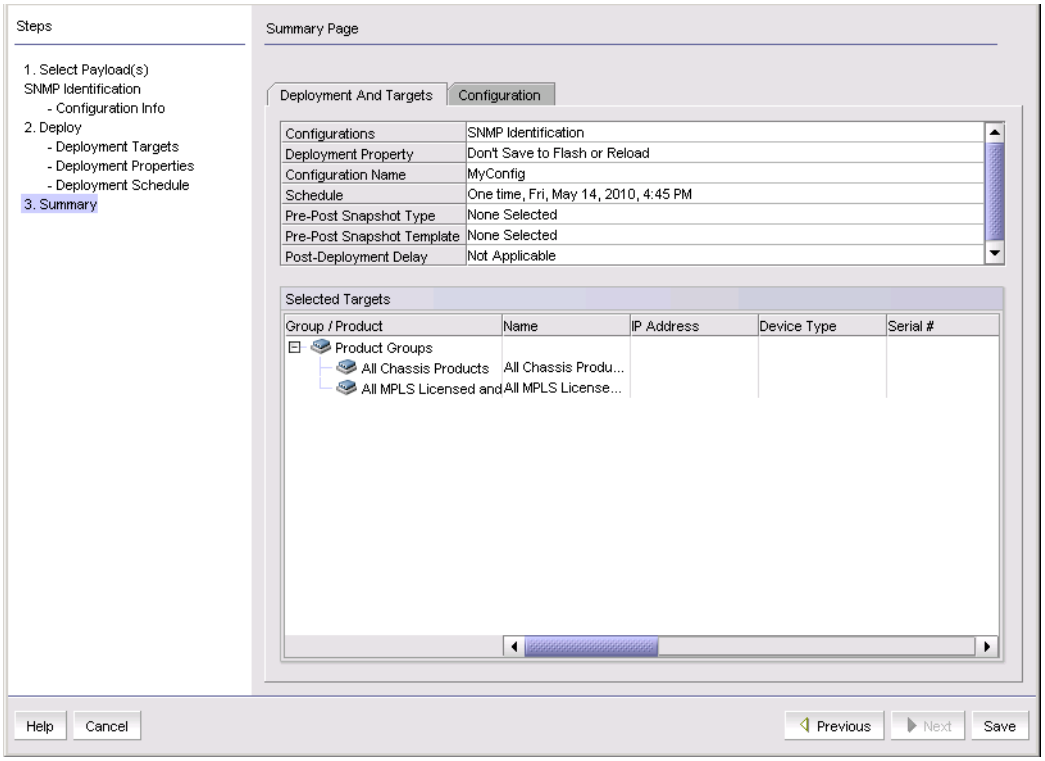


FIGURE 300 Configuration dialog box - Summary Page pane

14. Review the information on the **Summary Page** pane.

    - The **Deployment and Targets** tab shows the deployment definition and the targets in the configuration. The **Selected Targets** list allows you to verify to which devices the payloads in the configuration are deployed.
    - The **Configuration** tab summarizes the payloads in the configuration you have created.

    If you must make changes, click **Previous** to return to a previous pane, or click another pane in the **Steps** area on the left side of this pane.

15. Click **Save** or **Deploy**. The availability of the **Save** and **Deploy** buttons depends on what you selected on the **Deployment Properties** pane.

    - **Save** appears if you selected **Save configuration**. The saved configuration then appears in the **Product Configurations** list in the **Configuration Wizard** dialog box.
    - **Deploy** appears if you selected **One-time deployment, do not save configuration**. If you click **Deploy**, the **Deployment Status** dialog box displays. If you want to view the configuration deployment status at another time, select **Reports > Deployment**.

Duplicating a payload configuration

You can create a payload configuration by copying an existing configuration.

1. Select **Configure > Configuration Wizard**.
2. Select a configuration from the **Product Configurations** list.
3. Click **Duplicate**.

   The **Copy Configuration** dialog box displays.
4. Enter a name for the new payload configuration. If you do not enter a name, the Management application assigns the name "*XXX* copy", where *XXX* is the name of the original configuration.
5. Click **OK** to close the dialog box.

   You can then use the **Edit** button to make changes to the payload configuration.

Modifying a payload configuration

You can add payloads to a configuration, delete payloads from a configuration, and modify existing payloads in a configuration.

You can also change the deployment targets, properties, and schedule.

1. Select **Configure > Configuration Wizard**.
2. Select a configuration from the **Product Configurations** list.
3. Click **Edit**.

   The **Select Payload** pane displays. The payloads that currently exist in the configuration are checked.

   On the left side of the wizard, the **Steps** area displays the existing payloads and the deployment items you can change (targets, properties, schedule), as shown in Figure 301 on page 775.

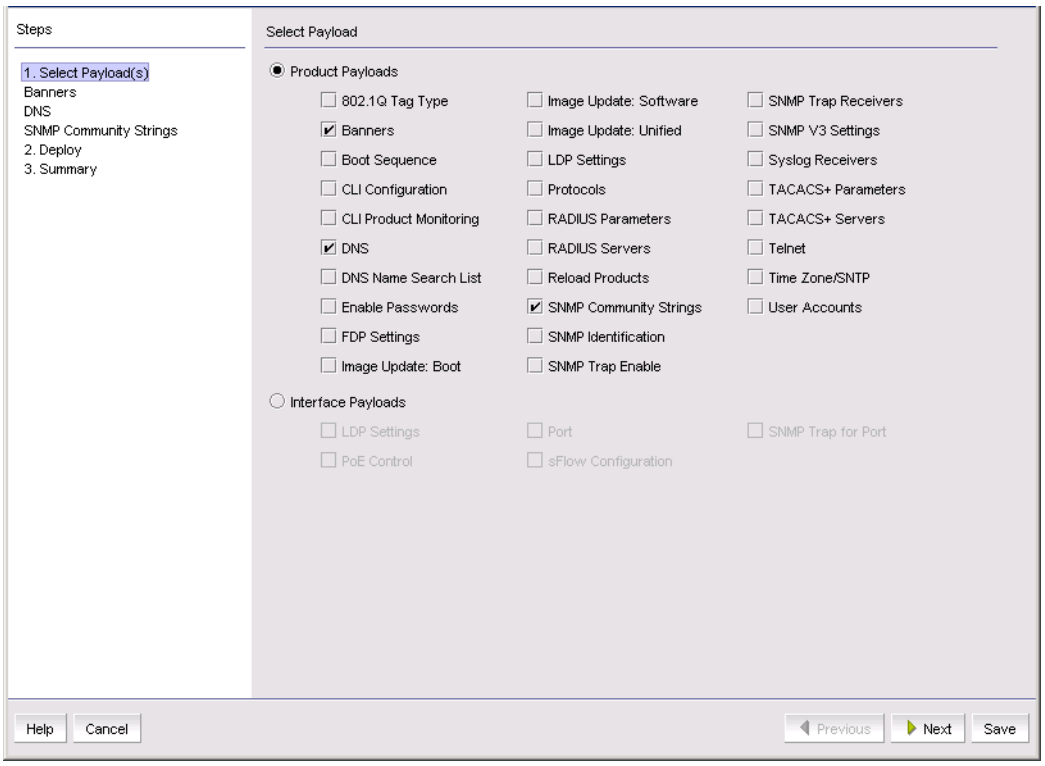


FIGURE 301 Configuration dialog box - Select Payload pane for editing a configuration

4. Add or remove payloads in the configuration.
   - To add a payload to the configuration, select either **Product Payloads** or **Interface Payloads**, and then select the payload you want to add.
   - To remove a payload from the configuration, clear the check box of the payload.

     Note that a configuration must have at least one payload. You cannot save a configuration unless it has at least one payload.
5. Modify what needs to be changed in the **Select Payload**, **Deployment Targets**, **Deployment Properties**, and other panes.
   - Click **Next** to navigate sequentially through the panes.
   - Click an item in the **Steps** area to jump directly to the appropriate section.
   - Click **Save** at any time to save your changes and return to the Configuration Wizard dialog box.

   Refer to the steps in "Creating a payload configuration" on page 767 for additional information.

Deploying a payload configuration

Payload configurations are deployed to targets in one of the following ways:

- On a scheduled basis, if a deployment schedule has been set up for the configuration.
- On demand, if **Save Without Scheduling Deployment** is selected in the **Deployment Schedule** pane of the Configuration Wizard. Configurations can be manually deployed when required.

Refer to step 12 in "Creating a payload configuration" on page 767 for more information on setting up a deployment schedule.

Use the following procedure to deploy the configuration on demand.

1. Select **Configure > Configuration Wizard**.
2. Select the configuration you want to deploy from the **Product Configurations** list.
3. Click **Deploy**.
4. Click **Yes** in the confirmation message.

   The **Deployment Status** dialog box displays.

   NOTE
   If a configuration has more than one payload and a failure occurs during deployment of a payload, the Management application aborts the deployment of that payload, but continues to deploy the remaining payloads.

5. Click **Close** when you are finished viewing the information.

Deleting a payload configuration

1. Select **Configure > Configuration Wizard**.
2. Select the configuration you want to delete from the **Product Configurations** list.
3. Click **Delete**.
4. Click **Yes** in the confirmation message.

Chapter

25

CLI Configuration Management

In this chapter

CLI configuration overview

NOTE
The CLI Configuration feature requires the IP CLI Configuration privilege.

NOTE
CLI Configuration deployment requires the IP - CLI Configuration Deploy privilege.

NOTE
The CLI Configuration feature cannot manage non-IP devices or third-party IP devices.

CLI Configuration provides a text-based interface that allows you to enter command line interface (CLI) commands to create configurations and reports for IronWare and Network OS devices. You can deploy the configurations and reports on demand or at a scheduled time.

Configuration requirements

Before you use the CLI Configuration, you should meet the following requirements:

- Telnet or SSH (or both) must be selected on the Management application server to match the protocol(s) with the devices. For more information about configuring Telnet or SSH, refer to "Product communication settings" on page 169.
- Authentication and authorization methods required to deploy the payloads must be enabled on the devices to which the configurations are to be deployed.
- Passwords required to access the device must be entered for the device. You can enter the CLI password from the following dialog boxes:
  - **Definition** tab of the **Configuration or Monitoring Template** dialog box (refer to "Product configuration templates" on page 779 or "Monitoring configurations" on page 795).
  - **Default Passwords** tab on the **Global Settings** tab of the **Discover - Setup IP** dialog box (refer to "Default IP user credentials" on page 52).
  - **Edit product** dialog box (refer to "Editing IP device discovery" on page 87).
  - **CLI Credential** dialog box (refer to "Configuring CLI credentials" on page 209).

Viewing existing templates

The Management application provides several example Configuration templates. For a list of the example templates, refer to "CLI Templates" on page 1339.

Select **Configure > CLI Configuration**.

The **CLI Configuration** dialog box displays.

- **Templates** table — Displays a list of existing configurations.
  - **Name —** Name of the device configuration.
  - **Description —** Information about the configuration.
  - **Type —** Whether the template is a Configuration or Monitoring template.
  - **Parameters —** Indicates if parameters are included in the configuration.
  - **Additional Targets —** Indicates whether you selected to be prompted for additional targets during manual deployment.
  - **Scheduled —** Whether the configuration is scheduled (Yes) or not (No).
- **Add** button — Click to create a new configuration ("Creating a new product configuration" on page 779 or "Creating a monitoring configuration" on page 795).
- **Edit** button — Click to edit an existing configuration ("Editing a product configuration" on page 788 or "Editing a monitoring configuration" on page 801).
- **Duplicate** button — Click to copy an existing configuration ("Copying a product configuration" on page 787 or "Copying a monitoring configuration" on page 800).
- **Delete** button — Click to delete the selected configurations ("Deleting a configuration" on page 793).
- **Verify** button — Click to verify the selected configuration ("Testing a configuration" on page 789).
- **Deploy** button — Click to deploy the selected configuration ("CLI configuration deployment" on page 794).

Product configuration templates

You can create, modify, duplicate, delete, verify, and deploy a product configuration from the **CLI Configuration** dialog box. Product configurations allow you to create device configuration by entering a set of configuration CLI commands. To view a list of existing configurations, refer to "Viewing existing templates" on page 778. For information about the example templates, refer to "CLI Templates" on page 1339.

Creating a new product configuration

To create a new configuration, complete the following steps.

1. Select **Configure > CLI Configuration**.

   The **CLI Configuration** dialog box displays.

2. Click **Add**.

   The **CLI Template** dialog box displays.

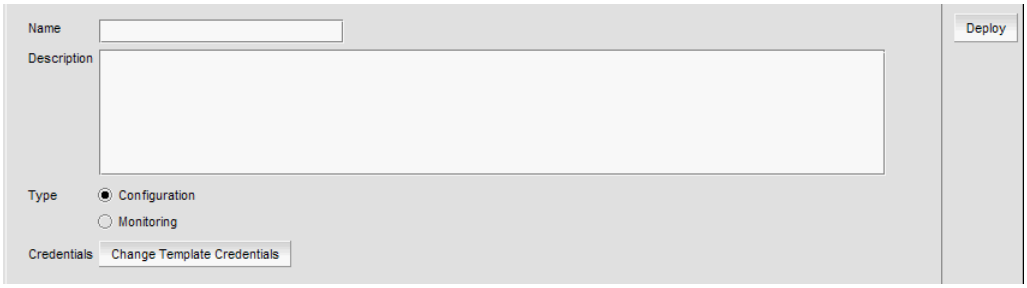


FIGURE 302 CLI Template dialog box - Definition tab

3. Click the **Definition** tab and enter a name and description for the new configuration.

NOTE
Do not use special characters in the name.

   a. Enter a name and description for the new configuration.

   b. Select **Configuration** to create a product configuration.

   c. To change CLI credentials, click **Change Template Credentials** and refer to "Changing product credentials" on page 784.

4. Click the **Target** tab and complete the following steps.

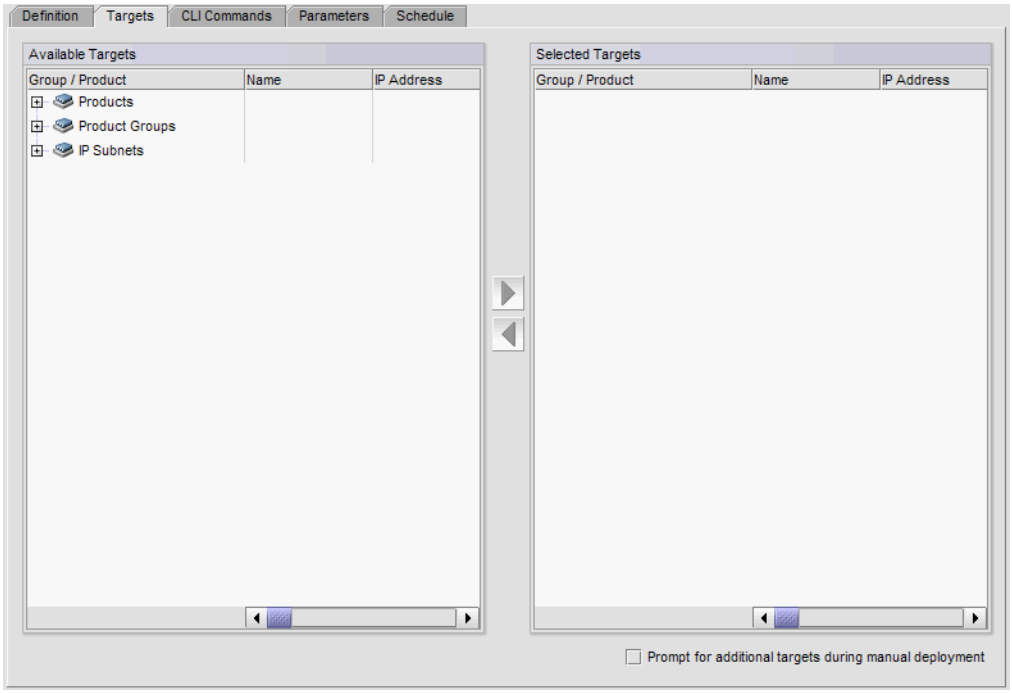


FIGURE 303 CLI Configuration Template dialog box - Target tab

a. Select the devices to which you want the configuration deployed from the **Available Targets** table.

   The **Available Targets** table displays an inventory of the available product targets and includes the same detail as the Product List (refer to "IP Product List" on page 284).

   You can deploy the configuration to individual devices, devices in a device group, or devices in an IP subnet.

   For VCS fabrics, you can deploy the configuration to one or more individual members in a fabric (select each member) or to all members of a fabric (select the VCS fabric).

b. Click the right arrow button to move your selection to the **Selected Targets** table.

   To search for devices, right-click anywhere in the table and select **Search**. For more information about searching for devices, refer to "Searching for a device" on page 299.

   The **Selected Targets** table displays the selected products and includes the same detail as the Product List (refer to "IP Product List" on page 284).

c. Select the **Prompt for additional targets during manual deployment** check box to be able to select additional targets during manual deployment.

5. Click the **CLI Commands** tab and complete the following steps.

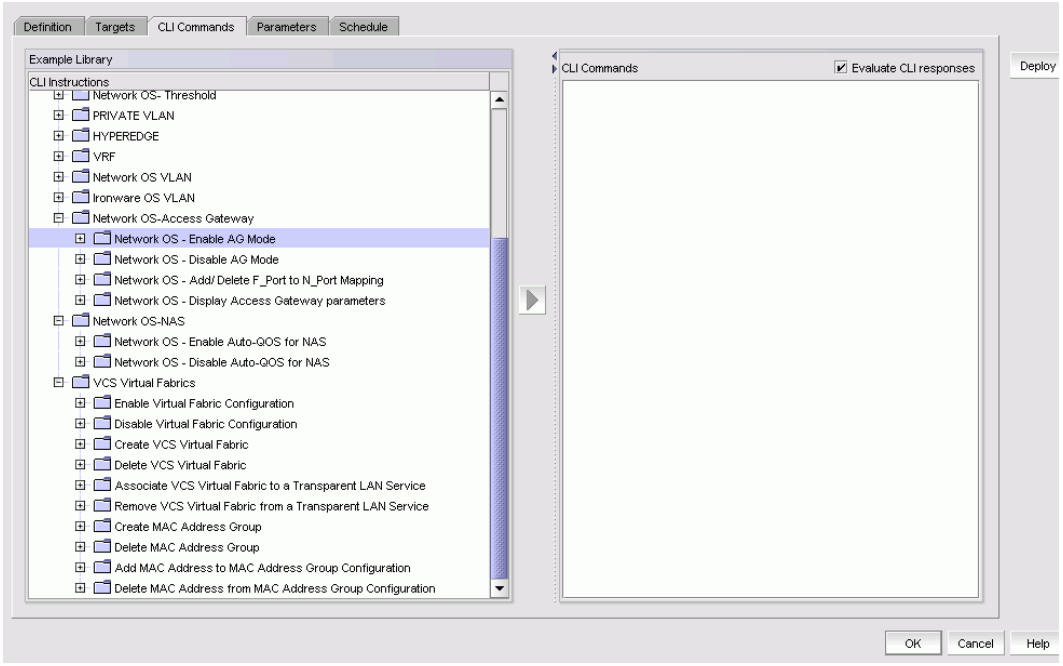


FIGURE 304 CLI Template dialog box - CLI Commands tab

a. (Configuration templates only) Select the **Evaluate CLI responses** check box to validate the CLI commands.

   You can add a dash (-) to the beginning of a CLI command to ignore command validation even when you select the **Evaluate CLI responses** check box.

   Clear the **Evaluate CLI responses** check box to send all CLI commands to the device regardless of the success or failure of the previous command.

b. Enter CLI commands in the **CLI Commands** field.

   For a list of guidelines to use when entering CLI commands, refer to "CLI command guidelines" on page 787.

   The Management application provides several CLI command examples (including ACL, MPLS, Network OS-AMPP, Network OS-Access Gateway, Network OS-QOS, MISCELLANEOUS, MCT, Network OS-THRESHOLDING, HYPEREDGE, VRF, VCS Virtual Fabrics, Network OS-NAS, PRIVATE VLAN, Ironware OS VLAN,and Network OS VLAN). To view the CLI command examples, navigate to the **Example CLI Commands** folder (refer to "CLI Templates" on page 1339).

   Add commands from the CLI templates or examples by selecting one or more commands from the **CLI Templates** or **Example CLI Commands** folder and clicking the right arrow button.

c. To enter a parameter for a CLI command, select the parameter type from the **CLI Commands** list - **Parameters** folder and click the right arrow to move the parameter type to the **CLI Commands** text area.

Parameters use the following format: $<*name*|*data_type*>, where *name* is the parameter and *data_type* is the type of parameter.

Parameter types include integer ($<name|INTEGER>), string ($<name|STRING>), slot/port ($<name|SLOT_PORT>), MAC address ($<name|MAC>), and IP address ($<name|IP_ADDRESS>).

d. Edit the parameter by entering the variable or character string you want to use for the parameter in place of the *name* variable.

NOTE
Each parameter must be unique. The Management application does not check for duplicate parameters.

```
access list 400 deny $<ip|IP_ADDRESS>
```

In the example, `access list 400 deny` is the CLI command, `ip` is the parameter variable and `IP_ADDRESS` is the parameter type.

e. (Optional) Select a template from the **CLI Templates** folder and click the right arrow to include it in the configuration.

This allows you to deploy more than one template to a device in a single deployment. Only templates defined in the Management application display. The list and button only display when there is at least one user-defined CLI template.

6. Click the **Parameters** tab and complete the following steps.

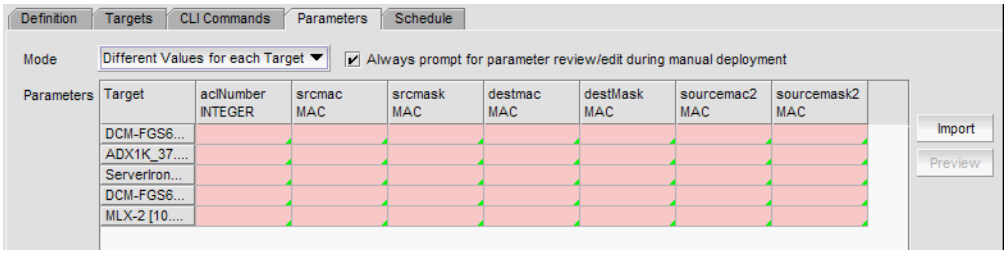


FIGURE 305 CLI Template dialog box - Parameters tab

a. Select the **Always prompt for parameter review/edit during manual deployment** check box to display the **Parameter** tab in the **Prompt** dialog box during manual deployment.

Clear to not display the **Parameter** tab in the **Prompt** dialog box during manual deployment. If this check box is clear and you do not fill in all parameter values, the **Prompt** dialog box displays.

When selected, the **Parameter** tab displays in the **Prompt** dialog box during manual deployment even if you filled in all parameter values on the **Parameters** tab of the **CLI Template** dialog box.

b. Select one of the following options from the **Mode** list for the parameter import mode.

- **Same Values for each Target —** Select to set the same values for all selected targets.
- **Different Values for each Target** — Select to set individual values for the selected targets.

c. Enter a value for each parameter in the associated field.

Note that the **Target** column remains visible at all times in the **Parameters** table.

Fields containing a green triangle ( ) in the lower right corner are editable. The fields only accepts valid values base on the parameter data type.

Parameters include the following options:

- String — Enter a string with a maximum of 64 ASCII characters.
- Integer — Enter an integer with a maximum of 12 numeric characters.
- Slot/Port — Enter the slot number and port number.
- MAC address — Enter hexadecimal characters with or without a valid delimiter (such as hyphen, colon, period, and space). Wildcards (such as ? and *) are supported.
- IP address — Enter an IPv4 or IPv6 address.

You can copy and paste new values for the parameter from an external file (plain text or table format). If the file you copy from is in table format, you can copy multiple fields (cells) at the same time.

To import parameter values from a CSV file, refer to "Importing parameter values into a configuration" on page 785.

7. Click the **Schedule** tab and complete the following steps.

a. Select the **Schedule** check box.

b. Choose one of the following options from the **Frequency** list.

- One Time (refer to "Configuring a one-time deployment schedule" on page 803)
- Hourly (refer to "Configuring an hourly deployment schedule" on page 803)
- Daily (refer to "Configuring a daily deployment schedule" on page 804)
- Weekly (refer to "Configuring a weekly deployment schedule" on page 804)
- Monthly (refer to "Configuring a monthly deployment schedule" on page 804)
- Yearly (refer to "Configuring a yearly deployment schedule" on page 805)

8. Review your entries on all the template tabs and choose one of the following options:

- Click **OK** to save the configuration and add it to the list of configurations on the **Configuration** tab. The new definition can be added to a configuration payload in the Configuration Wizard and deployed later.

  To test the configuration, refer to "Testing a configuration" on page 789.

- Click **Deploy** to deploy the configuration to the selected targets. Click **Yes** on the confirmation message.

  If you selected the **Prompt for additional targets during manual deployment** check box, the **Target** tab of the **Deployment of** *Configuration_Name* dialog box displays. Continue with step 9.

  If the configuration contains parameters that must be defined, the **Deployment of** *Configuration_Name* dialog box displays with a list of all parameters in the deployment. Go to step 10.

9. Define additional targets for the deployment (refer to step 4), as needed.

10. Edit the mode and the parameter values (refer to step 6), as needed.

11. Click **OK**.

    The **Deployment Status** dialog box displays, which allows you to view the progress and status of the deployment.

    Click **Abort** to stop the deployment.

    NOTE
    The abort action does not stop the tasks that have already started.

    When deployment is complete, click **Report** to view the **CLI Deployments Report**.

12. Click **Close** to close the **Deployment Status** dialog box.

    NOTE
    Closing the **Deployment Status** dialog box does not stop deployment.

    To check the results of the deployment in the Product CLI Report, refer to "CLI deployment reports" on page 802. For details about valid and invalid responses when you deploy a configuration, refer to "Valid and invalid responses from devices" on page 790.

Changing product credentials

Passwords required to access the device must be entered for the device.

1. Click **Change Template Credentials** on the **Definition** tab of the **CLI Template** dialog box.

   The **CLI Template** dialog box displays.

   NOTE
   If you selected the **Use User CLI Credential** check box in the **Policy** tab of the **Users** dialog box (refer to "Password policies" on page 198) and you configured credentials in your User Profile (refer to "Configuring CLI credentials" on page 209), the Management application only uses those credentials to access the device.

   NOTE
   Entering a password is not required if the password required to access the device is already entered during discovery or configured in your user profile.

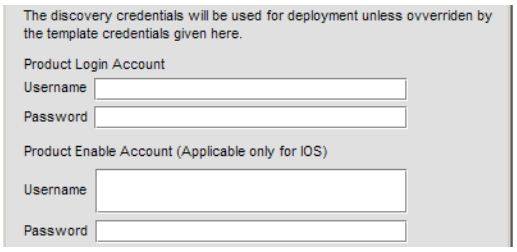


FIGURE 306 CLI Credentials dialog box

2. Enter the user name for the product in the **Product Login Account - Username** field.

NOTE
If Telnet is used to log in to the device and Telnet only requires a password, then enter the password in the **Password** field and leave the **Username** field blank.

3. Enter the password for the product in the **Product Login Account - Password** field.
4. (IronWare only) Enter the user name assigned to management privilege levels on the device in the **Product Enable Account - Username** field.

NOTE
If a device only requires the enable password, then enter the password in the **Password** field and leave the **Username** field blank.

5. (IronWare only) Enter the password assigned to management privilege levels on the device in the **Product Enable Account - Password** field.
6. Click **OK** on the **CLI Template** dialog box

Importing parameter values into a configuration

You can define the parameter values in a comma-separated value file (CSV) and then import them into the CLI template. The CSV file can include a description of the CLI template. The description must start with a pound sign (#) and cannot be longer than 512 characters.

The first line after the description defines the header for the import. The first entry in the header must be “Target”, then list all parameters (defined on the **CLI Commands** tab) to be included in the import.

The target can be an IP address (IPv4 or IPv6 format), the product group name (such as San Jose products), or All (all products). The parameters can be included in any order. The application ignores empty rows or columns during import.

NOTE
All values are case sensitive (including the “Target” header).

For example, if you define the following commands on the **CLI Commands** tab, Table 80 shows the CSV file content required for using different values for each target and Table 81 shows the CSV file content required for using the same values for each target

```
! Required for LSP egress address in LSP Manager as well as a soft interface for
IP routing
interface loopback  $<LOOPBACK_INTERFACE|INTEGER>
enable
ip ospf area  $<OSPF_AREA|INTEGER>
ip address   $<LOOPBACK_INTERFACE_IP|STRING>
```

TABLE 80 Different values for each target

#Description of the template. This template provides different values for each target..			
Target,	LOOPBACK_INTERFACE|INTEGER,	OSPF_AREA|INTEGER	LOOPBACK_INTERFACE_IP|STRING
10.20.30.100,	1,	4,	loopback1,
10.20.30.200,	2,	5,	loopback2,
Layer 2 Switch Products,	3,	6,	loopback3,

TABLE 81 Same value for each target

#Description of the template. This template provides different values for each target..			
Target,	LOOPBACK_INTERFACE|INTEGER,	OSPF_AREA|INTEGER	LOOPBACK_INTERFACE_IP|STRING
All,	1,	4,	loopback1,

To import parameter values, complete the following steps.

1. Click **Import** on the **Parameters** tab of the **CLI Template** dialog box.

   The **Open** dialog box displays.

2. Browse to the location of the parameters (CSV) file.
3. Click **Open**.

   The parameters specified in the CSV file display in the **Parameters** table. Note that the **Target** column remains visible at all times in the **Parameters** table.

   You can copy and paste new values for the parameter from an external file (plain text or table format). If the file you copy from is in table format, you can copy multiple fields (cells) at the same time.

Previewing CLI commands

1. Select a row in the **Parameters** table.
2. Click **Preview**.

   The **Preview of CLI Commands with Parameter Values** dialog box displays.

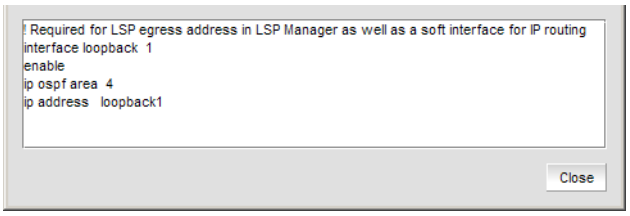


FIGURE 307 Preview of CLI Commands with Parameter Values dialog box

3. Click **Close**.

CLI command guidelines

When adding CLI commands to the configuration, use the following guidelines:

- Only configuration templates can be added to a template defined in the **CLI Template** dialog box.
- Templates can be nested and the same template can be included several times as long as it does not cause a circular dependency.
- Targets for deployment are only retrieved from the template you create, not any included templates.
- Only configuration- level commands, those that you enter when you are in the configure terminal mode, can be included in a device configuration. For example, you can enter the **snmp-server contact Administrator** command, but you cannot enter a **show run** command.
- Before you execute the **reload** or **copy tftp** commands, you must execute the **exit** command to exit the config terminal.
- Do not enter a **configure terminal** command. The Management application automatically assumes the commands you enter are under the configuration level.
- Add a space or a tab at the beginning of a command that is sublevel to the configuration command. For example, to enter the command for an interface in the device CLI, enter the following commands:

```
interface e 2/8
    port-name Interleaf
```

- To save the configuration to the device running configuration, either end the configuration with the **write memory** command or deploy the definition using the CLI configuration payload in the Configuration Wizard.

Copying a product configuration

To copy an existing configuration to create a new one, complete the following steps.

1. Select **Configure > CLI Configuration**.

   The **CLI Configuration** dialog box displays.

2. Click the **Configuration** tab.
3. Select the configuration you want to copy in the **Configuration** table and click **Duplicate**.

   The **CLI Configuration Template** dialog box displays.

4. Complete step 3 through step 4 from the "Creating a new product configuration" on page 779.
5. Review your entries on all the template tabs and choose one of the following options:
   - Click **OK** to save the configuration and add it to the list of configurations on the **Configuration** tab. The new definition can be added to a configuration payload in the Configuration Wizard and deployed later.

     To test the configuration, refer to "Testing a configuration" on page 789.

- Click **Deploy** to deploy the configuration to the selected targets. Click **Yes** on the confirmation message.

  If you selected the **Prompt for additional targets during manual deployment** check box, the **Target** tab of the **Deployment of** *Configuration_Name* dialog box displays. Continue with step 6.

  If the configuration contains parameters that must be defined, the **Deployment of** *Configuration_Name* dialog box displays with a list of all parameters in the deployment. Go to step 7.

6. Define additional targets for the deployment (refer to step 4), as needed.
7. Edit the mode and the parameter values (refer to step 6), as needed.
8. Click **OK**.

   The **Deployment Status** dialog box displays, which allows you to view the progress and status of the deployment.

   Click **Abort** to stop the deployment.

   NOTE
   The abort action does not stop the tasks that have already started.

   When deployment is complete, click **Report** to view the **CLI Deployments Report**.
9. Click **Close** to close the **Deployment Status** dialog box.

   NOTE
   Closing the **Deployment Status** dialog box does not stop deployment.

   To check the results of the deployment in the Product CLI Report, refer to "CLI deployment reports" on page 802. For details about valid and invalid responses when you deploy a configuration, refer to "Valid and invalid responses from devices" on page 790.

Editing a product configuration

To make changes to an existing configuration, complete the following steps.

1. Select **Configure > CLI Configuration**.

   The **CLI Configuration** dialog box displays.
2. Click the **Configuration** tab.
3. Select the configuration you want to edit in the **Configuration** table and click **Edit**.

   The **CLI Configuration Template** dialog box displays.
4. Complete step 3 through step 4 from the "Creating a new product configuration" on page 779.
5. Review your entries on all the template tabs and choose one of the following options:

   - Click **OK** to save the configuration and add it to the list of configurations on the **Configuration** tab. The new definition can be added to a configuration payload in the Configuration Wizard and deployed later.

     To test the configuration, refer to "Testing a configuration" on page 789.

- Click **Deploy** to deploy the configuration to the selected targets. Click **Yes** on the confirmation message.

  If you selected the **Prompt for additional targets during manual deployment** check box, the **Target** tab of the **Deployment of** *Configuration_Name* dialog box displays. Continue with step 6.

  If the configuration contains parameters that must be defined, the **Deployment of** *Configuration_Name* dialog box displays with a list of all parameters in the deployment. Go to step 7.

6. Define additional targets for the deployment (refer to step 4), as needed.
7. Edit the mode and the parameter values (refer to step 6), as needed.
8. Click **OK**.

   The **Deployment Status** dialog box displays, which allows you to view the progress and status of the deployment.

   Click **Abort** to stop the deployment.

   NOTE
   The abort action does not stop the tasks that have already started.

   When deployment is complete, click **Report** to view the **CLI Deployments Report**.
9. Click **Close** to close the **Deployment Status** dialog box.

   NOTE
   Closing the **Deployment Status** dialog box does not stop deployment.

   To check the results of the deployment in the Product CLI Report, refer to "CLI deployment reports" on page 802. For details about valid and invalid responses when you deploy a configuration, refer to "Valid and invalid responses from devices" on page 790.

Testing a configuration

To test a configuration, complete the following steps.

1. Select **Configure > CLI Configuration**.

   The **CLI Configuration** dialog box displays.
2. Select the configuration you want to verify in the **Templates** table and click **Verify**.
3. Click **Yes** on the "Do you want to verify?" message to confirm.

   If you selected the **Prompt for additional targets during manual deployment** check box, the **Target** tab of the **Deployment of** *Configuration_Name* dialog box displays. Continue with step 4.

   If the configuration contains parameters that must be defined, the **Deployment of** *Configuration_Name* dialog box displays with a list of all parameters in the deployment. Go to step 5.
4. Define additional targets for the deployment (refer to step 4), as needed.

5. Edit the mode and the parameter values (refer to step 6), as needed.

   The **Deployment Status** dialog box displays detailing whether the configuration will deploy successfully.

6. Click **Close** to close the **Deployment Status** dialog box.

Valid and invalid responses from devices

When you deploy a configuration to a device, some commands may send responses back to the Management application. By default, any message that the Management application receives is treated as an error, unless it matches an entry in the cliResponses.properties (IronWare) or NOSCliResponse.properties (Network OS) file. These files contain a list of messages that the Management application recognizes as valid responses.

If you think the response is valid, you can add the response to the list in the cliResponses.properties (IronWare) or NOSCliResponse.properties (Network OS) file using one of the following methods:

- Add the response to the cliResponses.properties (IronWare) file (refer to "Editing the CLI responses properties file" on page 790)
- Add the response to the NOSCliResponse.properties (Network OS) file (refer to "Editing the Network OS CLI responses properties file" on page 791)
- Add the response to the MotorolaControllerCliResponse.properties file (refer to "Editing the Network OS CLI responses properties file" on page 791)
- Using a dash character in CLI configuration manager (refer to "Using a dash character in CLI Configuration manager" on page 793)

Editing the CLI responses properties file

The cliResponses.properties (IronWare) file is under the *Install_Home*\conf\cli directory. Edit the file using a text editor. Add the response using the following Unicode regular expressions format.

For example, if you try to delete a nonexistent TACACS server by entering the following entry in CLI Configuration Manager:

```
no tacacs-server host 1.5.8.3
```

When you deploy the configuration, the following error messages are generated:

```
error: Failed to delete TACACS+ server 1.5.8.3
Error: Failed to delete TACACS+ server 1.5.8.3
```

To classify these messages as valid responses in the Management application, you can add the following entry to the appropriate responses file:

```
^no tac=^error: failed to delete
```

The strings on the left and the right side of the equal sign are Unicode regular expressions used for pattern matching. The expression on the left is matched against the command string, while the expression on the right is matched against the messages returned by the command that matches the pattern on the left. The entry in the example indicates that for any command that begins with "no tac", any messages that are returned beginning with "error: failed to delete" are valid responses. (Note that the matching is done in a case-insensitive manner, so you do not need to explicitly specify "error" and "Error" to match the messages shown in the example.) For details on the supported Unicode regular expression syntax, refer to "Regular Expressions" on page 1333.

The new response is available to the Management application as soon as you save the file; you do not need to restart the Management application.

Editing the Network OS CLI responses properties file

The NOSCliResponse.properties (Network OS) file is under the *Install_Home*\conf\cli directory. Edit the file using a text editor.

You can add a success response between the SUCCESS_RESPONSE_START and SUCCESS_RESPONSE_END tags using the following Unicode regular expressions format.

```
#Success Map
SUCCESS_RESPONSE_START
^su[port]*\s+s[witchd]*\s+=.*First Failure Data Capture.*enabled.*
^n[o]\s+su[port]*\s+s[witchd]*\s+=.*First Failure Data Capture.*disabled.*
^f[fdc]*=.*First Failure Data Capture.*enabled.*
^n[o]\sf[fdc]*=.*First Failure Data Capture.*disabled.*
SUCCESS_RESPONSE_END
```

You can add a failure response between the FAILURE_RESPONSE_START and FAILURE_RESPONSE_END tags using the following Unicode regular expressions format.

```
#Failure Map
FAILURE_RESPONSE_START
^nt[p]*\s+s[erv]*\s+=.*too many.*
^sn[mp\-serv]*\s+h[ost]*\s+=.*Maximum number of hosts in this version group
reached.*
^sn[mp\-serv]*\s+u[ser]*\s+=.*Maximum limit of users in this access group
reached.*no
^sn[mp\-serv]*\s+=.*too many.*
FAILURE_RESPONSE_END
```

The strings on the left and the right side of the equal sign are Unicode regular expressions used for pattern matching. The expression on the left is matched against the command string, while the expression on the right is matched against the messages returned by the command that matches the pattern on the left. For details on the supported Unicode regular expression syntax, refer to "Regular Expressions" on page 1333.

The new response is available to the Management application as soon as you save the file; you do not need to restart the Management application.

Editing the Motorola Controller CLI responses properties file

The MotorolaControllerCliResponse.properties file is under the *Install_Home*\conf\cli directory. Edit the file using a text editor.

You can add a success response between the SUCCESS_RESPONSE_START and SUCCESS_RESPONSE_END tags using the following Unicode regular expressions format.

```
#Success Map
SUCCESS_RESPONSE_START
^su[port]*\s+s[witchd]*\s+=.*First Failure Data Capture.*enabled.*
^n[o]\s+su[port]*\s+s[witchd]*\s+=.*First Failure Data Capture.*disabled.*
^f[fdc]*=.*First Failure Data Capture.*enabled.*
^n[o]\sf[fdc]*=.*First Failure Data Capture.*disabled.*
SUCCESS_RESPONSE_END
```

You can add a failure response between the FAILURE_RESPONSE_START and FAILURE_RESPONSE_END tags using the following Unicode regular expressions format.

```
#Failure Map
FAILURE_RESPONSE_START
^nt[p]*\s+s[erv]*\s+=.*too many.*
^sn[mp\-serv]*\s+h[ost]*\s+=.*Maximum number of hosts in this version group
reached.*
^sn[mp\-serv]*\s+u[ser]*\s+=.*Maximum limit of users in this access group
reached.*no
^sn[mp\-serv]*\s+=.*too many.*
FAILURE_RESPONSE_END
```

The strings on the left and the right side of the equal sign are Unicode regular expressions used for pattern matching. The expression on the left is matched against the command string, while the expression on the right is matched against the messages returned by the command that matches the pattern on the left. For details on the supported Unicode regular expression syntax, refer to "Regular Expressions" on page 1333.

The new response is available to the Management application as soon as you save the file; you do not need to restart the Management application.

Configuration command response validation

Command responses are only validated for configuration deployments. Validation occurs in the following order:

1. Failure Map — Checks the response message against the regex defined in the failure map. If a match is found, it is treated as failure response from the device and stops the validation process.
2. Success Map — Checks the response message against the regex defined in the success map. If a match is found, it is treated as a success response from the device and stops the validation process.
3. General Failure Strings — Checks the response message against the general failure strings. If a match is found, it is treated as a failure response from the device and stops the validation process.

NOTE
If the response message does not fall in any of the categories above, it is treated as a success response from the device and stops the validation process.

Using a dash character in CLI Configuration manager

You can override how the Management application treats messages without editing the CLI responses properties file. To do this, enter a dash (-) at the beginning of each configuration line. For example, to create a configuration that defines an IP address for port 3/2, enter the following commands in the CLI Configuration Manager:

```
-interface ethernet 3/2
- ip address 192.45.6.110 255.255.255.0
```

NOTE
Make sure there is no space between the dash and the first character of a command entered at the configuration level. When entering a sublevel command, you must use a space or a tab between the dash and the first character of the command.

Using the dash tells the Management application to ignore any response, even if the response is not in the cliResponses.properties file.

Configuration error checking

To prevent invalid commands from being entered in a configuration definition, the cliShowCommands.properties file under the *Install_Home*\conf\cli\ directory specifies what commands cannot be included in a configuration definition. The command lists the following:

- An entry in a command=disallowed format indicates a command that must not be entered in the **CLI Command** tab.

  For example, you see the ping=disallowed entry. Ping cannot be included in a configuration or monitoring definition.

- A command that does not have "disallowed" can only be used under the monitoring. For example, by default, the **sh** (show) command is included in the cliShowCommands.properties file. This means that the **sh** command can be entered only under monitoring. For more information on monitoring, refer to "Monitoring configurations" on page 795.

  You can add commands to the lists in the cliShowCommands.properties file. However, any commands you add to that file are commands that are treated as display commands only or are commands that cannot be used in a definition if they are listed with the "=disallowed" expression.

Deleting a configuration

To delete a configuration, complete the following steps.

1. Select **Configure > CLI Configuration**.

   The **CLI Configuration** dialog box displays.

2. Select one or more configurations to delete in the **Templates** table and click **Delete**.
3. Click **Yes** on the "Do you want to delete?" message to confirm.
4. Click **Close** to close the **CLI Configuration** dialog box.

CLI configuration deployment

Deploy the configuration using one of the following methods:

- At a scheduled date and time

  Schedule a configuration deployment in the **CLI Template** dialog box. For step-by-step instructions, refer to "Creating a new product configuration" on page 779 or "Creating a monitoring configuration" on page 795.

- On demand

  To deploy an existing configuration on demand, refer to "Deploying a configuration on demand" on page 794.

Deploying a configuration on demand

If you are using the on demand method, the configuration is saved to the device running configuration. If you want to save it to the device startup configuration, make sure the **write memory** command is the last command in the configuration or deploy the configuration using the Configuration Wizard. Once you deploy a device configuration definition, a Deployment Report and a Product CLI Report are generated.

To deploy a configuration on demand, complete the following steps.

1. From the **Configuration** tab of the **CLI Configuration** dialog box, select the configuration you want to deploy and click **Deploy**.
2. Click **Yes** on the "Do you want to deploy the configuration *Configuration_Name*?" message to confirm.

   If the configuration contains parameters that must be defined, the **Deployment of** *Configuration_Name* dialog box displays with a list of all parameters in the deployment.
3. Edit the mode and the parameter values (refer to step 6), as needed.
4. Click **OK**.

   The **Deployment Status** dialog box displays, which allows you to view the progress and status of the deployment.

   Click **Abort** to stop the deployment.

   NOTE
   The abort action does not stop the tasks that have already started.

   When deployment is complete, click **Report** to view the **CLI Deployments Report**.
5. Click **Close** to close the **Deployment Status** dialog box.

NOTE
Closing the **Deployment Status** dialog box does not stop deployment.

To check the results of the deployment in the Product CLI Report, refer to "CLI deployment reports" on page 802. For details about valid and invalid responses when you deploy a configuration, refer to "Valid and invalid responses from devices" on page 790.

Monitoring configurations

You can create, modify, duplicate, and delete a monitoring configuration from the **CLI Configuration** dialog box. Monitoring configurations allow you to create device reports by entering a set of show CLI commands. To view a list of existing configurations, refer to "Viewing existing templates" on page 778. For information about the example templates, refer to "CLI Templates" on page 1339.

Creating a monitoring configuration

To create a new monitoring configuration, complete the following steps.

1. Select **Configure > CLI Configuration**.

   The **CLI Configuration** dialog box displays.

2. Click **Add**.

   The **CLI Template** dialog box displays.

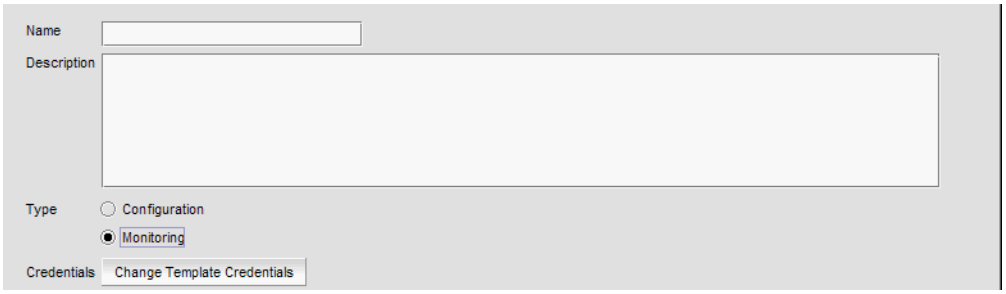


FIGURE 308 CLI Template dialog box - Definition tab

3. Click the **Definition** tab and complete the following steps.

   a. Enter a name and description for the new configuration.

NOTE
Do not use special characters in the name.

   b. Select **Monitoring** to create product reports using show commands.

   c. To change CLI credentials, click **Change Template Credentials** and refer to "Changing product credentials" on page 784.

4. Click the **Targets** tab and complete the following steps.

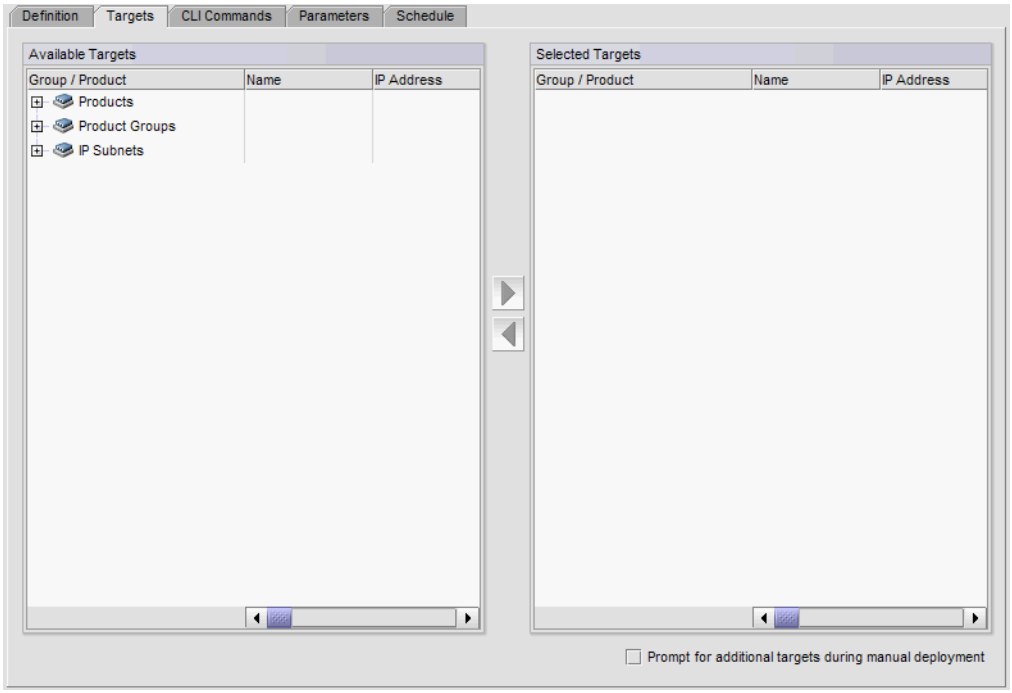


FIGURE 309 CLI Template dialog box - Target tab

a. Select the devices to which you want the configuration deployed from the **Available Targets** table.

   You can deploy the configuration to individual devices, devices in a device group, or devices in an IP subnet.

   For VCS fabrics, you can deploy the configuration to one or more individual members in a fabric (select each member) or to all members of a fabric (select the VCS fabric).

   The **Available Targets** table displays an inventory of the available product targets and includes the same detail as the Product List (refer to "IP Product List" on page 284).

b. Click the right arrow button to move your selection to the **Selected Targets** table.

   To search for devices, right-click anywhere in the table and select **Search**. For more information about searching for devices, refer to "Searching for a device" on page 299.

   The **Selected Targets** table displays the selected products and includes the same detail as the Product List (refer to "IP Product List" on page 284).

c. Select the **Prompt for additional targets during manual deployment** check box to be able to select additional targets during manual deployment.

5. Click the **CLI Command** tab and complete the following steps.

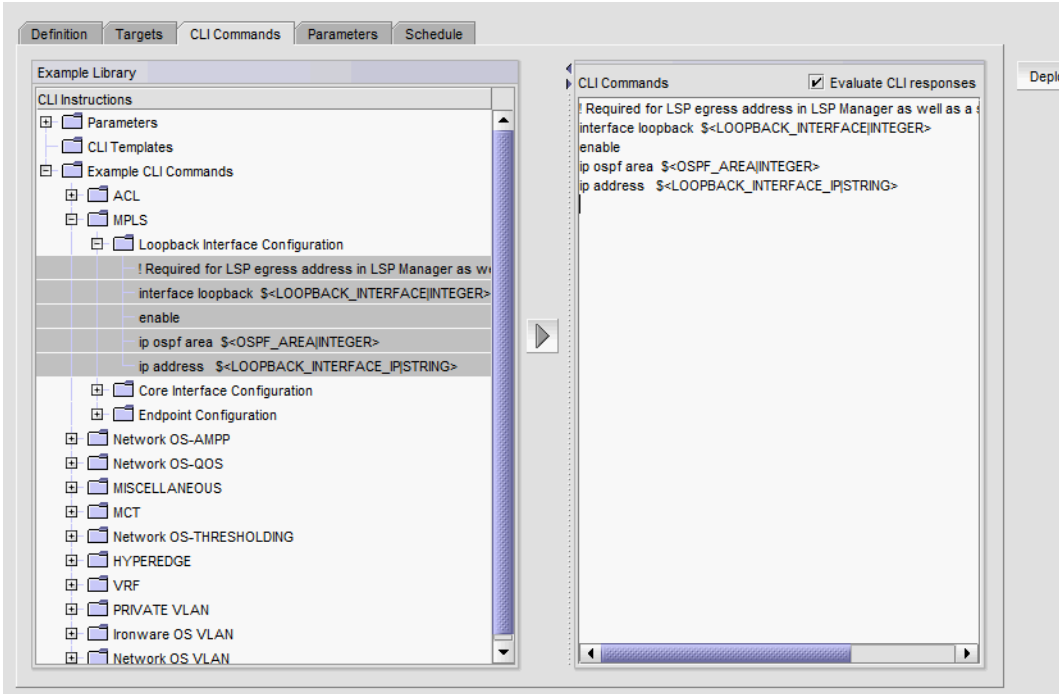


FIGURE 310 CLI Template dialog box - CLI Commands tab

d. Enter the show commands in the **CLI Commands** text area.

NOTE
Only commands listed in the cliShowCommands.properties file can be entered for a monitoring configuration. For more information, refer to "Configuration error checking" on page 793.

For a list of guidelines to use when entering CLI commands, refer to "CLI command guidelines" on page 787.

Add commands from the CLI templates or examples by selecting one or more commands from the **CLI Templates** or **Examples of CLI Commands** folder and clicking the right arrow button. For more information, refer to "CLI Templates" on page 1339.

e. To enter a parameter for a CLI command, select the parameter type from the **CLI Commands** list - **Parameters** folder and click the right arrow to move the parameter type to the **CLI Commands** text area.

Parameters use the following format: $<*name*|*data_type*>, where *name* is the parameter and *data_type* is the type of parameter.

Parameter types include integer ($<name|INTEGER>), string ($<name|STRING>), slot/port ($<name|SLOT_PORT>), MAC address ($<name|MAC>), and IP address ($<name|IP_ADDRESS>).

f. Edit the parameter by entering the variable or character string you want to use for the parameter in place of the *name* variable.

NOTE
Each parameter must be unique. The Management application does not check for duplicate parameters.

```
show interface ethernet $<port|SLOT_PORT:[Slot#]/Port#>
```

In the example, `show interface ethernet` is the CLI command, `port` is the parameter variable, `SLOT_PORT` is the parameter type, and `[Slot#]/Port#` is the format for the port number.

g. (Optional) Select a template from the **CLI Templates** folder and click the right arrow to include it in the configuration.

This allows you to deploy more than one template to a device in a single deployment. Only templates defined in the Management application display. This list only displays when there is at least one user-defined CLI template.

6. Click the **Parameters** tab and complete the following steps.

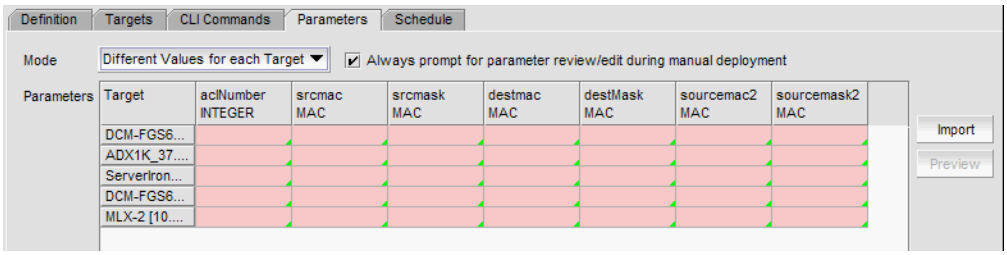


FIGURE 311 CLI Template dialog box - Parameters tab

a. Select the Always prompt for parameter review/edit during manual deployment check to display the **Parameter** tab in the **Prompt** dialog box during manual deployment.

Clear to not display the **Parameter** tab in the **Prompt** dialog box during manual deployment.

When selected, the **Parameter** tab displays in the **Prompt** dialog box during manual deployment even if you filled in all parameter values on the **Parameters** tab of the **CLI Template** dialog box.

b. Select one of the following options from the **Mode** list for the parameter import mode.

- **Same Values for each Target —** Select to set the same values for all selected targets.
- **Different Values for each Target** — Select to set individual values for the selected targets.

c. Enter a value for each parameter in the associated field.

Fields containing a green triangle ( ) in the lower right corner are editable. The fields only accepts valid values base on the parameter data type.

Parameters include the following options:

- String — Enter a string with a maximum of 64 ASCII characters.
- Integer — Enter an integer with a maximum of 12 numeric characters.
- Slot/Port — Enter the slot number and port number.
- MAC address — Enter hexadecimal characters with or without a valid delimiter (such as hyphen, colon, period, and space). Wildcards (such as ? and *) are supported.
- IP address — Enter an IPv4 or IPv6 address.

You can copy and paste new values for the parameter from an external file (plain text or table format). If the file you copy from is in table format, you can copy multiple fields (cells) at the same time.

To import parameter values from a CSV file, refer to "Importing parameter values into a configuration" on page 785.

7. Click the **Schedule** tab and complete the following steps.

a. Select the **Schedule** check box.

b. Choose one of the following options from the **Frequency** list.

- One Time (refer to "Configuring a one-time deployment schedule" on page 803)
- Hourly (refer to "Configuring an hourly deployment schedule" on page 803)
- Daily (refer to "Configuring a daily deployment schedule" on page 804)
- Weekly (refer to "Configuring a weekly deployment schedule" on page 804)
- Monthly (refer to "Configuring a monthly deployment schedule" on page 804)
- Yearly (refer to "Configuring a yearly deployment schedule" on page 805)

8. Review your entries on all the template tabs and choose one of the following options:

- Click **OK** to save the configuration and add it to the list of configurations on the **Monitoring** tab. The new definition can be added to a configuration payload in the Configuration Wizard and deployed later.

  To test the configuration, refer to "Testing a configuration" on page 789.

- Click **Deploy** to deploy the configuration to the selected targets. Click **Yes** on the confirmation message.

  If you selected the **Prompt for additional targets during manual deployment** check box, the **Target** tab of the **Deployment of** *Configuration_Name* dialog box displays. Continue with step 9.

  If the configuration contains parameters that must be defined, the **Deployment of** *Configuration_Name* dialog box displays with a list of all parameters in the deployment. Go to step 10.

9. Define additional targets for the deployment (refer to step 4), as needed.

10. Edit the mode and the parameter values (refer to step 6), as needed.

11. Click **OK**.

    The **Deployment Status** dialog box displays, which allows you to view the progress and status of the deployment.

    Click **Abort** to stop the deployment.

    NOTE
    The abort action does not stop the tasks that have already started.

    When deployment is complete, click **Report** to view the **CLI Deployments Report**.

12. Click **Close** to close the **Deployment Status** dialog box.

    NOTE
    Closing the **Deployment Status** dialog box does not stop deployment.

    To check the results of the deployment in the Product CLI Report, refer to "CLI deployment reports" on page 802. For details about valid and invalid responses when you deploy a configuration, refer to "Valid and invalid responses from devices" on page 790.

Copying a monitoring configuration

To copy an existing monitoring configuration to create a new one, complete the following steps.

1. Select **Configure > CLI Configuration**.

   The **CLI Configuration** dialog box displays.

2. Click the **Monitoring** tab.

3. Select the configuration you want to copy in the **Monitoring** table and click **Duplicate**.

   The **CLI Monitoring Template** dialog box displays.

4. Complete step 3 through step 4 from the "Creating a new product configuration" on page 779.

5. Review your entries on all the template tabs and choose one of the following options:

   - Click **OK** to save the configuration and add it to the list of configurations on the **Monitoring** tab. The new definition can be added to a configuration payload in the Configuration Wizard and deployed later.

     To test the configuration, refer to "Testing a configuration" on page 789.

   - Click **Deploy** to deploy the configuration to the selected targets. Click **Yes** on the confirmation message.

     If you selected the **Prompt for additional targets during manual deployment** check box, the **Target** tab of the **Deployment of** *Configuration_Name* dialog box displays. Continue with step 6.

     If the configuration contains parameters that must be defined, the **Deployment of** *Configuration_Name* dialog box displays with a list of all parameters in the deployment. Go to step 7.

6. Define additional targets for the deployment (refer to step 4), as needed.

7. Edit the mode and the parameter values (refer to step 6), as needed.

8. Click **OK**.

   The **Deployment Status** dialog box displays, which allows you to view the progress and status of the deployment.

   Click **Abort** to stop the deployment.

   NOTE
   The abort action does not stop the tasks that have already started.

   When deployment is complete, click **Report** to view the **CLI Deployments Report**.

9. Click **Close** to close the **Deployment Status** dialog box.

   NOTE
   Closing the **Deployment Status** dialog box does not stop deployment.

   To check the results of the deployment in the Product CLI Report, refer to "CLI deployment reports" on page 802. For details about valid and invalid responses when you deploy a configuration, refer to "Valid and invalid responses from devices" on page 790.

Editing a monitoring configuration

To make changes to any of the existing configuration, complete the following steps.

1. Select **Configure > CLI Configuration**.

   The **CLI Configuration** dialog box displays.

2. Click the **Monitoring** tab.

3. Select the configuration you want to edit in the **Monitoring** table and click **Edit**.

   The **CLI Monitoring Template** dialog box displays.

4. Complete step 3 through step 4 from the "Creating a new product configuration" on page 779.

5. Review your entries on all the template tabs and choose one of the following options:

   - Click **OK** to save the configuration and add it to the list of configurations on the **Monitoring** tab. The new definition can be added to a configuration payload in the Configuration Wizard and deployed later.

     To test the configuration, refer to "Testing a configuration" on page 789.

   - Click **Deploy** to deploy the configuration to the selected targets. Click **Yes** on the confirmation message.

     If you selected the **Prompt for additional targets during manual deployment** check box, the **Target** tab of the **Deployment of** *Configuration_Name* dialog box displays. Continue with step 6.

     If the configuration contains parameters that must be defined, the **Deployment of** *Configuration_Name* dialog box displays with a list of all parameters in the deployment. Go to step 7.

6. Define additional targets for the deployment (refer to step 4), as needed.

7. Edit the mode and the parameter values (refer to step 6), as needed.

8. Click **OK**.

   The **Deployment Status** dialog box displays, which allows you to view the progress and status of the deployment.

   Click **Abort** to stop the deployment.

   NOTE
   The abort action does not stop the tasks that have already started.

   When deployment is complete, click **Report** to view the **CLI Deployments Report**.

9. Click **Close** to close the **Deployment Status** dialog box.

   NOTE
   Closing the **Deployment Status** dialog box does not stop deployment.

   To check the results of the deployment in the Product CLI Report, refer to "CLI deployment reports" on page 802. For details about valid and invalid responses when you deploy a configuration, refer to "Valid and invalid responses from devices" on page 790.

CLI deployment reports

The CLI Deployments Report contains the reports generated when testing or deploying product configuration and monitoring definitions from the **CLI Configuration** dialog box to IronWare and Network OS devices. It is not available for third-party devices or non-IP devices.

If you are assigned to an area of responsibility (AOR), you can view only the CLI Deployments Report for the configurations that you deploy from the **CLI Configuration** dialog box.

Viewing CLI deployment reports

NOTE
You can launch the CLI Deployments Report directly from the **Deployment Status** dialog box by clicking **Report**. For information about deploying a configuration, refer to "CLI configuration deployment" on page 794

To view a CLI deployment report for a product from the main window, complete the following steps.

1. Select **Reports > Product CLI**.

   The **CLI Deployments Report** displays listing the reports that have been generated.

   To sort the list by a single column, click the column header.

   To reverse the sort order, click the column header again.

2. Click the name of the report you want to view.

   You can expand an entry to show the list of devices for which the report was generated and whether or not the report was successfully generated. If the report was not generated, error messages appear under the **Error** column.

3. Choose one of the following options:
   - To display a report for one device, click the IP address of the device on the list.
   - To display a report that includes all devices for which the report was generated, click the name of the report in the **Template Name** column.

   The **Product CLI Report** displays.

   To export a report refer to "Exporting and saving IP reports to a file" on page 1232.

CLI configuration scheduling

You can configure when and how often to run each configured CLI template. Options include:

- One Time (refer to "Configuring a one-time deployment schedule" on page 803)
- Hourly (refer to "Configuring an hourly deployment schedule" on page 803)
- Daily (refer to "Configuring a daily deployment schedule" on page 804)
- Weekly (refer to "Configuring a weekly deployment schedule" on page 804)
- Monthly (refer to "Configuring a monthly deployment schedule" on page 804)
- Yearly (refer to "Configuring a yearly deployment schedule" on page 805)

Configuring a one-time deployment schedule

To configure a one-time schedule, complete the following steps.

1. Select **One Time** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
3. Click the **Date** list to select a date from the calendar.

   To finish configuring the CLI template, return to step 8 of "Creating a new product configuration" on page 779.

Configuring an hourly deployment schedule

To configure an hourly schedule, complete the following steps.

1. Select **Hourly** from the **Frequency** list.
2. Select the minute past the hour you want deployment to run from the **Minutes past the hour** list.

   Where the minute value is from 00 through 59.

   To finish configuring the deployment schedule, return to step 8 of "Creating a new product configuration" on page 779.

Configuring a daily deployment schedule

To configure a daily deployment schedule, complete the following steps.

1. Select **Daily** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

   To finish configuring the deployment schedule, return to step 8 of "Creating a new product configuration" on page 779.

Configuring a weekly deployment schedule

To configure a weekly schedule, complete the following steps.

1. Select **Weekly** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Select the day you want deployment to run from the **Day of the Week** list.

   To finish configuring the deployment schedule, return to step 8 of "Creating a new product configuration" on page 779.

Configuring a monthly deployment schedule

To configure a monthly schedule, complete the following steps.

1. Select **Monthly** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Select the day you want deployment to run from the **Day of the Month** list (1 through 31).

   To finish configuring the deployment schedule, return to step 8 of "Creating a new product configuration" on page 779.

Configuring a yearly deployment schedule

To configure a yearly schedule, complete the following steps.

1. Select **Yearly** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
3. Click the **Date** list to select a date from the calendar.

   To finish configuring the deployment schedule, return to step 8 of "Creating a new product configuration" on page 779.

Chapter

26

Image Repository for IP Products

In this chapter

Obtaining software files

Program files required to run IronWare OS IP products can include boot, monitor, software, and unified management programs, depending on the product. These program files are imported into the Management application manually from the Firmware Management repository.

NOTE
Importing images requires users to have the Firmware Management privilege.

Multiple versions of files may be stored for a product. A stored image can be deployed to appropriate products managed by the Management application.

You can obtain copies of software files by downloading them from the Knowledge Portal (kp.brocade.com). Updates are available to customers that have current technical support maintenance contracts. For more information, contact your service representative.

Copy the software files to a directory that is accessible from the Management application server. The following sections discuss how to import images into the Management application:

- "Boot image management" on page 808
- "Software image management" on page 811
- "Unified image management" on page 814

Refer to the release notes for a specific software version to determine which files are required for the software version.

Products supporting the image import

Table 82 lists the products that support the boot images, software images, and unified images.

TABLE 82 Products supporting the image import

Image type	Products supported
Boot images	• Ethernet chassis (BigIron RX) • Ethernet routers (NetIron XMR, MLX, CES 00, CER) • Terathon (BigIron MG8, NetIron 40G, NetIron IMR 640) • Ethernet switches (FastIron Switches) and Data Center switch (TurboIron 24X) • ServerIron, ServerIron ADX • IP Encryption switch (SecureIron) • IronPoint FES
Software images	• Ethernet chassis (BigIron RX) • Ethernet routers (NetIron XMR, MLX, CES 00, CER) • Terathon (BigIron MG8, NetIron 40G, NetIron IMR 640) • ServerIron, ServerIron ADX • IP Encryption switch (SecureIron) • Ethernet switches (FastIron Switches) and Data Center switch (TurboIron 24X) • EdgeIron 4802CF, 48G, 48GS, and 8x 10G • IronPoint FES
Unified images	• Ethernet chassis (BigIron RX) (release 02.2.01) • Ethernet routers (NetIron XMR, MLX, CES 00, CER) (Ethernet Edge router (CER) release 03.5.00-application images only) • Terathon (BigIron MG8, NetIron 40G, NetIron IMR 640), (release 02.3.00) • VDX switches (release 2.1.0 and later) • NetIron Simplified XMR/MLX and CES/CER (release 5.3.0 and later)

Boot image management

Management of boot and monitor images from IronWare and Network OS products can be done using the following Management application modules:

- Firmware Management — Manually imports boot images into the Management application. This module also allows you to delete boot images from the Management application.
- Configuration Wizard — Deploys boot and monitor images that are available in the Management application to IronWare and Network OS products. The Configuration Management privilege is required to deploy boot and monitor images using the Configuration Wizard.

Viewing the list of boot images

You can view a list of boot and monitor images that are known to the Management application from the **Boot Images** tab of the **Firmware Management** dialog box if you have the Firmware Management privilege in your Management application user account or role.

The **Boot Images** tab lists the boot or monitor images in the Management application and contains the following buttons:

- **Import** — Opens the **Import Boot Image** dialog box that allows you to browse and select the boot or monitor image file you want to import into the Management application. Newly imported images are saved to the Management application. They are displayed on the **Boot Images** tab.
- **Delete** — Deletes the boot or monitor image from the Management application.
- **Help** — Provides information about the feature.

NOTE
The image features discussed in this section are available only to the products listed in "Products supporting the image import" on page 808.

Manually importing boot images

The **Import Boot Image** dialog box allows you to browse and select an image file and add it to the **Boot Images** list.

NOTE
You must select the **AllowManualImports** option in the **Options** dialog box — **IP Preferences** pane to display the **Import Boot Image** dialog box. If this option is not selected, the following error message displays: "The specified file is not a valid image file."

To import boot images into the Management application, perform the following tasks.

1. Obtain the boot and monitor images you need. Refer to "Obtaining software files" on page 807.
2. Click the **IP** tab.
3. Select **Configure > Firmware Management**.
4. From the **Firmware Management** dialog box, click the **Boot Images** tab.
5. Click **Import**.
6. In the **Import Boot Image** dialog box, enter the name of the image file you want to import. You can also click the **Browse** button to search for the file you want.
7. Click **OK**.

   After the import completes successfully, you see a message that the boot image imported successfully. The Boot Image table lists the image version and the image label.

   If the import fails because of missing or invalid information in the image header, one of the following displays:

   - If the **AllowManualImports** check box is not selected on the **Options** dialog box - **IP Preferences** pane (refer to "Configuring image repository preferences" on page 162), the following error message displays: "The specified file is not a valid image file." Click **Yes** to close the message.
   - If the **AllowManualImports** check box is selected on the **Options** dialog box - **IP Preferences** pane, the **Import Boot Image** dialog box displays. Continue to import the image by completing the following steps.

     a. Select the software type from the **Software Type** list.

     b. Select the hardware from the **Hardware Type** list (the hardware product where the image can be deployed).

c. Enter the image version in the **Image Version** field.

d. Enter the label for the image in the either the **Image Label** field or the **User Defined Label** field.

These fields are from 1 through 32 alphanumeric characters and allow the following special characters: underscore (_), period (.), and hyphen (-).

The image file name excludes the file extension. For example, if the file name is M2B07504.bin, the Image Label is M2B07504.

Enter additional information for the image in the **User Defined Label** field. This entry appears under the **More Information** column of the **Boot Images** list of the **Firmware Management** dialog box.

e. Click **OK** on the **Import Boot Image** dialog box.

If the imported file already exists or the import operation fails for any reason, a message displays with details.

8. Click **OK**.

Deploying boot images to products

The Management application stores previously imported boot and monitor images from IronWare and Network OS products. These images can be placed in a boot image payload and deployed to products using the Configuration Wizard.

Deleting boot images from the Management application

If a boot or monitor image must be deleted from the Management application, complete the following steps.

1. Click the **IP** tab.
2. Click the **Boot Images** tab on the **Firmware Management** dialog box.
3. Select the boot image that you want to delete.
4. Click **Delete**.

   A confirmation warning displays.
5. Click **Yes** to continue with the delete, or **No** to cancel it.

Software image management

Software images are program files other than boot, monitor, or unified images. You can manage software images using the following Management application modules:

- Discovery — Copies software images from IronWare and Network OS products on the network into the Management application.
- Backup Scheduler — Copies software images from IronWare and Network OS products on a regularly scheduled basis.
- Firmware Management — Manually imports software images into the Management application. This module also allows you to delete software images from the Management application.
- Configuration Wizard — Deploys software images that are available in the Management application to IronWare and Network OS products.

Viewing the list of software images

To view the list of software images, select the **Software Images** tab on the **Firmware Management** dialog box.

NOTE
You can view a list of software images that are known to the Management application from the **Software Images** tab of the **Firmware Management** dialog box if you have the Firmware Management privilege in your Management application user account or role.

For HyperEdge stacks, only the Master (ICX 6610) displays in the software images list.

The **Software Images** tab lists the software images in the Management application and contains the following buttons:

- **Import —** Opens a dialog box that allows you to browse and select the software image file you want to import and save in the Management application.
- **Delete** — Deletes the software image from the Management application.
- **Help** — Provides information about the feature.

Manually importing software images

To manually import software images into the Management application, perform the following tasks.

1. Click the **IP** tab.
2. Select **Configure > Firmware Management**.
3. From the **Firmware Management** dialog box, click the **Software Images** tab.
4. Click **Import**.
5. In the **Import Software Image** dialog box, enter the name of the image file you want to import. You can also click the **Browse** button to search for the file you want.
6. Click **OK**.

   After the import completes successfully, you see a message that the software image imported successfully. The **Software Image** table lists the image version and the image label.

If the import fails because of missing or invalid information in the image header, one of the following displays:

- If the **AllowManualImports** check box is not selected on the **Options** dialog box - **IP Preferences** pane (refer to "Configuring image repository preferences" on page 162), the following error message displays: "The specified file is not a valid image file." Click **Yes** to close the message.
- If the **AllowManualImports** check box is selected on the **Options** dialog box - **IP Preferences** pane, the **Import Software Image** dialog box displays. Continue to import the image by completing the following steps.

  a. Select the software type from the **Software Type** list.

  b. Select the hardware from the **Hardware Type** list.

  c. Enter the image version in the **Image Version** field.

  d. Enter the label for the image in the either the **Image Label** field or the **User Defined Label** field.

     These fields are from 1 through 32 alphanumeric characters and allow the following special characters: underscore (_), period (.), and hyphen (-).

  e. Click **OK** on the **Import Software Image** dialog box.

     If the imported file already exists or the import operation fails for any reason, a message displays with details.

Automatically retrieving software images from products

The Backup Scheduler of the Management application checks the products under the Management application at regular intervals to determine if they have new software images. New images are copied (backed up) to the Management application.

The Backup Scheduler contains two types of scheduled backups: automatic configuration backup and automatic software image backup. This section presents the procedure for automatic software image backup. Refer to "Scheduling a configuration backup" on page 762 for the automatic configuration backup procedure.

Make sure that the Management application is running; otherwise, scheduled tasks will not run.

NOTE
By default, the Backup Scheduler backs up software images once a day, at 2:00 am.

You can change the default schedule from the Backup Scheduler by performing the following tasks.

1. Click the **IP** tab.
2. From the Management application menu bar, select **Configure > Configuration > Schedule Backup**.

   or

   Right-click **Configuration > Schedule Backup**.

   The **Schedule Backup** dialog box displays, as shown in Figure 312.

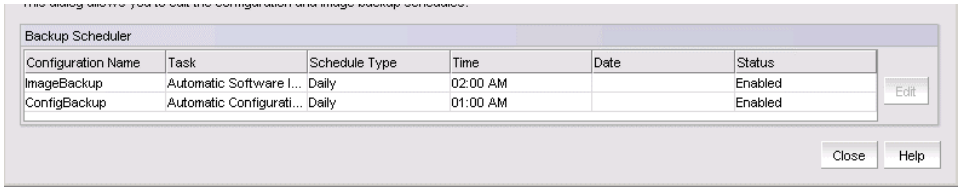


FIGURE 312 Schedule Backup dialog box

3. Select the automatic software image backup task from the list, and click **Edit**.

   The **Edit Automatic Software Image Backup** dialog box displays, as shown in Figure 313.

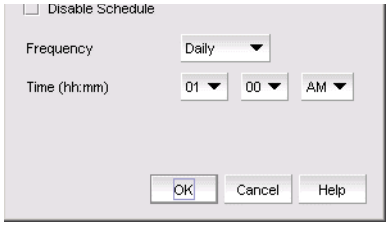


FIGURE 313 Edit Automatic Software Image Backup dialog box

4. Disable the scheduled backup or modify the frequency and time.

   Refer to "Scheduling a configuration backup" on page 762 for information about how to schedule a configuration backup.

5. Click **OK**.

Deploying software images to products

The Management application stores previously imported software images. These software images can be placed in a software image payload and deployed to products using the Configuration Wizard.

For a HyperEdge stack, you must deploy the ICX 6610 and ICX 6450 software images to the active master unit separately. Make sure that both software images have the same software image version. When both software image upgrades are complete, reload the HyperEdge stack. The master unit upgrades the software images to the appropriate member units.

Deleting software images from the Management application

If a software image stored in the Management application must be deleted, perform the following steps.

1. Click the **Software Images** tab on the **Firmware Management** dialog box.
2. Select the software image that you want to delete.
3. Click the **Delete** button.

   A confirmation warning displays.
4. Click **Yes** to continue with the delete, or **No** to cancel it.

Unified image management

Unified images contain all images required to manage the product. Instead of upgrading each type of image separately, you can use a unified image to upgrade all image types. For example, a unified image for the BigIron RX Series contains boot, monitor, management, and interface images. When deployed, a unified image can update all image types on a product simultaneously.

Unified images are not available for all IronWare and Network OS products, but if your product has a unified image, you can manage that image from the **Unified Firmware Images** tab of the **Firmware Management** dialog box. Management of images can be done using the following Management application modules:

- Firmware Management — Manually imports unified images into the Management application. This module also allows you to delete unified images from the Management application. Alternatively, you can click the **Update** button to download unified firmware images to the device.
- Configuration Wizard — Deploys unified images that are available in the Management application to IronWare and Network OS products.

NOTE
Refer to the release notes for your IronWare and Network OS product to determine if unified images are available for the product.

Viewing the list of unified images

You can view a list of unified images that are known to the Management application from the **Unified Firmware Images** tab of the **Firmware Management** dialog box if you have the Firmware Management privilege in your Management application user account or role.

To view the list of unified images, select the **Unified Firmware Images** tab from the **Firmware Management** dialog box, as shown in Figure 314.

NOTE
For Network OS VDX switches, you can select either the logical chassis cluster or the fabric cluster nodes.

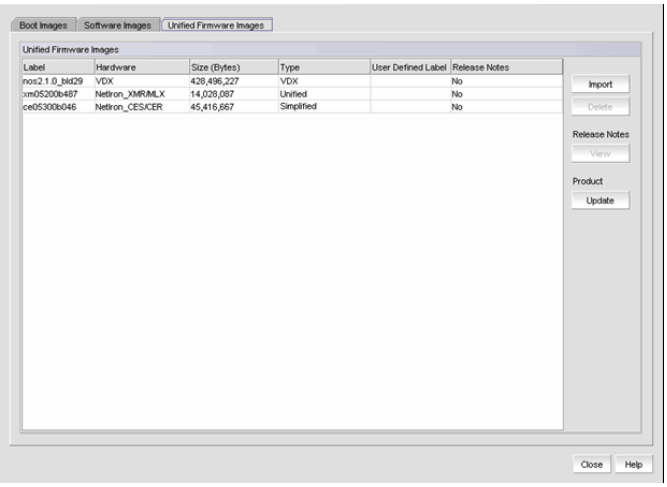


FIGURE 314 Firmware Management dialog box - Unified Firmware Images tab

The **Unified Firmware Images** tab contains the following buttons:

- **Import —** Opens a dialog box that allows you to browse and select the unified image file you want to import into the Management application. Newly imported images are saved to the Management application.
- **Delete** — Deletes the unified image from the Management application.
- **View** — Opens a dialog box that allows you to enter the location of the release notes or search for the location of the release notes.
- **Update** — Updates the firmware images by way of the Configuration Wizard.

Importing unified images into the Management application

The **Import Firmware Image from File** dialog box allows you to browse and select an image file and add it to the **Unified Firmware Images** tab.

NOTE
If the Management application does not recognize the image, you must enter the following information manually.

NOTE
Allowing for manual import is not supported for simplified NetIron and unified VDX images.

To import unified images into the Management application, perform the following tasks.

1. Obtain the unified image you need. Refer to "Obtaining software files" on page 807.
2. Click the **IP** tab.
3. Select **Configure > Firmware Management**.
4. From the **Firmware Management** dialog box, click the **Unified Firmware Images** tab.
5. Click **Import**.

   The **Import Firmware Image from File** dialog box displays.

NOTE
You must install the Management application on an external FTP server or SCP server to activate the **Import Firmware Image from File** dialog box.

6. In the **Import Firmware Image from File** field, enter the location of the unified image, or click **Browse** to search for an existing image file. The image file can be in one of the following formats: .tar, .gz, .zip, or .bin.
7. In the **Release Notes Location** field, enter the location of the release notes or click **Browse** to search for the location of the release notes. Release notes can be in one of the following formats: .pdf or .txt.

NOTE
Importing release notes is optional and only supported for simplified NetIron and VDX firmware images.

8. Click **OK**.

   After the import completes successfully, a message displays that the unified image imported successfully. The message also lists the image version and the image label.

   If the import fails because of missing or invalid information in the image header, one of the following displays:

   - If the **AllowManualImports** check box is not selected on the **Options** dialog box - **IP Preferences** pane (refer to "Configuring image repository preferences" on page 162), the following error message displays: "The specified file is not a valid image file." Click **Yes** to close the message.
   - If the **AllowManualImports** check box is selected on the **Options** dialog box - **IP Preferences** pane, the **Manual Import Unified Image** dialog box displays. Continue to import the image by completing the following steps.

     a. Enter the name of the unified image in the **Image File** field.

     b. Select an image type from the **Unified Image Type** list.

     c. Enter the image file name, excluding the file extension, in the **Image Label** field.

     d. Enter additional information for the image in the **User Defined Label** field. This entry appears under the **More Information** column on the **Unified Firmware Images** tab.

     e. Click **OK** on the **Manual Import Unified Image** dialog box.

        If the imported file already exists or the import operation fails for any reason, a message displays with details.

        After the import completes successfully, a message displays that the unified image imported successfully.

Updating unified images

Use the Configuration Wizard to update firmware images. You can access the Configuration Wizard using one of the following methods:

- Select **Configure > Configuration Wizard**.
- Complete the following steps.
    a. Select **Configure > Firmware > Management**.
    b. Click the **Unified Firmware Images** tab on the **Firmware Management** dialog box.
    c. Click **Update**.

Refer to "Modifying a payload configuration" on page 774 for information on updating firmware images using the Configuration Wizard.

For NetIron CER/CES devices running 5.4, when deploying the simplified firmware image from 5.4 to 5.5, complete the following steps.

1. Upgrade the simplified firmware image from 5.4 to 5.5.

   Note that the FPGA image fails to download.
2. Reload the product.
3. Upgrade the FPGA (pbifmetro.bin) image manually.
4. Reload the product.

Deploying unified images to products

The Management application stores previously imported unified images. These images can be placed in a unified image payload and deployed to products using the Configuration Wizard.

NOTE
Firmware images deploy to products one device at a time. If a combination of cluster nodes is selected and the standalone VDX switches are targets, the deployment occurs for the cluster nodes as well as for the standalone VDX switches.

Deleting unified images from the Management application

If a unified image must be deleted from the Management application, perform the following steps.

1. Click the **Unified Firmware Images** tab on the **Firmware Management** dialog box.
2. Select the unified image that you want to delete.
3. Click the **Delete** button.

   A confirmation warning displays.
4. Click **Yes** to continue with the delete, or **No** to cancel it.

Serial firmware update and activation for NOS devices

With Network OS release 4.0, you can update and activate firmware on an entire cluster (either logical chassis mode or fabric cluster mode), on selected nodes in the cluster, or on nodes in standalone mode, by performing the following steps.

1. Click the **IP** tab in the upper-left corner of the Management application.
2. Select **Ethernet Fabrics** from the view list on the Product List toolbar.

   Cluster node members (or root node) are displayed, depending on your configuration.
3. Select the desired node or nodes for firmware updates and activation.
4. Right-click the highlighted nodes, then select **Firmware > Firmware Management.**

   NOTE
   If you are performing a firmware activation (but not a serial update) on only one node, you can highlight this node, then perform a right-click and select **Firmware > Firmware Activate.** If this is the only action you want to perform, you are done and do not need to continue with the steps below.
5. In the **Firmware Management** dialog box, click the **Unified Firmware Images** tab.
6. Click **Update**.
7. From the **Hardware Type** list, select **VDX**.
8. Use the **Serial Update** and **Firmware Activate** check boxes as desired. For example:
   - You can select both boxes and enable the **Firmware Activate** check box to activate firmware on each node in a serial process.
   - You can leave the **Serial Update** check box clear and enable the **Firmware Activate** check box to activate firmware on each node in a parallel process.
   - You can select the **Serial Update** check box and leave the **Firmware Activate** check box unselected to begin the firmware download serially on selected nodes while delaying firmware activation on each node.
9. Click **Next**.
10. Follow any additional online instructions, and the procedure(s) that you selected begin.

Chapter

VLAN Management

27

In this chapter

VLAN Manager

NOTE
VLAN Management is not supported on Fabric OS devices.

VLAN Manager allows you to manage Virtual Local Area Networks (VLANs) on Brocade products. You can use VLAN Manager to view existing VLAN configurations on the products and the network, and edit the configuration on supported platforms, including Network OS platforms but not the Brocade 6910. By default, interfaces on a device that are not assigned to a VLAN are members of the default port VLAN; therefore, all device interfaces assigned to the default VLAN constitute a single Layer 2 broadcast domain.

When you assign an interface to a port VLAN, that interface is automatically removed from the default VLAN, VLAN 1. Interfaces assigned to port VLANs can be defined as untagged, tagged, and converged ports. An untagged port can be a member of only one VLAN, while a tagged port can be a member of more than one VLAN. Interfaces defined as converged allow tagged and untagged traffic to pass through an interface at the same time.

Default VLAN

When you enable port-based VLANs, all ports in the system are added to the default VLAN. The default VLAN ID is 1. The default VLAN is configurable except on Network OS devices. If you want to use the VLAN ID "VLAN 1" as a configurable VLAN, you can assign a different VLAN ID to the default VLAN. You must specify a valid VLAN ID that is not already in use. For example, if you have already defined VLAN 10, do not try to use "10" as the new VLAN ID for the default VLAN. Valid VLAN IDs are from 1 through 4095. For DCB and Network OS products, the user-configurable range is from 1 through 3583 (3584 through 4095 are reserved). When GVLAN is enabled, the VLAN range supported for the Brocade VDX 8770 and Brocade VDX 6740 and VDX 6740-1G is from 4091 through 4095.

Super-aggregated VLAN

A super-aggregated VLAN allows multiple VLANs to be placed within another VLAN. This feature allows you to construct Layer 2 paths and channels. It is useful for Virtual Private Network (VPN) applications in which you need to provide a private, dedicated, Ethernet connection for an individual client that can transparently reach its subnet across multiple networks.

Private VLAN

NOTE
PVLAN read-only support is provided.

Private VLAN (PVLAN) provides device isolation through the application of Layer 2 forwarding constraints. PVLAN allows end devices to share the same IP subnet while being isolated at Layer 2. This enables network designers to employ larger subnets and thereby reduce the address management overhead.

There are three types of PVLAN:

- Primary VLAN — A primary VLAN is a unique and common VLAN identifier within the PVLAN domain and its VLAN ID pairs.
- Isolated VLAN — An isolated VLAN is a secondary VLAN that isolates all hosts connected to its ports at Layer 2.
- Community VLAN — A community VLAN is a secondary VLAN that is associated with a group of ports that connect to a certain community of end devices based on mutual trust relationships.

A PVLAN domain is built with at least one pair of VLAN IDs: one primary VLAN ID (Vp) plus one or more secondary VLAN IDs (Vs).

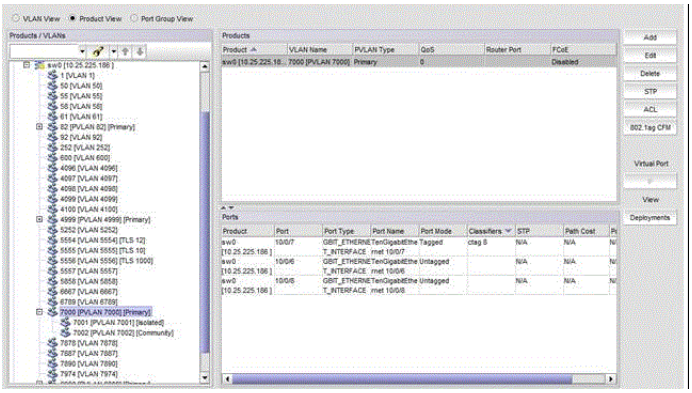


FIGURE 315 Private VLAN

Remote Switched Port Analyzer

Remote Switched Port Analyzer (RSPAN) VLAN is used to monitor source ports, VLANs, and destination ports on different switches in your network. You can configure any VLAN as an RSPAN VLAN that meets the following conditions:

- The same RSPAN VLAN is used for an RSPAN session in all the switches.
- All participating switches support RSPAN.

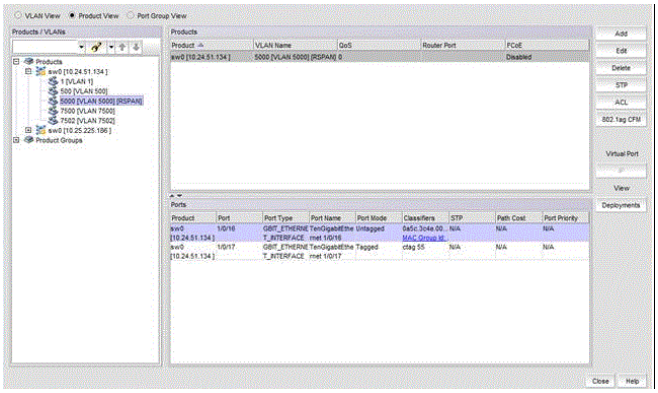


FIGURE 316 Remote Switch Port Analyzer

Transparent LAN Support

Transparent LAN Support (TLS) supports the VLAN group rather than an individual VLAN. The TLS service provided is associated with a single transparent VLANs that represents all the VLAN in a group. When Transparent LAN Support (TLS) is assigned to a Virtual Fabric VLAN, the ports that are tagged to TLS allow you to configure multiple cTags.

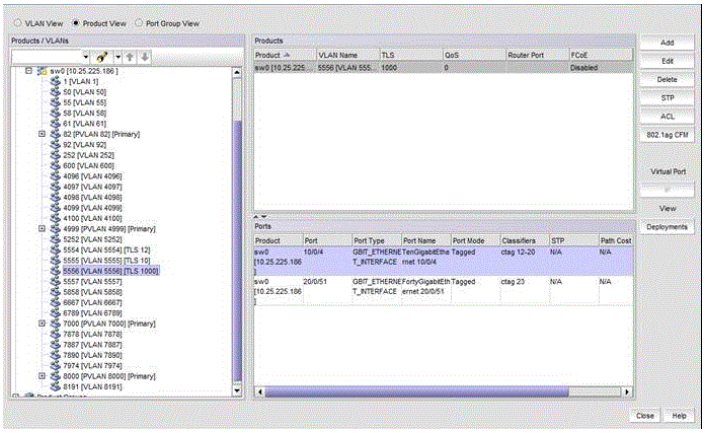


FIGURE 317 Transparent LAN Support

Configuration requirements for VLAN Manager

Before you can manage VLANs with VLAN Manager, you must complete the following tasks:

- Make sure that the discovery process has been run. Discovery captures configuration information from IronWare OS products and places that information in the Management application database. Refer to Chapter 3, “Discovery” for details on running discovery.
- Make sure the VLAN Manager privilege is in your Management application user role or account if you need to use VLAN Manager.
- If you want to view VLAN connectivity in the Layer 2 topology, make sure Foundry Discovery Protocol (FDP) or Link Layer Discovery Protocol (LLDP) is enabled on the devices on the network.

Displaying a list of VLANs

To view the list of VLANs that were discovered on the network, select **Configure > VLANs**.

The **VLAN View** tab of the **VLAN Manager** dialog box displays.

The VLAN Manager toolbar contains the following buttons:

- **Add** — Launches the **Add VLAN** dialog box.
- **Edit** — Launches the **Edit VLAN** dialog box.
- **Delete** — Launches the **Delete VLAN** dialog box.
- **STP** — Allows you to configure STP, RSTP, MSTP, PVST, or RPVST information for a product, port, or VLAN.
- **ACL** — Launches the **ACL Configuration** dialog box, where you can assign access control lists to a VLAN.
- **802.1ag CFM** — If the Management application manages at least one of the service provider products (NetIron XMR, MLX, CES, or CER), this button launches the **802.1ag CFM** configuration dialog box.
- **Virtual Port IP** — Launches the **IP Address** dialog box, which allows you to add an IP address to a Switch Virtual Interface (SVI) on DCB products (also known as a Virtual Routing Interface).
- **Deployments** — Launches the **Deploy VLANs** dialog box and displays only saved VLAN and STP deployments.

VLAN management in a VCS environment

Table 83 lists the VLAN management features that are supported in VCS mode (Fabric mode), logical chassis mode, and standalone mode.

TABLE 83 VLAN management features supported for VCS mode

Feature	VCS (FC mode)	Logical chassis mode	Standalone mode
VLAN topology	Yes (shown at the fabric level)	Yes	Yes
STP topology	No	No	Yes
VLAN Manager	Yes (shown at the fabric level)	Yes	Yes
STP views	No	No	Yes
VLAN reports	Yes	Yes	Yes
STP reports	No	No	Yes

VLAN Manager tabs

VLAN Manager has three views:

- VLAN view

  Displays distinct Layer 2 broadcast domains by VLAN ID. If FDP or LLDP is not enabled on a device, each VLAN from each device is displayed in separate folders by VLAN ID. If FDP or LLDP is enabled on the devices, a VLAN folder shows device connectivity on the Layer 2 broadcast domains.

If there are super-aggregated VLANs that have been configured on the network, VLANs are grouped by their super-aggregated VLAN memberships.

If the VLANs are in different networks, they display as different nodes, even if FDP or LLDP is not enabled on the device.

- For VCS fabric technology, a single VCS node displays in the VLAN view based on VLAN membership of the fabric nodes. This view is supported in Fabric mode.
- Network OS products in standalone mode display like any other product in the VLAN view.

- Product view

  Displays the VLANs configured on a device. The information is grouped by products. Select a product to view the VLANs that are on that device.

  - For VCS fabric technology, a single VCS node displays in the Product view. All the VLANs across its nodes display in Fabric mode.
  - Network OS products in standalone mode display like any other product in the Product view.

- Port Group view

  Displays all VLANs configured for the selected port group. Port group support is only available in the VLAN editor launched from the **Port Group View** tab.

  - The **Products** list displays the switch name, VLAN name, PVLAN type, TLS, QoS, router port, and FCoE.

    NOTE
    The **PVLAN Type** column is displayed only when you configure PVLAN using the CLI.

  - The **Ports** list displays the VLAN interface parameters for the selected product: switch name, port identifier, port type, port name, port mode, STP, path cost, port priority, and classifiers.

NOTE
The product must be part of the area of responsibility (AOR), along with the port groups, to display and perform all the operations.

Displaying VLANs in the VLAN view

The **VLAN View** tab displays all the VLANs discovered on the network and lists them by VLAN IDs (Figure 318).

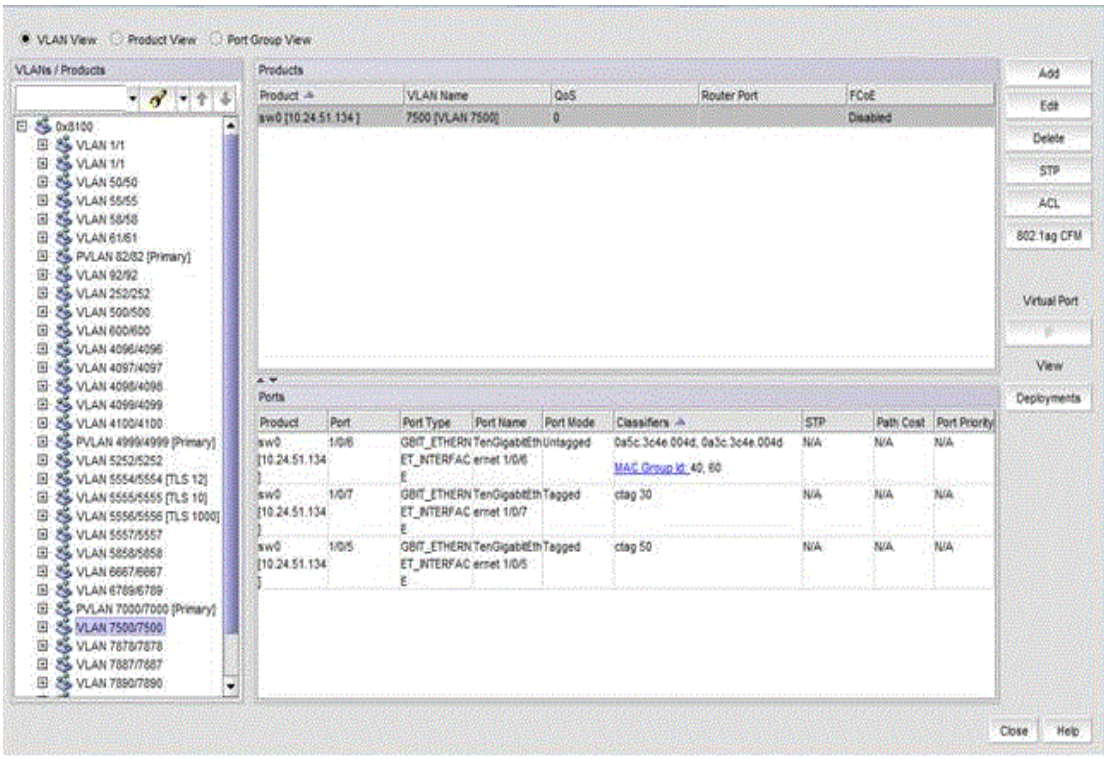


FIGURE 318 VLAN Manager dialog box - VLAN View tab

To view the VLANs or products in the **VLAN View** tab, complete the following steps.

1. Click the **VLAN View** tab in the **VLAN Manager** dialog box.
2. Expand the folder under the **VLAN View** tab, then double-click a super-aggregated VLAN to display its port VLANs or products.

   VLANs are listed by their topologically distinct broadcast domains. A VLAN that is listed several times means that the products on which the VLAN has been configured cannot communicate with each other. Either they are not physically connected or FDP or LLDP is not enabled on these products. If FDP or LLDP is enabled, then each VLAN lists the products in that broadcast domain.
3. Select a VLAN to expand the list of products listed under that VLAN. Use the Search tool to find VLANs, products, or ports quickly.

   A VLAN may be listed several times. For example, the first three VLAN1s have only one product. Each product in each VLAN is in its own broadcast domain and either does not have connectivity with other products or FDP or LLDP is not enabled on that product.

   The fourth VLAN1 has several products listed under it. All those products are in the same Layer 2 broadcast domain.

   When a port VLAN is selected, the **Edit**, **Delete**, and **STP** buttons become available. At this point, you can create or modify port VLANs, delete a port VLAN, configure STP or RSTP definitions for IronWare OS products, and configure STP, MSTP, RSTP, PVST, and RPVST definitions for Network OS products in standalone mode.

4. Click a product under a port VLAN to select it. The interfaces on that product that belong to the VLAN are listed in the interface list.

   The list shows the following information:

   - Port — The interface number. This can be a port number represented as a unit, slot number or port number, or a virtual routing interface ID.
   - Port Type — A description of the type of interface on the product, for example, ETHERNET_INTERFACE or VIRTUAL_INTERFACE.
   - Port Name — The name of the interface, if one was configured.
   - Port Mode — Indicates the tag mode of the interface. Tagged represents the port is in dual mode but is in the tagged state for that particular VLAN. Untagged represents the port is untagged for that particular VLAN. The third port mode is Converged.
   - STP — Indicates whether STP is enabled or disabled.
   - Path Cost — The STP cost of using the port to reach the root bridge.
   - Port Priority — The preference that STP gives this port relative to other ports for forwarding traffic out of the spanning tree.
   - Classifiers — The VLAN Classifier group IDs associated with Access/Converged ports and link aggregation groups. The following values are displayed if Virtual Fabrics is configured on a Network OS device.
     - cTag — Tagged mode
     - MAC Address and MAC Group ID — Untagged mode

Displaying VLANs by products

The **Product View** tab of the **VLAN Manager** dialog box presents the products that have been discovered on the network and the VLANs that have been assigned to them.

NOTE
Only products assigned to Management application areas of responsibility (AORs) are listed under the VLANs in the **Product View** tab.

To view VLANs, complete the following steps.

1. Click the **Product View** tab in the **VLAN Manager** dialog box.

   The **Product View** tab of the **VLAN Manager** dialog box displays (Figure 319).

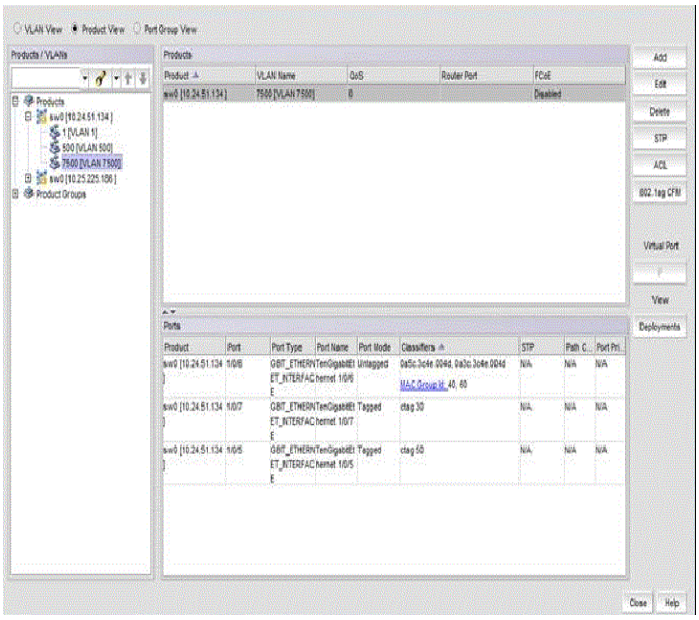


FIGURE 319 VLAN Manager dialog box - Product View tab

2. Expand a product to display the port VLANs that have been configured on that product.
3. Click a VLAN in the list to display the interfaces on that product that belong to the VLAN.
4. Click **MAC Group IDs** to display the MAC group address (Figure 320).

   The MAC group address dialog box is displayed.

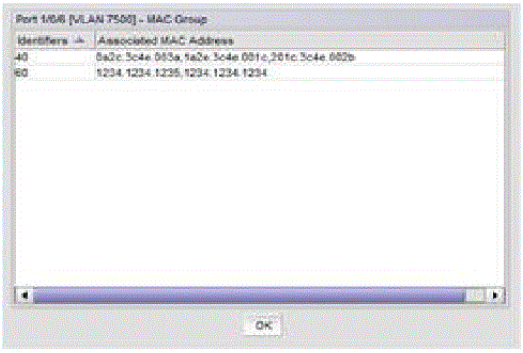


FIGURE 320 MAC Group Address

NOTE
The MAC addresses are displayed with the associated MAC group IDs

Port VLANs

VLAN Manager facilitates the creation, modification, and deletion of port VLANs on products that are known to the Management application. It also aids in the bulk deployment of these VLANs. For example, VLAN 3 can be configured on four products. If the VLAN definition for VLAN 3 is modified, the new definition can be deployed to all four products at one time.

The Configure Port VLAN function in VLAN Manager allows you to define a port VLAN definition that adds a new VLAN to a product or modify an existing port VLAN on a product. The port VLANs can be designated as tagged, untagged, or converged.

Adding or modifying port VLANs

To create or modify port VLANs, complete the following steps.

1. On the **VLAN Manager** dialog box, click the **VLAN View** or **Product View** tab to enable the **Add** button.
2. Click **Add** to add port VLANs or click **Edit** to modify existing port VLANs.

   The **Ports** tab of the **Add VLAN** dialog box displays (Figure 321).

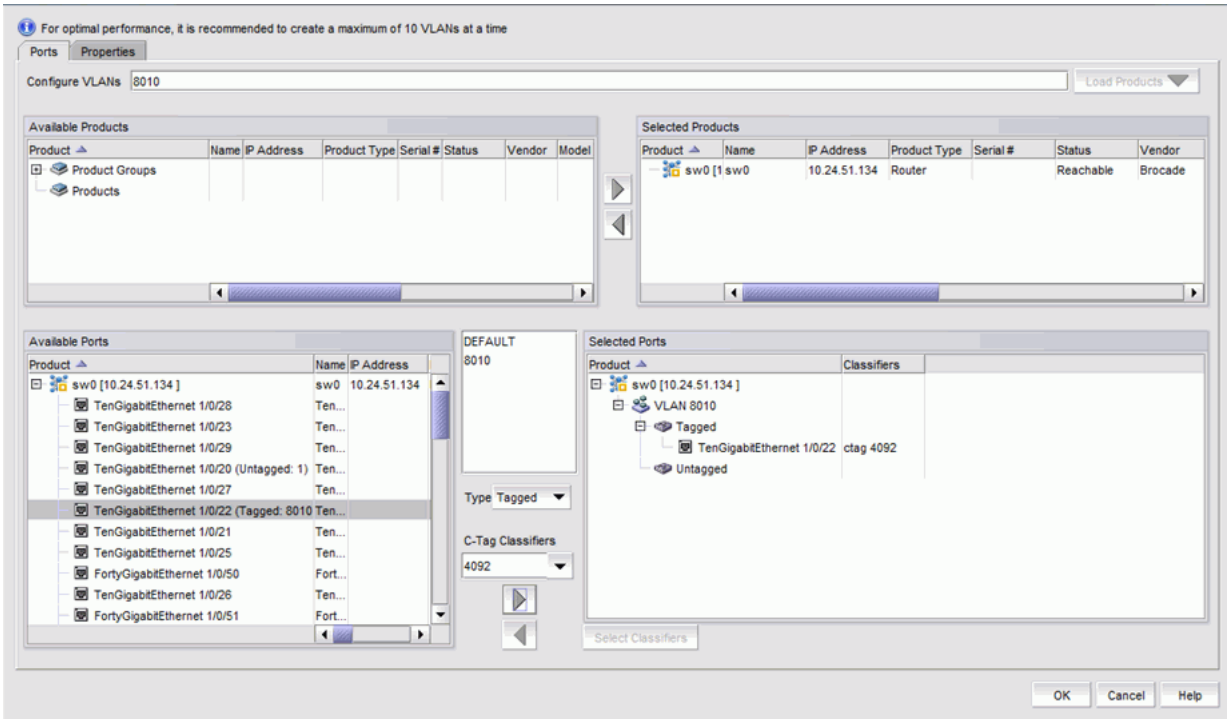


FIGURE 321 **Add VLAN dialog box - Ports tab**

3. Enter a VLAN ID in the **Configure VLANs** field.

   You can enter more than one ID, either by range (for example, 10-20, 30-40) or by separating individual IDs with a comma (for example, 10, 45, 79, 30). For DCB products, the VLAN ID range is from 1 through 3583 and for Network OS products the range is from 1 through 8191.

   cTag classifiers are supported for Virtual Fabrics and the range is from 2 through 4094.

4. Click the **Load Products** button. Products that already have the entered VLAN IDs configured on them are automatically moved to the **Selected Products** list. The **Load Products** button is disabled by default.
5. Under the **Available Products** list, select one or more products to which the VLAN will be assigned. You can also use the Search tool to find ports.
6. Click the right arrow button to move your selection to the **Selected Products** list.
7. Expand the folder for a selected product in the **Available Ports** list to display all the interfaces or trunk groups on the product that can be added to the VLAN.

   The **Selected Ports** list displays the list of configured VLANs. Initially, these VLANs contain no ports. If no ports or trunk groups are selected, an empty VLAN is created on the products (DCB and Network OS products).
8. In the **Available Ports** list, select the interfaces that you want to assign to a VLAN.

   If you place your pointer over an interface in the **Available Ports** list, a tooltip appears, showing the VLAN assignment of the interface. You can also use the Search toolbar to search for ports under the **Available Ports** list, then assign the ports found to the VLAN.
9. In the **Available Ports** list, select the port-channel that you want to assign to a VLAN.
10. In the **Select VLANs** list, select the VLAN you want to assign to the selected interfaces. The list includes the default VLAN (VLAN1) and the VLAN or VLANs you are currently creating. You can assign one or more VLANs to the selected ports.

    In the **Selected Ports** list, each VLAN node is shown as Tagged, Untagged, or Dual Mode. If a port is already tagged in one VLAN, it can be marked as Tagged in other VLANs. The port can also be marked as Untagged in other VLANs, which changes its mode to Dual Mode. Dual Mode is not supported on Network OS products.
11. Complete one of the following tasks:
    - If you want to assign the interface to the VLAN as an untagged port, select **Type** as **Tagged** and click right arrow button.
    - If you want to assign the interface to the VLAN as a tagged port, select **Type** as **Untagged** and click right arrow button.
    - If you want to make the VLAN on the interface dual mode, assign that interface as tagged and select the same interface and assign as untagged to another VLAN. Dual mode ports can be added to any VLAN except for the default (VLAN 1).
12. Add a cTag by completing the following steps.
    a. Select the port from the **Available Ports** list.
    b. From the **VLAN ID** folder, select a VLAN ID greater than 4096.
    c. From the **Type** list, select **Tagged**.

       The **cTag classifier** list is enabled.
    d. Enter the valid cTag ID (from 2 through 4094) and click the right arrow.
13. Click the **Select Classifiers** button to launch the **Select Classifier Groups** dialog box, shown in Figure 322, where you can assign classifiers and rules for supported DCB and Network OS platform-based VLANs.

The **Select Classifiers** button is disabled by default. To enable the button, select an untagged and classifier-configured port in the **Selected Ports** list..

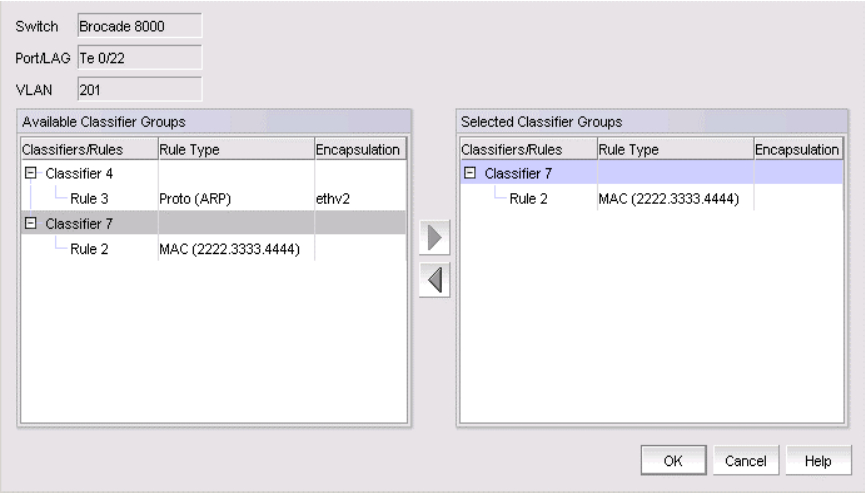


FIGURE 322 **Select Classifier Groups dialog box**

NOTE
The cTag classifier list is disabled when **Untagged** is selected.

NOTE
The **MAC** and **MAC Group classifier** configurations are not supported in Network Advisor

Adding or modifying dual mode ports

You can configure an interface in a VLAN as a dual mode port by assigning it as a tagged port to one VLAN and as an untagged port to another VLAN. You can add a dual mode port to any VLAN except the default VLAN, VLAN 1.

NOTE
Dual mode is not supported on Network OS products.

To add or modify a dual mode port, perform the following steps.

1. Follow the steps in "Adding or modifying port VLANs" on page 827 to familiarize yourself with adding tagged and untagged ports to a VLAN.
2. Select **Configuration Manager > VLAN Manager**.

   The **VLAN Manager** dialog box - **VLAN View** tab displays.
3. Click the **Product View** tab.
4. Click **Add**.
5. From the **Available Ports** list on the **Ports** tab of the **Add VLAN** dialog box, select the interface that will be added as a dual mode port.
6. Select a VLAN from the **Select VLANs** list.

7. Click the **Untag** button and click the left arrow to assign the port as an untagged port to the selected VLAN. The **Selected Ports** list shows the interface listed under the VLAN to which it was assigned.
8. Select the same interface from the **Available Ports** list.
9. Select another VLAN from the **Select VLANs** list.
10. Click the **Tag** button and click the right arrow to assign the port as a tagged port to the second VLAN. The **Selected Ports** list shows the port as untagged under one VLAN and tagged under another VLAN.

Assigning DCB ports to a VLAN

In Data Center Bridging (DCB) switches, the L2 interface mode of the port determines whether a port can be in an untagged, tagged, or converged mode. Table 84 shows the L2 mode and tagged mode compatibility on the DCB interface.

TABLE 84 L2 mode and tagged mode compatibility on a DCB interface

L2 mode	Tagged mode
Access, Converged	Untagged
Trunk, Converged	Tagged
Converged	Dual

NOTE
To make L2 interface mode changes, you must have the DCB Management privilege.

You can change the L2 interface mode of a port using the **Add LAG** dialog box. Refer to "Adding a LAG" on page 493 for instructions.

Adding VLAN properties

The **Add VLAN** dialog box has two tabs: **Ports** and **Properties**. The VLAN properties vary for different products, for example:

- When an IronWare OS VLAN is selected, the **Name**, **QoS**, **Spanning Tree,** and **Router Interface** fields, and the **Transparent VLAN Flooding enable** check box display.
- When a DCB VLAN or product is selected and moved to the **Products/VLAN** list, the **Name** and **Admin Status** fields and the **FCoE** check box display. All the fields displayed for DCB products are read-only.

To add VLAN properties, complete the following steps.

1. On the **Add VLAN** dialog box, click the **Properties** tab.

   The **Add VLAN** dialog box — **Properties** tab, shown in Figure 323, displays.

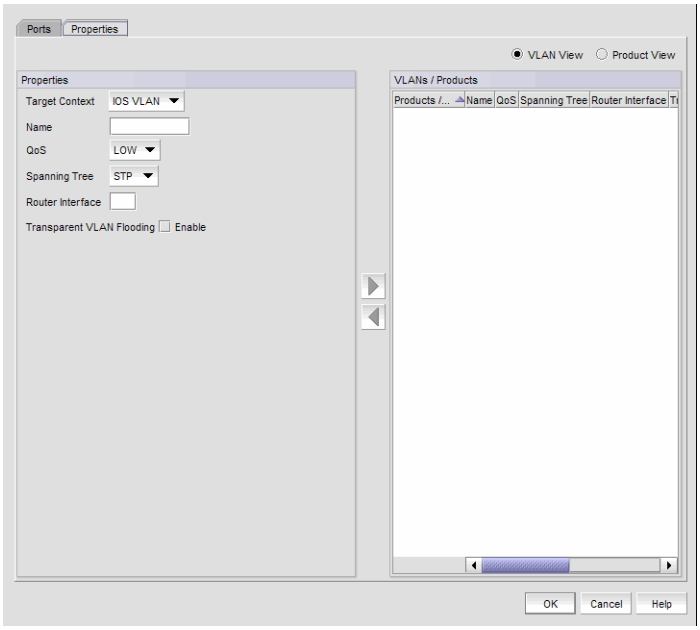


FIGURE 323 Add VLAN dialog box — Properties tab

2. Click the **VLAN View** option to view the products to which the VLANs are to be deployed, or click the **Product View** option to display the VLANs that are to be deployed to that product.
3. Select the Fabric OS (FOS) VLAN, IronWare (IOS) VLAN, or Network OS (NOS) VLAN type from the **Target Context** list. You must select only one VLAN type. If multiple VLAN types are selected, the target context becomes the default and an error message displays.
4. Enter the following information:

   For **IOS VLAN** Properties:

- **Name** — Displays the name of the VLAN, which is editable.

- **QoS** — Select a QoS level from the list.
  - Select Low (None or 0) through High (7) for NetIron CES products. Select None for NetIron CER and NetIron CES products if the product does not have VLAN priority configured. (None applies only to NetIron CER and NetIron CES products.)
  - Select Low (0) through High (7) for all other IronWare OS IP products.
- **Spanning Tree** — Select the type of Spanning Tree Protocol from the **Spanning Tree** list. The list options include STP, RSTP, and None.
- **Router Interface** — If you want to add a virtual routing interface to the VLAN, enter the virtual routing interface number in this field. You can add an IP address to the virtual routing interface once the VLAN is deployed.
  - From the **Product View** tab, you can configure one virtual routing interface per VLAN for each product.
  - From the **VLAN View** tab, you can edit virtual routing interfaces on multiple products for a specific VLAN.

    The **Router Interface** field is editable for products that support routing and have a router image of the firmware installed.
- **Transparent VLAN Flooding** (NetIron 5.4 and later) — Selecting this check box allows packets to be forwarded without any form of CPU intervention including MAC learning and MAC destination lookups.

  NOTE
  Because this feature floods all VLAN packets in hardware, it is not expected to work in conjunction with routing functions.

  For **FOS VLAN** properties:
  - **Name** — Displays the name of the VLAN, which is editable.
  - **Admin Status** — Displays one of the following administrative statuses for the VLAN interface:
    - Up — The special routing interface is up and can route traffic from other VLANs.
    - Down — The special routing interface is down and cannot route traffic from other VLANs.
  - **FCoE** — Indicates whether Fibre Channel over Ethernet (FCoE) is enabled or disabled on the VLAN.

  For **NOS VLAN** properties:
  - **Target Context** — Select a VLAN type (FOS VLAN, IOS VLAN, or NOS VLAN) from the list.
  - **Name** — Displays the name of the VLAN, which is editable.
  - **QoS** — Select a QoS level from the list.
  - **Spanning Tree** — Select the type of Spanning Tree Protocol from the list. The list options include STP, RSTP, MSTP, PVST, RPVST, and None.
  - **Virtual Interface** — Select the check box to enable the virtual interface.

5. Click **OK** to save the changes.

Modifying port VLAN properties

Complete the following steps to modify port VLANs using the **VLAN View** tab or the **Product View** tab on the **Edit VLAN** dialog box.

1. On the **VLAN Manager** dialog box, click the **VLAN View** or **Product View** tab.
2. If in the VLAN view, select and expand a VLAN entry, or if in the Product view, select and expand a product and click the **Edit** button.

   NOTE
   When a Network OS VLAN is selected, the **Name** and **Admin** fields display. In VCS Fabric mode, the VLAN name from the seed switch of the fabric displays.

   The **Ports** tab of the **Edit VLAN** dialog box displays.
3. Select the IronWare (IOS) VLAN, Fabric OS (FOS) VLAN, or Network OS (NOS) VLAN type from the **Target Context** list. You must select only one VLAN type. If multiple VLAN types are selected, the target context becomes the default and an error message displays.
4. Modify the information detailed in step 4 of "Adding VLAN properties" on page 831.
5. Click **OK** to save the changes.

Deleting port VLANs from products

Deleting a port VLAN removes all the interfaces on a product from that VLAN. A port VLAN can be deleted in both the VLAN and Product views.

Deleting a port VLAN in VLAN view

1. On the **VLAN Manager** dialog box, select **VLAN View**.
2. Select the VLAN to be deleted. You can select multiple VLANs by holding down the **Ctrl** and **Shift** keys and clicking the VLAN nodes.
3. Click **Delete** to launch the **Deploy VLANs** dialog box.
4. Deploy the VLAN configuration to the product by completing the deployment steps in "Deploying VLAN configurations" on page 834.

   Once the VLAN is deployed, it is deleted from the product.

Deleting a port VLAN in Product view

1. On the **VLAN Manager** dialog box, select **Product View**.
2. Expand the product on which you want the VLAN to be deleted.
3. Select the VLAN under the product. You can select multiple VLANs by holding down the **Ctrl** and **Shift** keys and clicking the VLAN nodes.
4. Click **Delete** to launch the **Deploy VLANs** dialog box.
5. Deploy the VLAN configuration to the product by completing the deployment steps in "Deploying VLAN configurations" on page 834.

   Once the VLAN is deployed, it is deleted from the product.

Deploying VLAN configurations

The **Deploy VLANs** dialog box allows you to deploy a VLAN configuration to target products. Duplicate action is not supported.

1. Select a deployment option:
    - Click the **Deploy now** option if you want to deploy the VLAN definition.
    - Click the **Save deployment only** option if you want to save the VLAN definition without scheduling its deployment.
    - Click the **Schedule** option if you want to schedule the deployment of the VLAN definition.
2. Select a **Save Configuration** option:
    - Click the **Save to running** option to save the configuration while the system is running.
    - Click the **Save to running and startup** option to save the configuration both while the system is running and when the system starts up.
    - Click the **Save to running and startup then reboot** option to save the configuration both while the system is running and when the system starts up, and then automatically reboot.
3. Enter a name in the **Name** field that will be used to identify the configured VLAN.
4. Enter a description in the **Description** field that will be used to identify the configured VLAN.
5. Click the **Schedule** check box, which is available if you selected **Schedule** as a deployment option, to select a frequency.
6. Click the **Snapshots** check box if you want the Management application to run and save a report after this configuration is deployed to the device. You can run snapshots before and after deployments only for IronWare products. Snapshots are not supported for DCB products.
7. Click **OK** to deploy the configuration on the selected port VLAN.
8. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected products.
9. Click **Close** to close the **Deployment Status** dialog box.

Spanning Tree Protocol configuration

Spanning Tree Protocol (STP) is a Layer 2 protocol that ensures a loop-free topology for any bridged local area network (LAN). STP allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails. STP creates a spanning tree within a mesh network of connected Layer 2 bridges and disables those links that are not part of the tree, leaving a single active path between any two network nodes.

NOTE
STP is disabled when a Network OS product is in VCS mode and an error message is displayed if you configure STP from the Management application. The VCS nodes do not participate in the STP topology; however, STP can be enabled on external switches connected to the VCS fabric.

The Management application supports the following types of STP:

- STP — The Spanning Tree Protocol (IEEE 802.1d) is a link layer network protocol that ensures a loop-free topology for any bridged LAN.

- RSTP — Rapid Spanning Tree Protocol (IEEE 802.1w Internet standard) is a refinement of STP, which provides for faster spanning tree convergence after a topology change.
- MSTP — Multiple Spanning Tree Protocol (IEEE 802.1s Internet standard) allows several VLANs to be mapped to a reduced number of spanning tree instances. This is possible because most networks do not need more than a few logical topologies. Each instance handles multiple VLANs that have the same Layer 2 topology.

DCB, Network OS (v3.0.0 and later), and IronWare products in standalone mode support viewing of STP, Rapid STP (RSTP), and Multiple STP (MSTP). Network OS products in standalone mode also support Per-VLAN Spanning Tree (PVST) and Rapid PVST (RPVST). For Network OS (v4.0.0 and later), configurations of Spanning Tree Protocol on PVLAN can be viewed in the **STP Configuration** dialog box.

Configuring STP or RSTP on a port VLAN

You can configure Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) attributes from the **VLAN View** tab or the **Product View** tab on the **VLAN Manager** dialog box.

NOTE
The **VLAN View** tab displays VLAN membership information for the Brocade 6910 switch; however, STP configuration is not supported on the IronWare OS 6910 switch.

1. Perform one of the following tasks to select the VLAN on which STP or RSTP will be configured:
   - On the **VLAN View** tab, expand the list of VLANs and select one or multiple VLANs on which STP or RSTP will be configured.
   - On the **Product View** tab, expand the product, product group, or IP subnet folder that contains the products on which the VLAN you want is configured. Then expand the entry to display its VLAN and select the VLAN where STP or RSTP will be configured. You can select more than one VLAN from this tab.

   For either view, you can use the Search tool to look for the VLAN on which STP or RSTP will be configured.

   NOTE
   The parameters display differently depending on whether the STP configuration is at the product, VLAN, or port level.

   Either of these methods enables the **STP** button on the **VLAN Manager** dialog box.
2. Click the **STP** button on the **VLAN Manager** dialog box to display the **STP Configuration** dialog box (Figure 324).

   The products on which the VLAN is configured appear on the dialog box.

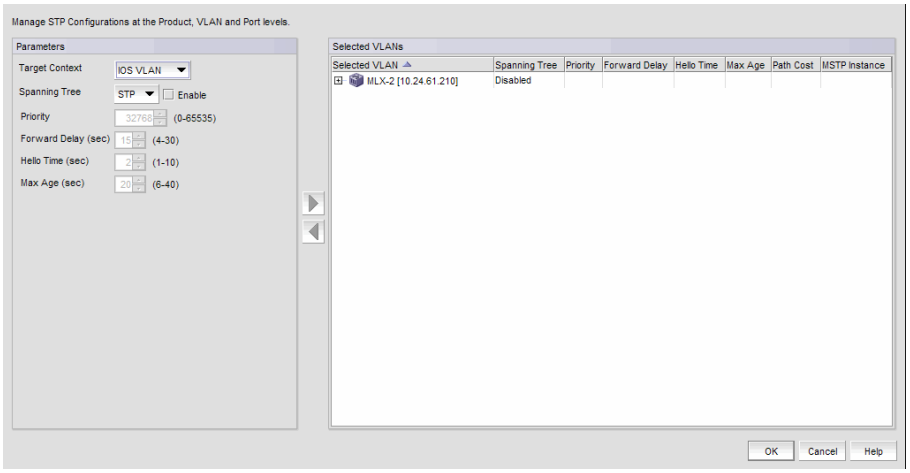


FIGURE 324 STP Configuration dialog box

3. Select the target switch, VLAN, or port from the **Target Context** list. Target contexts and spanning tree options at the product, VLAN, or port level are listed in Table 85.

TABLE 85 Spanning tree configuration matrix

Target context	STP type
IOS VLAN	STP, RSTP
IOS Port	STP, RSTP
FOS Product	STP, RSTP, MSTP
FOS VLAN	MSTP
FOS Port	STP, RSTP, MSTP
NOS Product	STP, RSTP, MSTP, PVST, and RPVST
NOS VLAN	MSTP
NOS Port	STP, RSTP, MSTP, PVST, and RPVST

4. Select the type of Spanning Tree Protocol from the **Spanning Tree** list.
5. Select the **Enable** check box if you want to enable the protocol you selected.
6. Enter a value in the **Priority** field to identify the root bridge in a spanning tree (instance of STP). The bridge with the lowest value has the highest priority and is the root. A higher numerical value means a lower priority; thus, the highest priority is 0. The values range from 0 through 61440 for a Fabric OS device; the default is 32768. The values range from 0 through 65535 for an IronWare OS device; the default is 32768.
7. Enter the number of seconds a bridge waits (the listen and learn period) before it begins to forward data packets in the **Forward Delay** field. The values range from 4 through 30 seconds. The default is 15 seconds.
8. Enter the number of seconds a root bridge waits before it sends the next BPDU in the **Hello Time** field. The values range from 1 through 10 seconds. The default is 2 seconds.
9. Enter the number of seconds a bridge waits for a hello packet from the root bridge before initiating a topology change in the **Max Age** field. The values range from 6 through 40 seconds. The default is 20 seconds.

10. The **Force Version** list is available only if you selected **RSTP**. This parameter forces the bridge to send BPDUs in a specific format. You can enter one of the following values:
    - 0: The bridge has been forced to operate in STP default mode.
    - 1: The bridge has been forced to operate in RSTP default mode.
11. Specify an interval in the **Re-enable Port Interval** field, available only if you selected **RSTP**. This interval specifies the number of seconds to wait before the port is enabled. The values range from 10 through 1000000. The default is 300.
12. Click the **Re-Enable Port State** check box, which is available only if you selected **RSTP**, to enable or disable the timeout mechanism for the port.
13. Select the **Path Cost** option: **Standard** or **Custom**, available only if you selected **RSTP**. The path cost is the cost of using the port to reach the root bridge. When selecting among multiple links to the root bridge, STP chooses the link with the lowest path cost and blocks the other paths. Each port type has its own default STP path cost.
14. Click the right arrow button to move the selected product to the **Selected VLANs** list.
15. Click **OK** to launch the **Deploy STP** dialog box.

Deploying an STP configuration on a port VLAN

The **Deploy STP** dialog box allows you to view the STP configuration summary and configure deployment parameters for a selected VLAN.

The **Deploy STP** dialog box allows you to deploy an STP configuration to target products. Duplicate action is not supported.

1. Select a deployment option:
    - Click the **Deploy now** option if you want to deploy the STP configuration.
    - Click the **Save deployment only** option if you want to save the STP configuration without scheduling its deployment.
    - Click the **Schedule** option if you want to schedule the deployment of the STP configuration.
2. Select a **Save Configuration** option:
    - Click the **Save to running** option to save the configuration while the system is running.
    - Click the **Save to running and startup** option to save the configuration both while the system is running and when the system starts up.
    - Click the **Save to running and startup then reboot** option to save the configuration both while the system is running and when the system starts up, and then automatically reboot.
3. Enter a name in the **Name** field that will be used to identify the configured VLAN.
4. Click the **Schedules** check box, which is available if you selected **Schedule** as a deployment option, to select a frequency.
5. Click the **Snapshots** check box if you want the Management application to run and save a report after this configuration is deployed to the device.
6. Click **OK** to launch the **Deployment Status** dialog box.
7. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected products.

8. After the deployment has successfully completed, click **Close** to close the **Deployment Status** dialog box.

Configuring MSTP on a product

You can configure MSTP attributes from the **VLAN View** tab or the **Product View** tab on the **VLAN Manager** dialog box.

1. Perform one of the following tasks to select the VLAN on which MSTP will be configured:
   - On the **VLAN View** tab, expand the list of VLANs and select one or multiple VLANs on which MSTP will be configured.
   - On the **Product View** tab, expand the product, product group, or IP subnet folder that contains the products on which the VLAN you want is configured. Then expand the entry to display its VLAN and select the VLAN where MSTP will be configured. You can select more than one VLAN from this tab.

   Either of these methods enables the **STP** button on the **VLAN Manager** dialog box. For either view, you can use the Search tool to look for the VLAN on which MSTP will be configured.
2. Click the **STP** button on the **VLAN Manager** dialog box to display the **STP Configuration** dialog box.
3. Select the target switch, VLAN, or port from the **Target Context** list.
4. Select **MSTP** from the **Spanning Tree** list.

   The products on which the VLAN is configured appear on the **STP Configuration** dialog box (Figure 325).

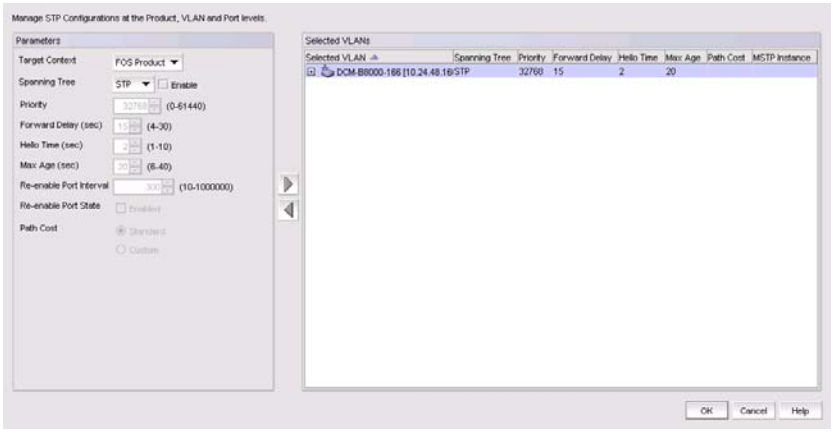


FIGURE 325 STP Configuration dialog box (with MSTP selected)

5. Select the **Enable** check box if you want to enable MSTP.
6. Enter a value in the **Priority** field to identify the root bridge in a spanning tree (instance of MSTP). The bridge with the lowest value has the highest priority and is the root. A higher numerical value means a lower priority; thus, the highest priority is 0. The values range from 0 through 61440. The default is 32768.
7. Enter the number of seconds a bridge waits (the listen and learn period) before it begins to forward data packets in the **Forward Delay** field. The values range from 4 through 30 seconds. The default is 15 seconds.

8. Enter the number of seconds a root bridge waits before it sends the next BPDU in the **Hello Time** field. The values range from 1 through 10 seconds. The default is 2 seconds.
9. Enter the number of seconds a bridge waits for a hello packet from the root bridge before initiating a topology change in the **Max Age** field. The values range from 6 through 40 seconds. The default is 20 seconds.
10. Enter the interval after which the port will be enabled in the **Re-enable Port Interval** field. The value ranges from 10 through 1000000. The default is 300.
11. Click the **Re-enable Port State** check box to enable the timeout mechanism for the port.
12. Select the **Path Cost** behavior option (**Standard** or **Custom**).
13. Specify the number of hops in a region before the Bridge Protocol Data Units (BPDUs) are discarded and the information held for a port is aged in the **Max Hops** field. The hop count determines when to trigger a reconfiguration. The value ranges from 1 through 40. The default is 20.
14. Enter **MSTP** in the **Region** field.
15. Enter the revision number for the configuration in the **Revision** field. The values range from 0 through 255. The default is 0.
16. Click **OK** to launch the **Deploy STP** dialog box.

Assigning an MSTP instance to a VLAN

NOTE
For Network OS products in standalone mode, you can configure from 1 through 31 MSTP instances and for Fabric OS DCB switches, you can configure from 1 through 15 MSTP instances; for the Fabric OS converged 10 GbE switch module for the IBM BladeCenter, you can configure from 1 through 31 MSTP instances.

1. Click the **STP** button on the **VLAN Manager** dialog box to display the **STP Configuration** dialog box.
2. Select a VLAN node (in this example, a FOS node) in the **Selected VLANs** list, and click the left arrow button.

   The target is automatically set to **FOS VLAN** in the **Target Context** list.
3. Select **MSTP** from the **Spanning Tree** list.

   The **STP Configuration** dialog box displays the **Available MSTP Instances** list.
4. Select one instance from the **Available MSTP Instances** list and, using the right arrow button, assign it to a VLAN in the **Selected VLANs** list.

Adding an MSTP instance

1. Click the **STP** button on the **VLAN Manager** dialog box to display the **STP Configuration** dialog box.
2. Select a VLAN node (in this example, a FOS node) in the **Selected VLANs** list, and click the left arrow button.

   The target is automatically set to **FOS VLAN** in the **Target Context** list.
3. Select **MSTP** from the **Spanning Tree** list.

The **STP Configuration** dialog box displays the **Available MSTP Instances** list.

4. Select an MSTP instance from the list under the **Available MSTP Instances** list, or enter the MSTP instance number.
5. Click **Add**.

   A new row is added to the **Available MSTP Instances** list. You can change the bridge priority, which is set, by default, to 32768.

VLAN routing

A VLAN restricts the broadcast domain to only its interface members. If nodes connected to two different VLANs want to communicate, they require an external router to route between the VLANs. Optionally, DCB products offer the ability to create a Switch Virtual Interface (SVI) to route between VLANs.

An SVI is a VLAN of switch ports represented by one interface to a routing or bridging system. There is no physical interface for the VLAN and the SVI provides the Layer 3 processing for packets from all switch ports associated with the VLAN. There is one-to-one mapping between a VLAN and an SVI; therefore, only a single SVI can be mapped to a VLAN. The VLAN is mapped to a network address using the SVI. All the nodes in the VLAN will belong to the subnet of the SVI.

NOTE
An SVI is also called a Virtual Routing Interface (VRI) in IronWare OS terms and Virtual Ethernet (VE) in Network OS terms. The SVI in DCB products, VRI in IronWare OS products, and VE in Network OS products are the same.

Managing IP addresses on an SVI

Switch Virtual Interfaces (SVIs) can be added to port VLANs when you create or modify VLAN definitions. SVIs can only be created in Layer 3 products.

Once VLAN definitions are deployed to products, you can add an IP address to the SVI by completing the following steps.

1. On the **VLAN Manager** dialog box, complete one of the following tasks:

- Click the **VLAN View** tab and expand the VLAN node. Select the product that contains the SVI that you want to define. The list of interfaces appears in the interface list. Click the SVI in the list of interfaces to select it.
- On the **Product View** tab, expand the product or group folders. Expand the products under the folder and select the VLAN that contains an SVI. The list of interfaces appears in the interface list. Click the SVI in the list of interfaces to select it.

NOTE
You must select the **Virtual Interface (Port Type)** row in the **Ports** table to enable the **IP** button.

2. Click the **IP** button.

   The **Virtual Port - IP Configuration** dialog box displays, as shown in Figure 326. If IP addresses have been configured for the SVI, they are listed in the **Selected IP Addresses** list.

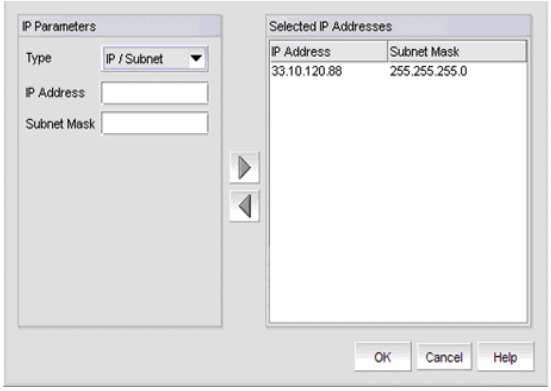


FIGURE 326 Virtual Port - IP Configuration dialog box

3. Complete one of the following steps:

- To add a new IP address to the SVI, enter the IP address in the **IP Address** field and click the right arrow button to move it to the **Selected IP Addresses** list.
- To modify an IP address of an SVI, select the IP address from the list and click the left arrow button to move the IP address back to the **IP Parameters** list. Because this list is for a single IP address, multiple IP addresses cannot be edited.

4. Enter the following information:

- **Primary** or **Secondary** options (DCB products only) — Indicates whether the IP address is the primary or secondary IP address of the VLAN.
- **Type** — Select the type of IP address you want to assign to the VLAN. Choose **CIDR** or **IP/Subnet**.
- Enter the IP address in the fields provided:
  - If you chose the **CIDR** format, enter a subnet address in the subnet_address/subnet_mask_bits format (for example, 192.168.2.10/24).
  - If you chose the **IP/Subnet** format, enter a subnet address in the subnet_address/subnet_mask format (for example, 192.168.2.10/255.255.255.0).

5. Click the right arrow button to add the IP address to the **Selected IP Addresses** list. If additional IP addresses are needed, continue adding them to the SVI and VE. You can assign a maximum of 255 IP addresses on DCB products and a maximum of 24 IP addresses on IronWare OS products.

6. Click **OK** to begin the deployment of the address to the product.

   The **Deploy IP Configuration** dialog box displays (Figure 327).

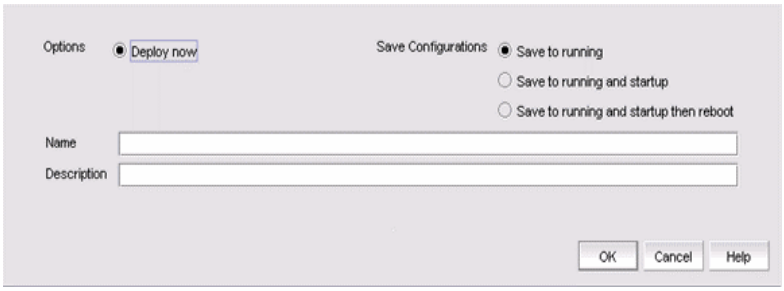


FIGURE 327 Deploy IP Configuration dialog box

7. Click the **Deploy now** option.
8. Select a **Save Configurations** option:

- Click the **Save to running** option to save the configuration while the system is running.
- Click the **Save to running and startup** option to save the configuration both while the system is running and when the system starts up.
- Click the **Save to running and startup then reboot** option to save the configuration both while the system is running and when the system starts up, and then automatically reboot.
- Enter a name in the **Name** field that will be used to identify the configured VLAN.

9. Enter a description in the **Description** field that will be used to identify the configured VLAN.
10. Click **OK** to deploy the IP address.

Chapter

MPLS Management

28

In this chapter

MPLS pre-configuration

Before you use the MPLS, you should make sure that you meet the following requirements.

1. Make sure all MPLS-capable devices meet the MPLS license requirements (refer to "MPLS licensing" on page 844.
2. Configure a loopback interface on each Ethernet router device and assign an IP address.
3. Make sure the customer-facing ports are not running FDP/CDP to be configured as a VLL or VPLS endpoint. Disable FDP/CDP on those ports.
4. Complete the following steps using a command line interface. For step-by-step procedures, refer to your product's configuration guide.
    a. Make sure that core-facing interfaces have unique IP address for MPLS.
    b. Make sure OSPF or IS-IS is configured for traffic engineering (if you need LSP functionality).
    c. Make sure the core-facing interfaces and loopback interfaces are part of OSPF or IS-IS for traffic engineering (if you need LSP functionality).
5. Enable MPLS on core-facing interfaces using the Management application (refer to "Configuring LDP" on page 845).
6. Create LSPs between the Provider Edge routers in both directions using the Management application (refer to "LSP" on page 846).

7. Create VLL instances using the Customer-facing ports using the Management application (refer to "VLL manager" on page 869).
8. Create VPLS instances using the Customer-facing ports using the Management application (refer to "VPLS Manager" on page 884).

MPLS licensing

The following are MPLS capable products:

- Ethernet Backbone router, Ethernet Core router, and Ethernet router running version 5.0.00 or earlier
- Ethernet Edge router and Ethernet Carrier router with MPLS software license running version 5.1.00 or later
- Ethernet Edge router and Ethernet Carrier router running version 5.0.00 or earlier

The following configurations are supported as MPLS configurations:

- Virtual Leased Line (VLL and Local-VLL).
- Virtual Private LAN Services (VPLS).
- Label Switching Path (LSP) features, including RSVP LSP and related configurations.

During discovery, all MPLS-licensed products are added to the **MPLS Licensed and Configured Products** product group (Figure 328).

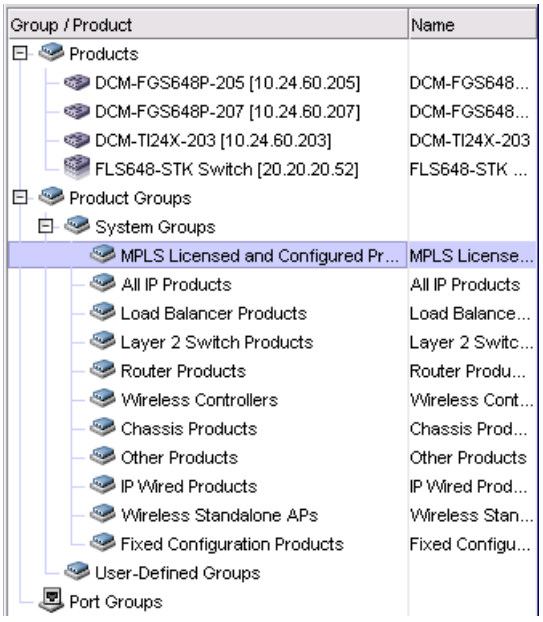


FIGURE 328 MPLS Licensed and Configured Products group

The following conditions must be met for inclusion in the **MPLS Licensed and Configured Products** product group:

- Your version of the Management application supports MPLS.
- Adding the product does not exceed the MPLS product license limit.

  For more information about how the Management application counts MPLS products, refer to *Brocade Network Advisor Software Licensing Guide*.

When the license limit is at 90%, when launching a VLL, VPLS or LSP, the following message is displayed:

```
Managed MPLS count has crossed 90% of licensed MPLS count.
```

This is shown once per session.

If the MPLS product license limit is reached, when an MPLS capable product is discovered with a configuration, those MPLS configurations (VLL, VPLS or LSPs) will not be discovered, and the following message is logged in Master Log:

```
Managed MPLS count exceeds the licensed MPLS count.
```

When a network discovery is performed and if the network contains many MPLS-licensed products, there is no particular order in which the products are added to the **MPLS Licensed and Configured Products** product group. Any products in that group may be used in VLL, Local-VLL, VPLS or LSP configurations.

It is possible to add an MPLS-capable product that is not in the product group when configuring a VLL, Local-VLL or VPLS if the license limit is not exceeded. When the license limit is reached, an add/edit/duplicate/delete operation can be performed only on the products in the product group.

MPLS overview

Multi-protocol Label Switching (MPLS) is a packet-switching protocol that handles packet forwarding decisions based on the content of a label assigned to the packet. Label-based switching provides independence from the underlying data link layer protocol, allowing MPLS to carry traffic that uses different underlying structures and protocols, such as SONET frames, ATM frames, Ethernet frames, and IP packets. MPLS provides the basis for the following:

- Label-switched paths (LSPs).
- Virtual Leased Line (VLL) implementations.
- Virtual Private Line Services (VPLS).

For more information about MPLS, refer to your product's *Configuration Guide*.

Configuring LDP

LDP is configured from the Configuration wizard **Product Payload - LDP Settings** dialog box.

1. Select the **Set** option to set the selected settings in the product configuration. This creates a new configuration newly or overwrites the existing configuration. **Unset** removes the settings.

NOTE
To enable MPLS on the target devices, select the **Set** option then click **Add** and complete the wizard.

2. Select the checkboxes and enter the required information in the fields provided as follows:
   - **Advertise Labels ACL** - Enables the 64 character text field for entering an Access Control List (ACL) name.
   - **Hello Interval** - The interval in seconds between sending LDP hello messages. The range is 1-32767. The hello interval must be smaller than the hold time set by **Hello Timeout**.
   - **Use FEC 128 for autodiscovered peers** - FEC 129 is the default. FEC 128 applies only to VPLS environments that include both static-configured peers and auto-discovered peers.
   - **Hello Timeout** - This value represents the hold time value in seconds. The hold time is the amount of time that an MPLS interface waits to receive a hello message from its peers. If a hold time value is set per interface, that value is used. If not, the value received in hello messages from its peers is used. The range is 1-65535.
   - **Hello Timeout for Targeted Sessions** - For targeted sessions, the value received in hello messages from its peers determines the time that an MPLS interface waits for a peer to send a hello message. The range is 1-65535.
   - **Hello Interval for Targeted Sessions** - Interval between sending targeted Hellos. The range is 1-65535.
   - **Keepalive Count** - The number of keepalive intervals until a timeout.
   - **Keepalive Interval** - The interval between sending session keepalives.
   - **LDP Sessions** - Selecting the checkbox activates the **LDP Sessions** fields and buttons:
3. Click **Add** to adds a row to the **LDP Sessions** table.

   The **Edit** button allows you to edit a selected entry in the table.

   The **Delete** button allows you to delete a selected entry in the table.

LSP

The LSP allows you to manage RSVP LSPs and associated configurations such as Admin Groups and Paths. You can perform the following tasks from the LSP:

- View, add, edit, duplicate, or delete admin groups.
- View, add, edit, duplicate, or delete paths.
- View, add, edit, duplicate, or delete RSVP LSPs.
- View, add, edit, duplicate, or delete saved configurations.

An **LDP Configuration** button is provided in the LSP as a convenience to add LDP settings to the product payload if you are deploying LDP. Refer to "Configuring LDP" for a description of the procedure.

In addition to the topology information in the TED, the product considers attributes and requirements specified in configuration statements for the LSP. The LSP allows you to specify and adjust many of the parameters used when the product calculates a traffic-engineered path for a signalled LSP, including the following:

- An RSVP signalled LSP address for the egress LER.
- Explicit path to be used by the LSP.
- Bandwidth required by the LSP.
- Setup priority for the LSP.
- Metric for the LSP.
- Whether the LSP includes or excludes links belonging to specified administrative groups.

Viewing LSP Admin Group information

MPLS interfaces on an LSP can be organized into administrative groups (admin groups). LSP admin groups are typically used to manage CSPF path selection by including or excluding network segments identified as admin groups. Take the following steps to view LSP admin groups.

1. Select **Configure > MPLS > LSP**.
2. Select the **Admin Groups** tab (Figure 329).

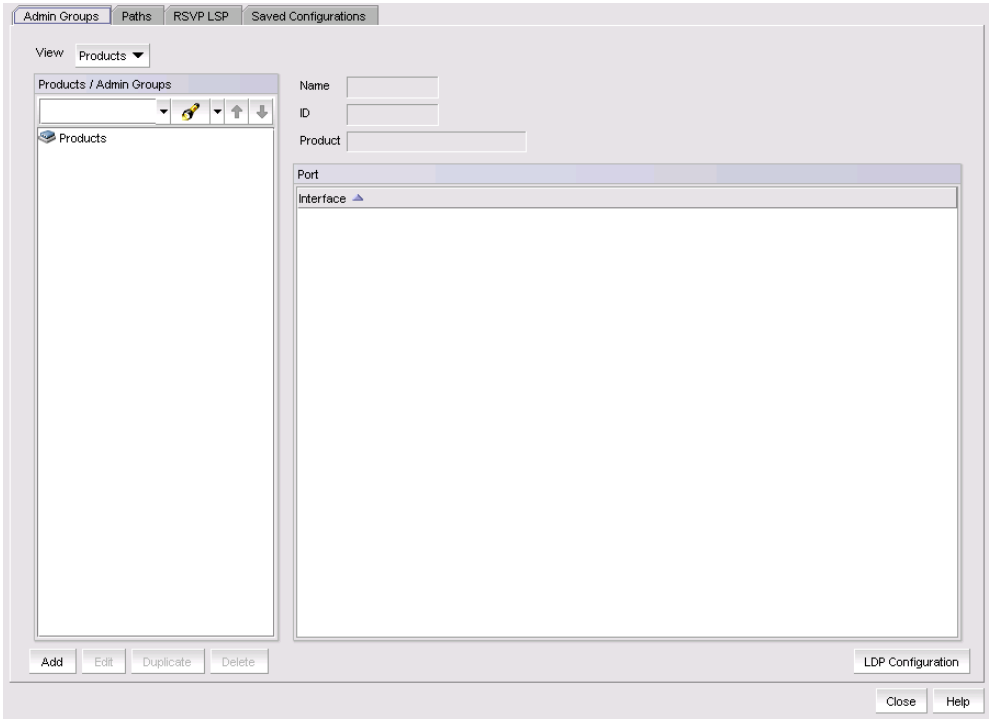


FIGURE 329 LSP dialog box, Admin Groups tab

3. Use the **View** selector to choose between displaying by **Product** or Admin Group **ID**.
   - **Product** - The product view shows a tree structure under **Products/Admin Groups** with products at the top level. Click the product name to expand the tree and display any associated admin groups.
   - **ID** - The ID view groups admin group instances by admin group ID. An admin group instance may be configured in multiple products, so the same product may be displayed under different admin group IDs.
4. Select a product or ID in the tree structure. The admin group name, ID, and product name display in the **Name**, **ID**, and **Product** fields, and the interfaces in the admin group display under **Ports**.

Viewing LSP path information

An LSP path is a list of router hops across an MPLS domain. Paths are configured separately from LSPs. This allows paths to be used by any LSP that knows the path name. Take the following steps to view LSP paths.

1. Select **Configure > MPLS > LSP**.
2. Select the **Paths** tab (Figure 330).

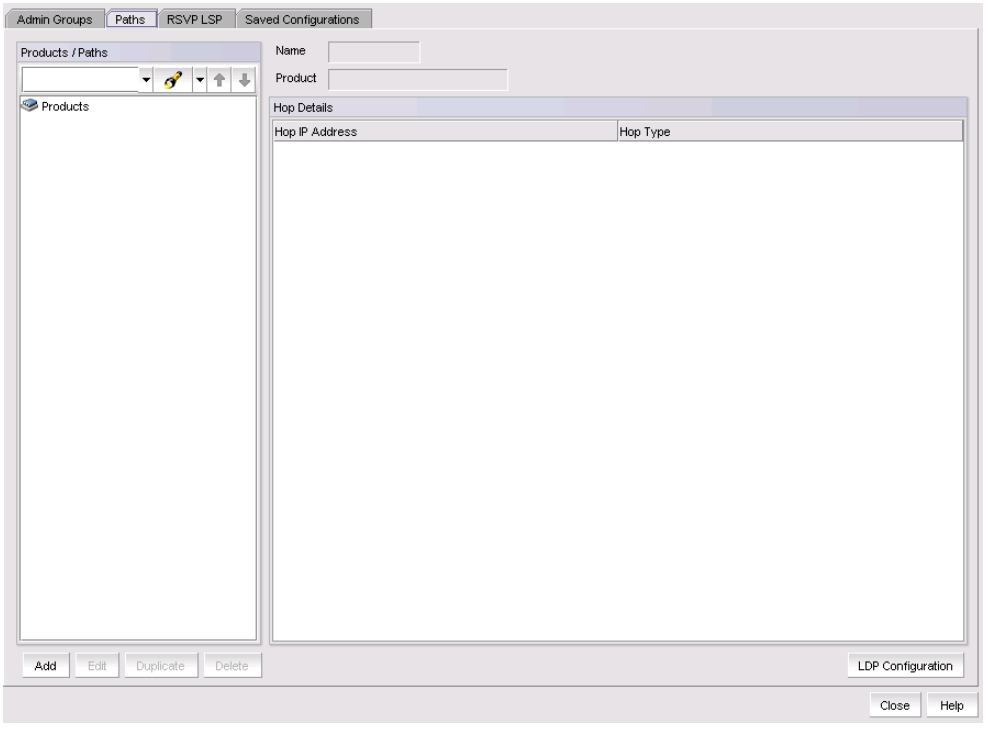


FIGURE 330 LSP dialog box, Paths tab

3. A tree structure displays under **Products/Paths** with products at the top level. Click the product name to expand the tree and display any associated paths.

4. Select a path to display the path name in the **Name** field, the Product name in the **Product** field, and the **Hop Details**. The **Hop Details** include the following:
   - **Hop IP Address** - The IP addresses for all the defined hops are listed.
   - **Hop Type** - Either **Strict** or **Loose**. Strict means that the node must be directly connected to the previous node on the **Hop Details** list. Loose, means that there may be one or more hops between the previous node on the **Hop Details** list.

Viewing RSVP LSP information

Resource Reservation Protocol (RSVP) controls signalling messages sent to each LSR in the LSP to reserve resources for traffic-engineered paths and cause labels to be dynamically associated with interfaces. Take the following steps to view RSVP LSP information.

The dialog box allows you to view a list of RSVP LSPs by product or by RSVP LSP name. You can also add, edit, duplicate, or delete RSVP LSPs, and launch the LDP Configuration wizard.

1. Select **Configure > MPLS > LSP**.
2. Select the **RSVP LSPs** tab (Figure 331).

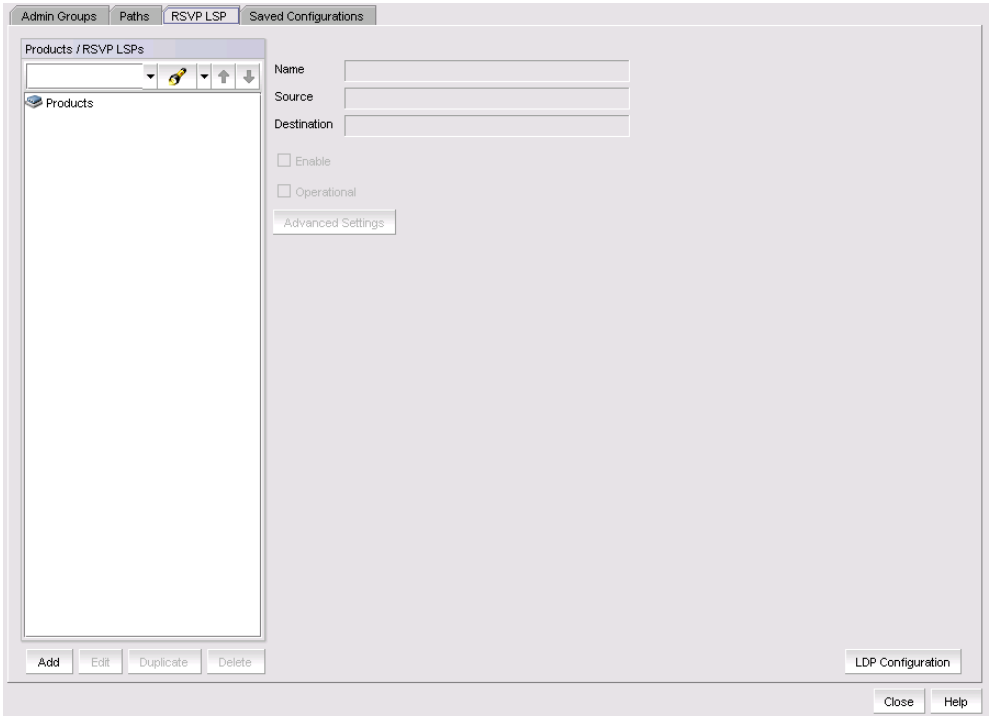


FIGURE 331 LSP dialog box, RSVP LSP tab

3. A tree structure displays under **Products/RSVP LSPs** with products at the top level. Click the product name to expand the tree and display all associated LSPs.
4. Select an LSP to display the LSP name in the **Name** field, the source product name (ingress LER) in the **Source** field, and destination product name (egress LER) the **Destination** field. Click the **Advanced Settings** button to view the **RSVP LSP Advanced Settings** dialog box (Figure 338).

   Refer to "Configuring advanced RSVP LSP settings" for a description of **Advanced Settings**.

5. Click **LDP Configuration** to launch the LDP configuration wizard.

Viewing saved LSP configurations

Take the following steps to view all saved LSP configurations.

1. Select **Configure > MPLS > LSP**.
2. Select the **Saved Configurations** tab (Figure 332).

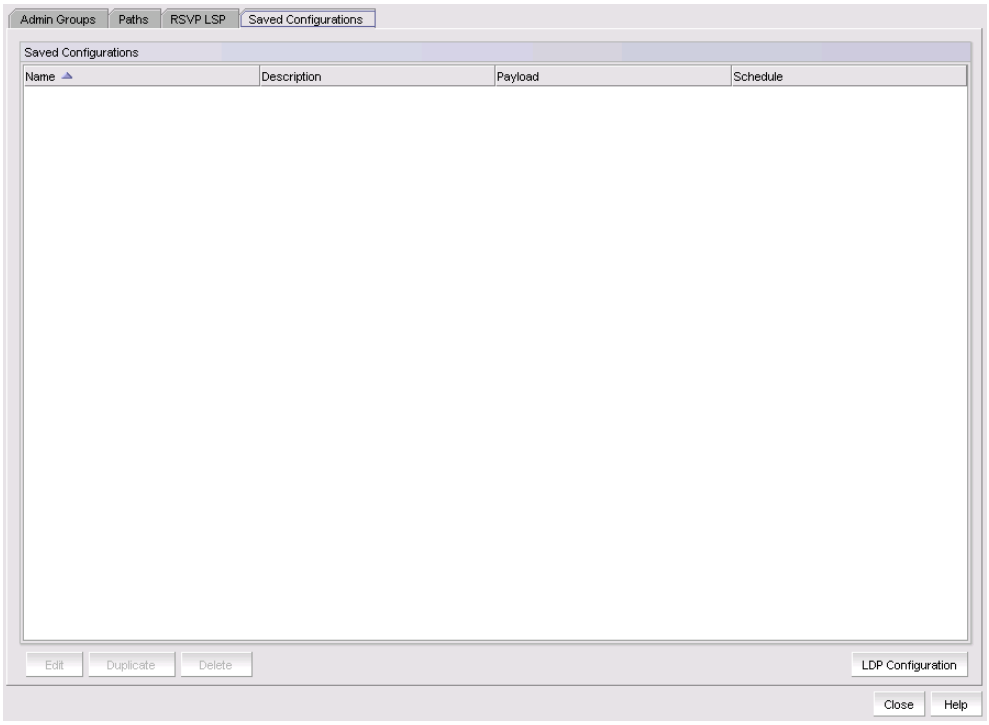


FIGURE 332 LSP dialog box, Saved Configurations tab

Saved LSP configurations are listed by name, description, payload, and deployment schedule.

Related topics

"MPLS overview"

"Configuring LDP"

Adding an LSP admin group

MPLS interfaces can be organized into administrative groups (admin groups). Typically, an admin group is used to identify a network segment. You can use admin groups to manage CSPF path selection by including or excluding network segments identified as admin groups. If you include an admin group, only those segments in that admin group are selected. If you exclude an admin group, that admin group is excluded from CSPF path selection.

Metrics can be associated with individual admin groups and applied on the particular segments. If you do not use include and exclude to manage admin groups, paths are selected based on the metrics associated with the individual admin groups.

This dialog box is the first page of the **Admin Group Configuration Wizard.** It allows you to provide a name and ID for the Admin Group and to assign the ports used as interfaces.

1. Select **Configure > MPLS > LSP**.
2. Select the **Admin Groups** tab.
3. Click the **Add** button.

   The **Admin Group Configuration** dialog box of the Admin Group Configuration wizard displays (Figure 333).

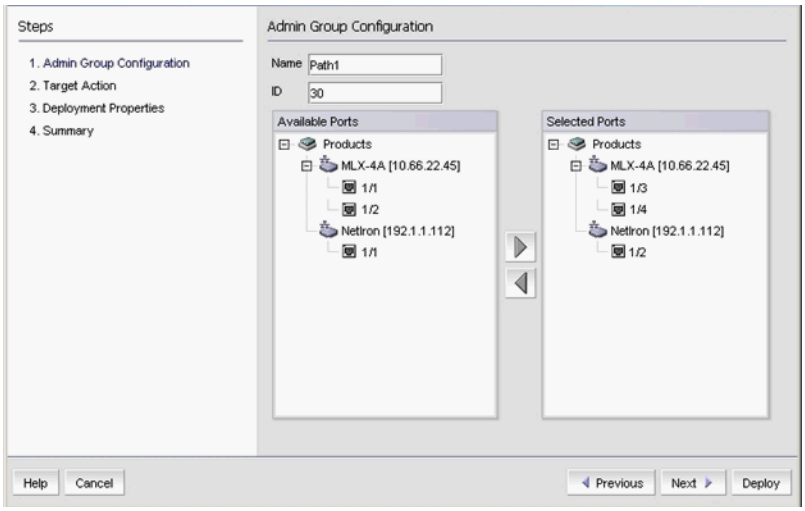


FIGURE 333 **Add Admin Groups Configuration dialog box, Configuration Info pane**

4. Enter an a name for the Admin Group in the **Name** field. A maximum of 32 ASCII characters is allowed.
5. Enter an Admin Group ID in the **ID** field. The ID must be an integer from 0 to 31.
6. Under **Available Ports**, select the ports you want to include in the admin group and click the right arrow button to move the ports to **Selected Ports**. Note that only those physical interfaces (ports) which have an IP address assigned are shown. All other interfaces are filtered out do not display.
7. If this is a one-time deployment and you don't want to save the admin group configuration to flash, click **Deploy**. If you want the configuration to persist, click **Next**.

   If you click **Next**, the **Persistence Properties** dialog box of the Admin Group Configuration wizard displays (Figure 334).

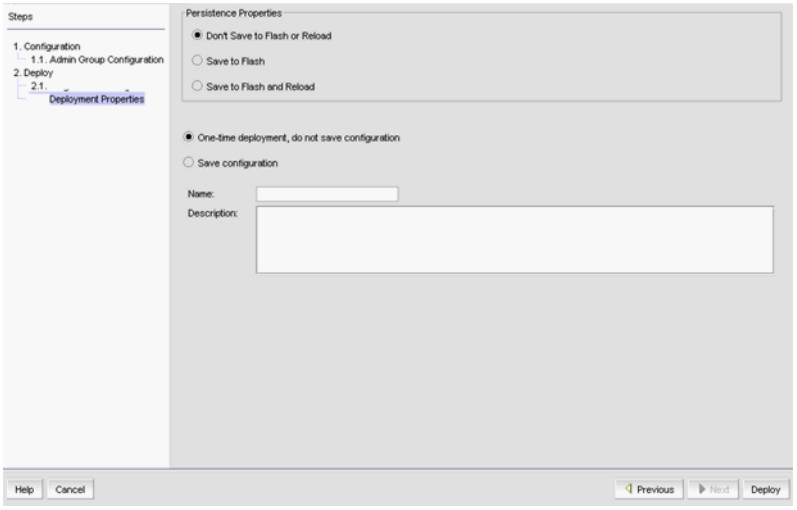


FIGURE 334 Add Admin Groups Configuration dialog box, Deployment Properties pane

8. Select the desired properties.
9. Click **Deploy**.

Editing an LSP admin group

You can edit an LSP admin group by taking the following steps.

1. Select **Configure > MPLS > LSP**.
2. Select the **Admin Groups** tab.
3. Select the admin group you want to edit.
4. Click the **Edit** button.

   The **Edit Admin Group Configuration** dialog box of the Admin Group Configuration wizard displays (Figure 333). Refer to "Adding an LSP admin group" for a description of how to use the Admin Group Configuration wizard.

Duplicating an LSP admin group

When you want to add a new LSP admin group, you can save work by duplicating an existing admin group and editing the name and any other parameters you may want to change. You can duplicate an LSP admin group by taking the following steps.

1. Select **Configure > MPLS > LSP**.
2. Select the **Admin Groups** tab.
3. Select the admin group you want to duplicate.
4. Click the **Duplicate** button.

   The **Copy Admin Group Configuration** dialog box of the Admin Group Configuration wizard displays (Figure 333). The **Name** field contains the name of the duplicated admin group with **_Copy** appended. Refer to "Adding an LSP admin group" for a description of how to use the Admin Group Configuration wizard.

Deleting an LSP admin group

You can delete an LSP admin group by taking the following steps.

1. Select **Configure > MPLS > LSP**.
2. Select the **Admin Groups** tab.
3. Select the admin group to be deleted.
4. Click the **Delete** button.

   The **Delete Admin Group Configuration** dialog box of the Admin Group Configuration wizard displays.
5. Click on a series of **Next** buttons to deploy.

Adding an LSP path

An LSP path is a list of router hops across an MPLS domain. Paths are configured separately from LSPs. This allows paths to be used by any LSP that knows the path name. An LSP always has a primary path and may have several secondary paths for redundancy.

Creating a path is not absolutely necessary when configuring an LSP. If you do not create a path, CSPF uses the information in the TED to calculate the path.

1. Select **Configure > MPLS > LSP**.
2. Select the **Paths** tab.
3. Click the **Add** button.

   The **Path Configuration** dialog box of the Path Configuration wizard displays (Figure 335).

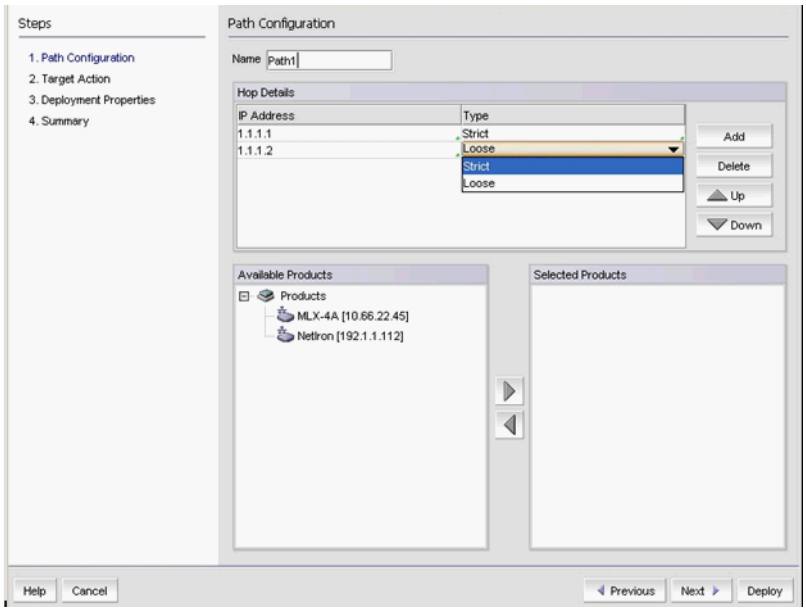


FIGURE 335 Path Configuration dialog box

4. Enter a name for the path in the **Name** field. A maximum of 32 ASCII characters is allowed.

5. Click the **Add** button. Use the **Up** and **Down** buttons to move the selected hop higher or lower in the table.

   An empty line is added under **Hop Details**. The first entry is always considered to be the local node and the Ingress LER. LER nodes should be then be added in order from Ingress to Egress. If you need to change the order, you can select an entry and use the **Up** and **Down** arrows to change its position. Actual routing depends on whether or not **Type** is set to **Strict** or **Loose**. This is described in step 7.

6. Enter the IP address for the hop under **IP Address**.

7. Under **Type**, select either **Strict** or **Loose**.

   If you choose **Strict**, the node must be directly connected to the previous node on the **Hop Details** list. If you choose **Loose**, you allow the possibility that there may be one or more hops between the previous node on the **Hop Details** list and the node you are adding to the list.

8. Under **Available Products**, select the product where you want the hop configured and click the right arrow to move the selected product to **Selected Products**.

   The **Available Products** list displays a filtered list of discovered products. To be included on the list, the products must meet the following requirements:

   - Ethernet routers
   - Ethernet Carrier and Edge routers running 5.1.00 must have the MPLS license enabled on the router.

9. Continue adding hops until the path is complete.

10. Click on a series of **Next** buttons to deploy.

11. Click **Deploy** to save and deploy the path definition.

Editing an LSP path

You can edit an LSP path by taking the following steps.

1. Select **Configure > MPLS > LSP**.

2. Select the **Paths** tab.

3. Select the path you want to edit.

4. Click the **Edit** button.

   The **Path Configuration** dialog box of the Path Configuration wizard displays (Figure 335). Refer to"Adding an LSP path" for a description of how to use the Path Configuration wizard.

Duplicating an LSP path

When you want to add a new LSP path, you can save work by duplicating an existing path and editing the name and any other parameters you may want to change. You can duplicate an LSP path by taking the following steps.

1. Select **Configure > MPLS > LSP**.
2. Select the **Paths** tab.
3. Select the path you want to duplicate.
4. Click the **Duplicate** button.

   The **Path Configuration** dialog box of the Path Configuration wizard displays (Figure 335). The **Name** field contains the name of the duplicated path with **_Copy** appended. Refer to"Adding an LSP path" for a description of how to use the Path Configuration wizard.

Deleting an LSP path

You can delete an LSP admin path by taking the following steps.

1. Select **Configure > MPLS > LSP**.
2. Select the **Paths** tab.
3. Select the path you want to delete.
4. Click the **Delete** button.

   The **LSP Delete Path Configuration** wizard displays (Figure 336).

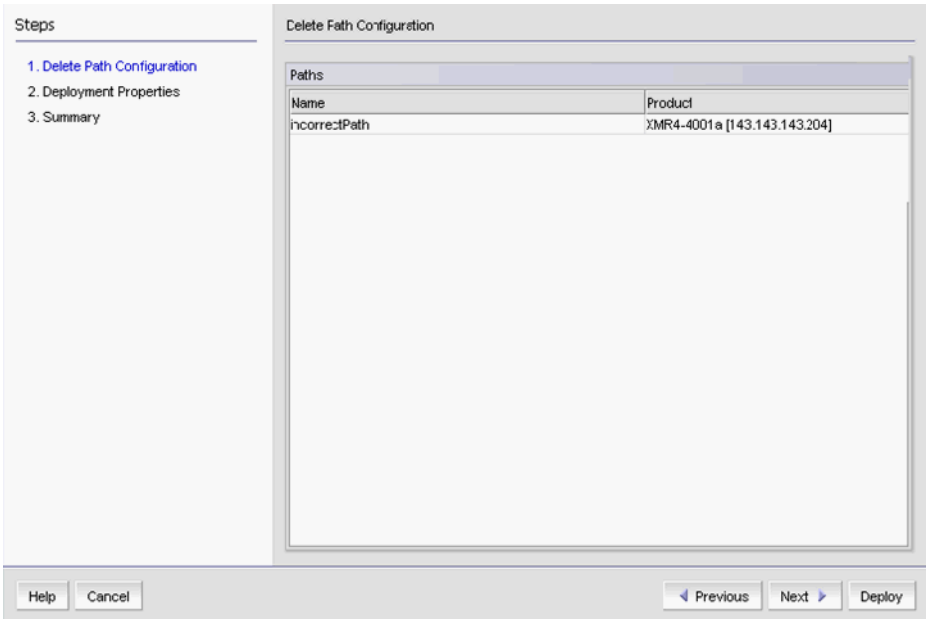


FIGURE 336 Delete Path Configuration wizard

5. Click on a series of **Next** buttons to deploy.

Configuring advanced RSVP LSP settings

Resource Reservation Protocol (RSVP) can be used to send signalling messages to each LSR in the LSP to reserve resources and cause labels to be dynamically associated with interfaces. This enables you to engineer network traffic routing to avoid points of congestion and make efficient use of high bandwidth interfaces.

Two separate protocols are needed to perform this task:

- Routing protocol - The routing protocol distributes network topology information through the network so that the route of an LSP can be calculated automatically.
- Signaling protocol- The signaling protocol informs the switches along the route which labels and links to use for each LSP.

1. Select **Configure > MPLS > LSP**.
2. Select the **RSVP LSP** tab.
3. Click the **Add** button.

   The **RSVP LSP Configuration** dialog box of the RSVP LSP Configuration wizard displays (Figure 337).

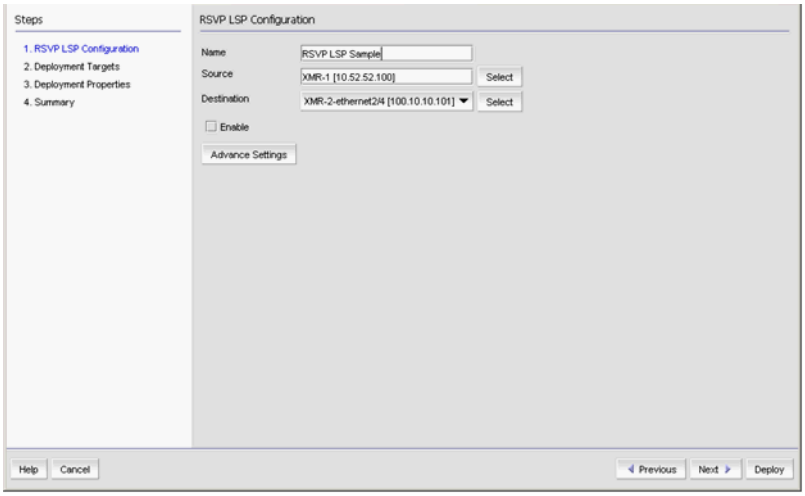


FIGURE 337 RSVP LSP Configuration dialog box

4. Enter a name for the configuration in the **Name** field. A maximum of 32 ASCII characters is allowed.
5. Click the **Select** button and select the source product from the listed products.
6. Click the **Select** button and select the destination product from the listed products.

   The destination product's loopback interface is used as the 'destination IP address'.

7. **Enable** is pre-selected to automatically enable LSP configuration when it is deployed. If want the LSP configuration to be disabled when it is deployed, clear this check box.

8. Click **Advanced Settings** to establish traffic engineering parameters.

   The **RSVP LSP Advanced Settings** dialog box has three tabs: **Global**, **Paths**, and **Fast Reroute**. The default view is the **Global** tab (Figure 338).

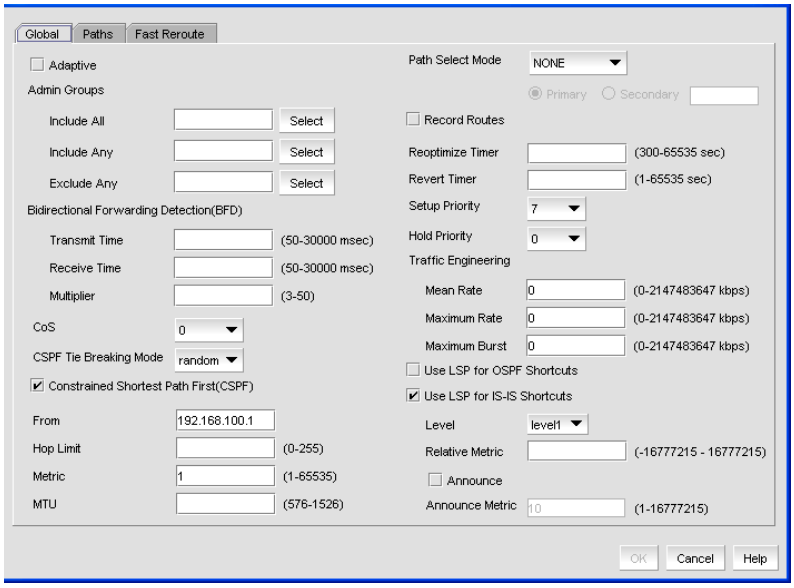


FIGURE 338 RSVP LSP Advanced Settings Global tab

From the **Global** tab you can set the following:

- **Adaptive** checkbox - Select the **Adaptive** checkbox to allow you to change parameters while an LSP is in enabled state.
- Under **Admin Groups** settings use the **Select** buttons to use admin groups to manage CSPF path selection by including or excluding network segments identified as admin groups. The **Admin Groups Selector** dialog box displays (Figure 339).

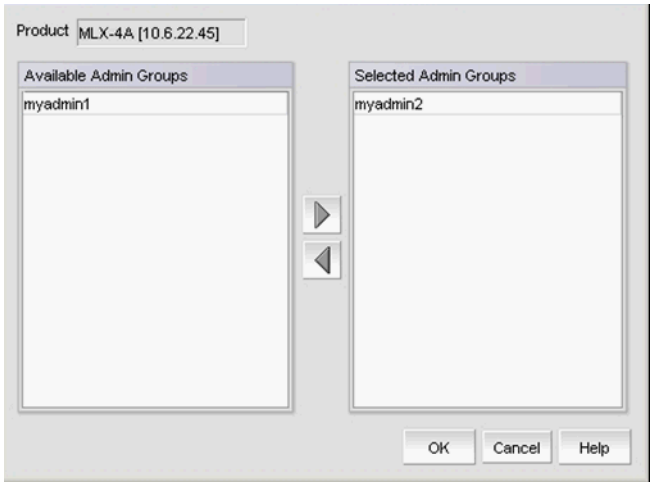


FIGURE 339 Admin Groups Selector dialog box

You can place selected admin groups into any of the following categories:

- **Include All** - An interface must be a member of all selected groups.
- **Include Any** - An interface is included if it is a member of any of the selected groups.
- **Exclude All** - Interfaces in the selected groups are excluded.

- **Bidirectional Forwarding Detection (BFD)** check box - This check box allows you to enable or disable BFD. If you enable BFD, the following parameters need to be specified:
  - **Transmit Time** - The interval in seconds between BFD messages sent by this router to its peers indicating that it is still operational. The allowable range is shown on the dialog box.
  - **Receive Time** - The interval in seconds that this router will wait for a BFD messages sent by its peers. The allowable range is shown on the dialog box. This value is used with the **Multiplier** value to determine when a peer is no longer considered operational.
  - **Multiplier** - The number of times that this router will wait to receive a message before a peer is no longer considered operational. The actual time the router will wait is equal to (**Receive Time**) X (**Multiplier**). The allowable range is shown on the dialog box.
- **CoS** - Assigns a layer two class of service to the LSP. A value of 7 is the highest priority, and a value of 0 is the lowest priority. Select None to remove any current CoS setting.
- **CSPF Tie Breaking Mode** - It is possible that CSPF may calculate multiple equal cost paths between an ingress LER and an egress LER. For that case, you can choose a tie breaking mode to determine which path is used. The choices for tie breaking mode are as follows:
  - **Least Fill** - The path that is least used.
  - **Most Fill** - The path that is most used.
  - **Random** - A random choice is made between the equal cost paths.
- **Constrained Shortest Path First (CSPF)** - Select this check box if you want the ingress LER to use CSPF to calculate a traffic-engineered path between the ingress and egress LERs. CSPF uses the configured attributes of the LSP and information in the Traffic Engineering Database (TED) to calculate the path.
  - **From** - In situations where you want additional control over the path, you can specify an interface address in the **From** field. In this case, the path calculation resolves to the actual interface rather than the router ID when configuring a hop.
  - **Hop Limit** - If you want CSPF to use a hop limit when choosing a path, enter the number of hops in the **Hop Limit** field. The range is 0-255. If no hop limit is specified, a hope limit of 255 is assumed.
- **Metric** - You can assign a metric to an LSP to establish a preference/priority scheme for LSP usage. The metric is expressed an integer. The range is as shown on the dialog box. The lower the number, the higher the preference. An LSP with a metric of 1 will be used before an LSP with a metric of 2. By default, all LSPs are assigned a metric of 1.
- **MTU** - Sets the maximum transmission unit (MTU) size in bytes for packets traversing the LSP. The range is displayed on the dialog box.

- **Path Select Mode** - The choices are **Manual** and **Unconditional**. If Manual is chosen, traffic is shifted to an alternate path only if the selected path fails. If the path recovers, traffic is shifted back. If Unconditional is chosen, the traffic stays on the selected path even if the path fails. If you do not want to specify a path select mode or want to remove the configured path select mode, select **None**.
  - **Primary** - Selected by default.
  - **Secondary** - Activated if a **Path Selection Mode** other than **None** is selected. To define a secondary path, enter the secondary path name in the **Secondary** field.
- **Record Routes** - Select this checkbox to record LSP path information so that it can be displayed.
- **Reoptimize Timer** - The re-optimize timer is a periodic timer for triggering the activation of all pending LSP configuration changes.
- **Revert Timer** - The revert timer allows a period of time to elapse after a failback to a primary path. This allows some time for conditions on a path to stabilize and prevents unnecessary repetitive failover/failbacks that might occur if a path goes up and down frequently.
- **Setup Priority** - The setup priority is used in concert with **Hold Priority** to determine priority for an LSP at the ingress LER. The setup priority determines priority when several LSPs are enabled at the same time, as is the case at start-up or after a re-boot. The setup priority is also used in concert with the **Mean Rate** to determine if there is enough reservable bandwidth available on an interface to allow the LSP to be activated.
- **Hold Priority** - The hold priority can be used to prevent an operating LSP from giving up resources to an LSP with a higher setup priority. Both the setup and hold priorities allow values from 0 to 7, with 0 as the highest priority and 7 as the lowest. To be useful, the hold priority needs to equal to or less than the setup priority. For example, assume you have two LSPs with a setup priority of 2 and a hold priority of 1. If either LSP should be interrupted by a re-boot, the hold priority would prevent shifting of resources because the setup priority is lower. The hold priority is also used in concert with the **Mean Rate** to allocate reservable bandwidth to an LSP.
- **Traffic Engineering** - The following settings determine the bandwidth requirements for an LSP:
  - **Mean Rate** - Sets the average data rate supported. **Mean Rate** is used in concert with **Hold Priority** in allocating reservable bandwidth for an LSP. As LSPs are activated, bandwidth is allocated to meet their mean rate requirements. As bandwidth is allocated, the amount of reservable bandwidth available is correspondingly reduced. The LSP's hold priority is used to conserve the use of the remaining bandwidth. available bandwidth is adjusted downward for lower priority LSPs to ensure that bandwidth remains available higher priority LSPs. If the mean rate for a given priority becomes higher than the bandwidth available for that priority, that LSP is preempted and the bandwidth is made available to LSPs with a higher hold priority.

    Mean Rate is also used with **Setup Priority** in determining if there is enough reservable bandwidth available to allow an LSP to be activated. In this case as bandwidth is allocated and the amount of reservable bandwidth available is correspondingly reduced, there may not be enough bandwidth available to meet the mean rate requirements for an LSP with a low setup priority.

- **Maximum Rate** - Sets the maximum data rate supported for data bursts above the mean rate.
- **Maximum Burst** - Sets the maximum number of bytes that can be handled at the maximum rate.

- **Use LSP for OSPF shortcuts** - Enables the use of traffic engineering data carried in OSPF extensions that contain information about the interface's metric, bandwidth reservations, and admin group memberships.
- **Use LSP for IS-IS shortcuts** - Enables you to configure the IS-IS shortcut parameters. This setting allows you to configure the target product to send out IS-IS TE packets for all of its MPLS-enabled interfaces.

  When an MPLS-enabled product receives an IS-IS TE packet, it stores the traffic engineering information in its Traffic Engineering database (TED). The product then uses information in the TED when performing calculations to determine a path for an LSP.

  - **Level** — Select a level (level1 or level2) for the LSP.
  - **Relative Metric** — Enter a relative metric (-16777215 through 16777215) for the LSP.
  - **Announce** check box — Select to enable announce for the LSP. The default is 10.
  - **Announce Metric** — Only available when you select the **Announce** check box. Enter an announce metric (1 through 16777215) for the LSP.

9. Select the **Paths** tab (Figure 340).

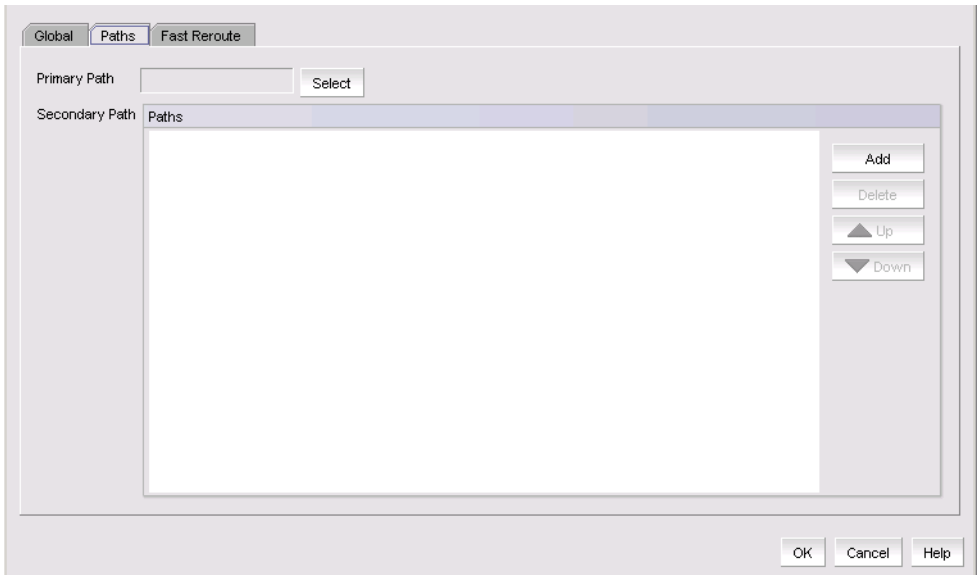


FIGURE 340 RSVP LSP Advanced Settings Paths tab

From the **Paths** tab you can configure primary and secondary paths for the LSP.

a. Use the **Primary Path Select** button to display the **Path Selector** dialog box (Figure 341).

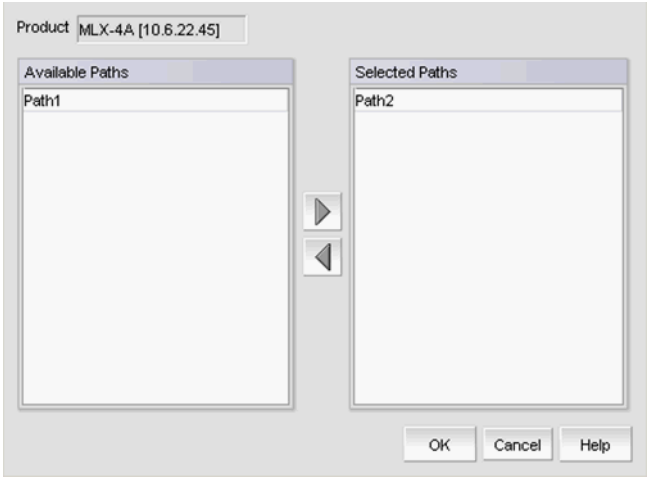


FIGURE 341 Path Selector dialog box

b. Select the path you want to use as the primary path from **Available Paths**, and use the right arrow to move the path to **Selected Paths**.

c. Click **OK**.

Secondary paths for the LSP are listed under **Paths**. Use the **Add** and **Delete** buttons to add or delete a secondary path. Use the up and down arrows to move entries up and down in the table.

10. Select the **Fast Reroute** tab (Figure 342).

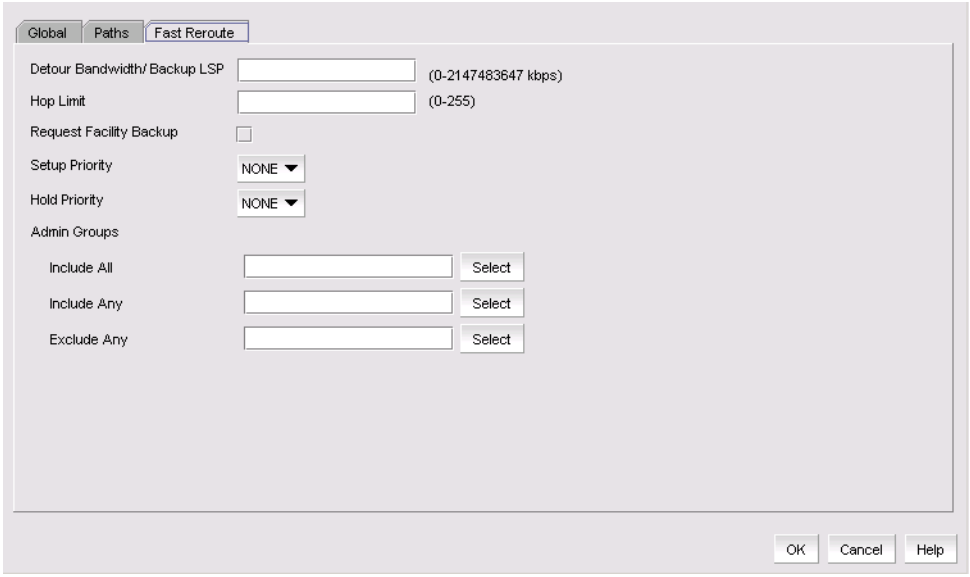


FIGURE 342 RSVP LSP Advanced Settings Fast Reroute tab

From the **Fast Reroute** tab you can configure an LSP to request a facility backup provided by a bypass LSP in the event of a failure along the LSP path. Each LSR in an LSP except the egress router may act as a Point of Local Repair (PLR). If a failure occurs on an LSP, the PLR tries to initiate a bypass LSP to provide a backup route for the protected path. The PLR then becomes the ingress of a bypass LSP. The bypass LSP carries the traffic of the LSPs it protects around the break. The point past the break where traffic re-enters is called the merge point.

In Figure 343, R2 is the PLR. The double line that originates at R2 and then traverses R6 and R7 to terminate at R4 is the bypass LSP. The bypass LSP terminates in R4 and traffic merges back into the protected LSPs. This router is the merge point and the egress router for the bypass LSP.

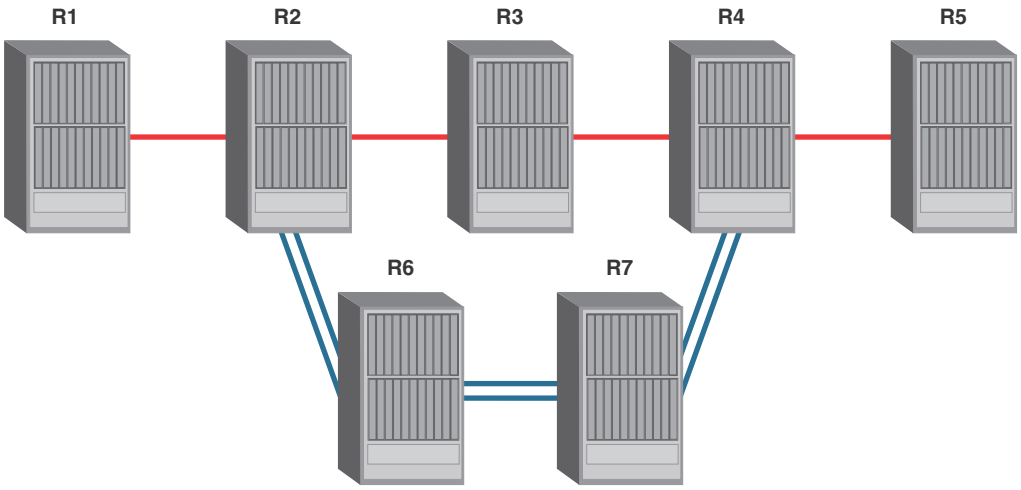


FIGURE 343 Bypass LSP

When you use fast reroute to request a facility backup, the characteristics of the backup LSP should match well with the LSP that is requesting the facility backup:

- The value specified in the **Detour Bandwidth/Backup LSP** and the **Hop Limit** fields should be the same as the requesting LSP.
- Select the **Request Facility Backup** checkbox to enable the facility backup request.
- **Setup Priority** and **Hold Priority** should be the same as the requesting LSP.
- Admin group **Include All**, **Include Any**, and **Exclude Any** selections should be the same as the requesting LSP. Use the **Select** buttons to display the **Admin Groups Selector** dialog box (Figure 339).

Editing an RSVP LSP

You can edit an RSVP LSP by taking the following steps.

1. Select **Configure > MPLS > LSP**.
2. Select the **RSVP LSP** tab.
3. Select the RSVP LSP you want to edit.
4. Click the **Edit** button.

   The **RSVP LSP Configuration** dialog box of the RSVP LSP Configuration wizard displays (Figure 337). Refer to "Configuring advanced RSVP LSP settings" for a description of how to use the RSVP LSP Configuration wizard.

Duplicating an RSVP LSP

When you want to add a new RSVP LSP, you can save work by duplicating an existing RSVP LSP and editing the name and any other parameters you may want to change. You can duplicate an RSVP LSP by taking the following steps.

1. Select **Configure > MPLS > LSP**.
2. Select the **RSVP LSP** tab.
3. Select the RSVP LSP you want to duplicate.
4. Click the **Duplicate** button.

   The **RSVP LSP Configuration** dialog box of the RSVP LSP Configuration wizard displays (Figure 337). **Name** field contains the name of the duplicated RSVP LSP with **_Copy** appended. Refer to "Configuring advanced RSVP LSP settings" for a description of how to use the RSVP LSP Configuration wizard.

Deleting an RSVP LSP

You can delete an RSVP LSP by taking the following steps.

1. Select **Configure > MPLS > LSP**.
2. Select the **RSVP LSP** tab.
3. Select the RSVP LSP you want to delete.
4. Click the **Delete** button.

   The **Delete RSVP LSP Configuration** wizard displays (Figure 344).

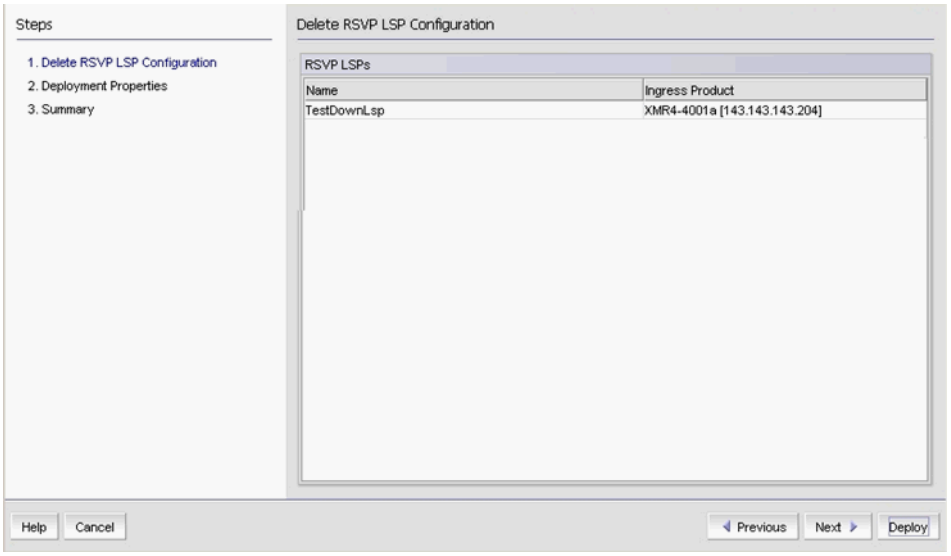


FIGURE 344 Delete RSVP Configuration wizard

5. Click a series of **Next** buttons to deploy the payload.

Editing a saved LSP configuration

You can edit a saved LSP configuration by taking the following steps.

1. Select **Configure > MPLS > LSP**.
2. Select the **Saved Configuration** tab.
3. Select the saved configuration
4. Click the **Edit** button.

Duplicating a saved LSP configuration

When you want to add a new LSP configuration, you can save work by duplicating an existing configuration and editing the name and any other parameters you may want to change. You can duplicate an LSP configuration by taking the following steps.

1. Select **Configure > MPLS > LSP**.
2. Select the **Saved Configuration** tab.
3. Select the saved configuration
4. Click the **Duplicate** button.

Deleting a saved LSP configuration

You can delete a saved LSP configuration by taking the following steps.

1. Select **Configure > MPLS > LSP**.
2. Select the **Saved Configuration** tab.
3. Select the saved configuration
4. Click the **Delete** button.

Displaying LSP Topologies

Refer to the View Management chapter for descriptions for topology map layout options and navigation aids.

You can display topology maps for configured LDP and RSVP LSPs by taking the following steps.

1. Select **Monitor > MPLS > LSP Topology**.

   The **LSP Topology View** displays (Figure 345).

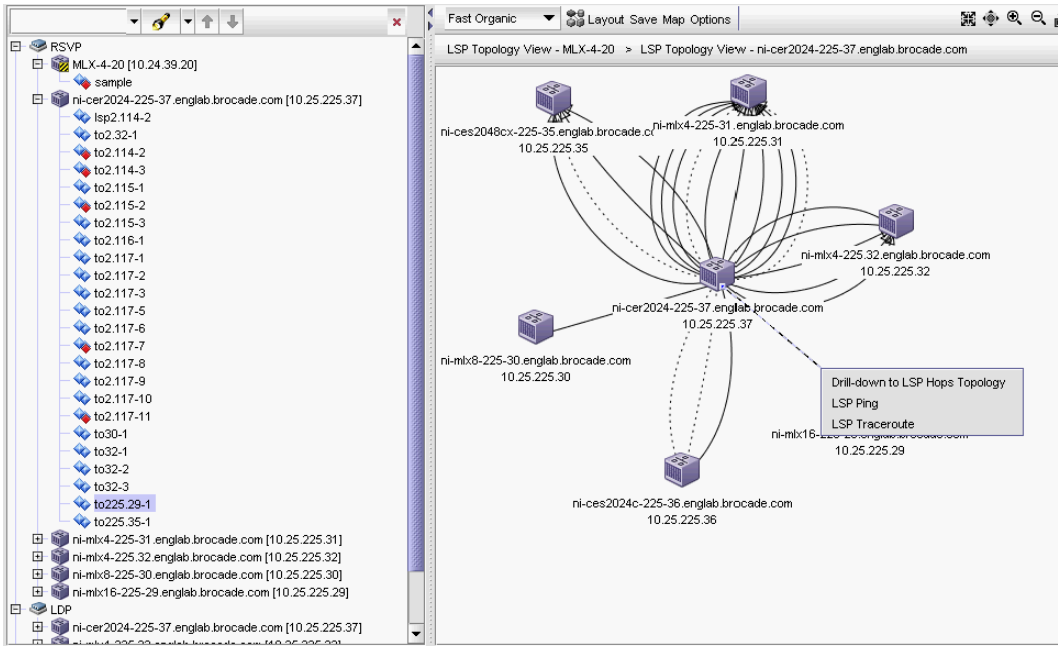


FIGURE 345 LSP Topology View

2. You can select any of several options to gather information.
   - The tree structure has folders for RSVP LSPs, LDP LSPs, and products without LSP configurations. Selecting an RSVP LSP in the tree highlights the corresponding LSP in the topology view.
   - Hovering over a link on the topology view shows the LSP name as a tooltip.
   - Double-clicking the product shows all LSPs originating from the product.
3. If you would like to filter the display, use the **Options** selector in the tool bar to launch the **LSP Topology View Options** dialog box (Figure 347).

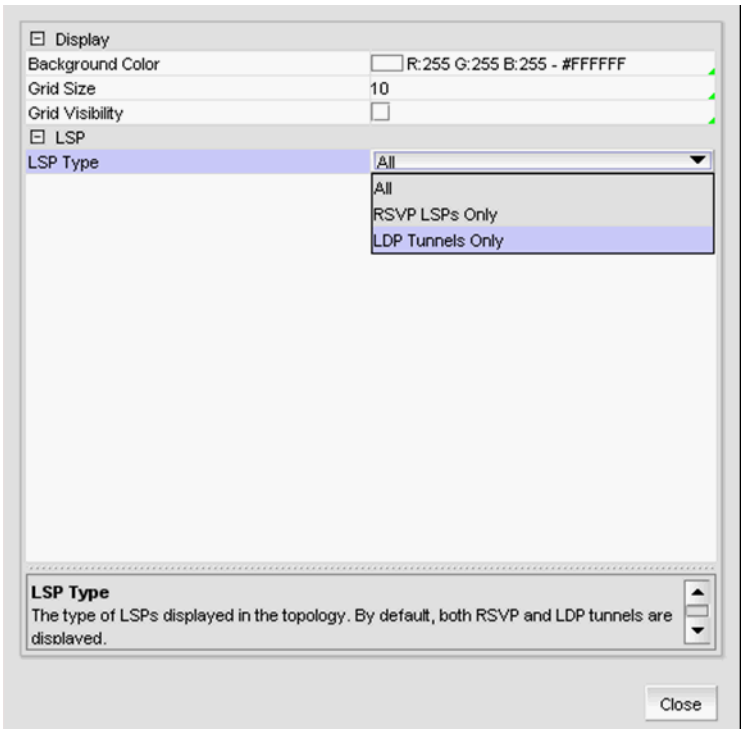


FIGURE 346 LSP Topology View Options

4. Use the **LSP Type** selector to limit the display to **RSVP LSPs Only** or **LDP Tunnels Only**.

   If you right-click on an LSP, three options are displayed (Figure 347).

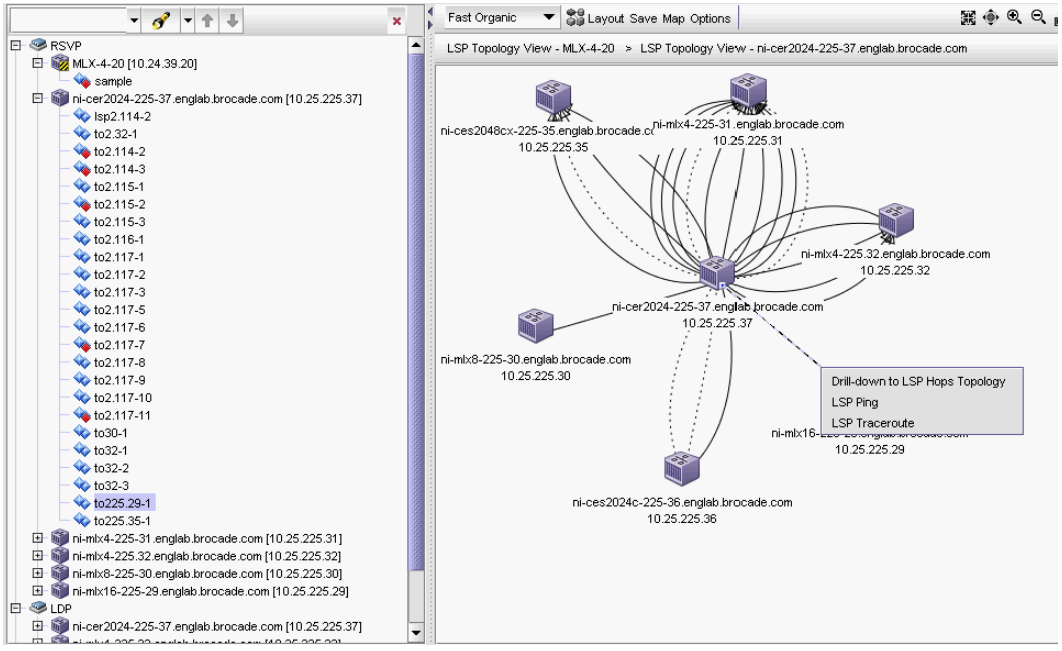


FIGURE 347 LSP right-click options on the Topology View

- Select **Drill-down to LSP Hops Topology** to display LSPs and hops as a line from the ingress router with an arrow to indicate direction. Operationally enabled LSPs are shown with a solid line. Operationally disabled LSPs are shown with a dotted line.
- Select **LSP Ping** to launch the **LSP Ping** dialog box.
- Select **LSP Traceroute** to launch the **LSP Trace Route** dialog box.

MPLS Virtual Leased Line (VLL) overview

MPLS VLL provides point-to-point Ethernet or VLAN connectivity over an MPLS domain. VLL is also known as Pseudo-Wire emulation. Figure 348 illustrates a basic VLL configuration.

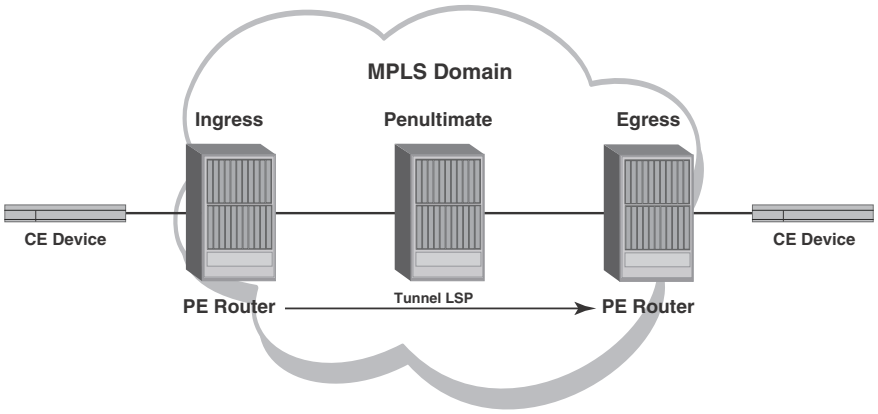


FIGURE 348 Basic VLL configuration

Packets are forwarded over an MPLS VLL as described below.

1. A Customer Edge (CE) product forwards a packet to an LER serving as a Provider Edge (PE) router at the edge of the MPLS domain.
2. The PE router assigns the packet to an RSVP-signalled LSP whose destination is an LER (also serving as a PE router) that is connected to a CE product at the far end of the MPLS domain. The PE router at the other end of the MPLS domain is known as this PE router's ***VLL peer***. The RSVP-signalled LSP used to reach the VLL peer is known as the ***tunnel LSP***. Alternatively, an LDP-signalled, tunneled LSP can be used.

   If a Class of Service (COS) value is set for the VLL, the product selects a tunnel LSP that also has this COS value, if one is available. If no tunnel LSP with this COS value is available, the product selects a tunnel LSP with the highest configured COS value (although never higher than the COS setting for the VLL).

   If there are multiple tunnel LSPs that can be used to reach the VLL peer, the PE router selects one of the tunnel LSPs by using a round-robin method.

The PE router pushes two labels onto the packet:

- The inner ***VC label*** is used for determining what happens to the packet once it reaches the VLL peer. This label is significant only to the VLL peer.
- The outer ***tunnel label*** is used for forwarding the packet through the MPLS domain. This label corresponds to an RSVP-signalled tunnel LSP.

After applying the two labels to the packet, the PE router forwards it to the next LSR in the tunnel LSP.

3. The penultimate LSR in the tunnel LSP removes the tunnel label and forwards the packet (now with the VC label as the top label) to the PE router at the other edge of the MPLS domain.
4. The VLL peer at the egress of the tunnel LSP examines the VC label. This VC label is mapped to an ***endpoint*** for the VLL. The endpoint of a VLL specifies what happens to packets exiting the VLL.

   The endpoint can specify either an untagged port or a tagged port. For untagged ports, the endpoint consists of an interface. For tagged ports, the endpoint consists of an interface and the Outer VLAN ID and Inner VLAN ID. The egress LER removes the VC label and forwards the packet out the interface specified as the endpoint. If the endpoint is a tagged port, the product transmits the packet with the specified VLAN ID, forwarding it out the specified interface to the CE product.

The two VLL peers advertise VC labels to each other using the ***Label Distribution Protocol (LDP)***. Each PE router attempts to initiate an LDP session with its VLL peer. After the LDP session is established, the locally assigned VC label, along with a VLL VC ID, is advertised to the VLL peer. In a similar way, the PE also learns the remotely assigned VC label from the VLL peer. Alternatively, you can configure static local and remote VC labels manually on both VLL peers; in this case, LDP is not used.

NOTE
If MTUs are mismatched on both sides of a VLL session, the session does not come up.

VLL manager

The VLL Manager allows you to manage VLL instances. You can perform the following tasks from the VLL manager:

- View current VLL instances.
- View VLL configurations.
- Add, edit, duplicate, or delete VLL instances.

NOTE
When configuring a VLL, a check is made to determine if there are LSPs configured for the target products. You may proceed with configuration, but an LSP is needed for a working connection.

Viewing VLL instances

To view currently defined VLL instances, do the following:

1. Select **Configure > MPLS > VLL**.
2. Select the VLL Manager **Views** tab (Figure 349).

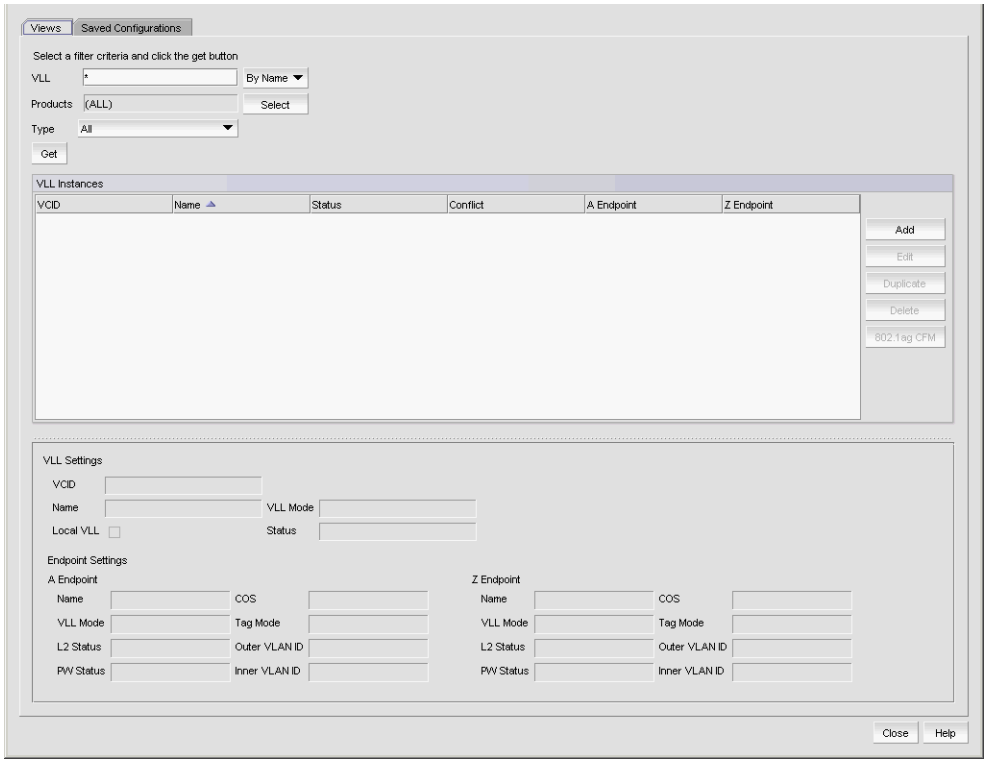


FIGURE 349 VLL Manager Views tab

3. You can filter output by name or by VCID by using the selector next to the VLL field.
   - You can use an Asterisk (*), as a wildcard character if you select **By Name**.
   - You can enter individual VCIDs or a range of VCIDs if you select **By VCID**.

   NOTE
   If you choose **By VCID** you can search only for remote VLLs (VLLs whose endpoints are on two different products), but not for local VLLs (VLLs whose endpoints are on the same product).

4. Enter a product name or click the **Select** button to launch the **Select Products** dialog box to select a product.
5. Select **Type** to filter VLLs by type. The choices are **All** (all VLLS matching the name or VCID criteria), **Local-VLL**, and **Remote VLL**.
6. Click the **Get** button to begin the search for the VLL name.

   VLLs that match the filter criteria display under **VLL Settings** and **Endpoint Settings**.

   The table shows the following information:

   - VCID of the VLL. This cell is blank for a local VLL.
   - Name of the VLL.
   - Status of the VLL:
     - All peers are up
     - All peers are down
     - Some peers are down
     - Undefined
   - Conflict - Indicates if there are conflicts with VLL endpoint instances. Conflicts can arise, especially with VLLs configured using the product CLI. If there are conflicts, this column also indicates they type of conflict that exists:
     - Name mismatch - Name of the VLL in the two products are not the same
     - No endpoint - The VLL has no endpoint defined
     - Duplicate VCID - Another VLL is using the VCID
     - Peer is missing - A VLL peer is missing
     - VLL mode mismatch - VLL mode type between the two products are not the same
   - A Endpoint - The first endpoint of the VLL. It displays the product name, IP address where the endpoint is configured, and the port name.
   - Z Endpoint - The second endpoint of the VLL. It displays the product name, IP address where the endpoint is configured, and the port name.

7. Select a row in the table to display details for the selected VLL in the **Details** area.

   VLL settings display the following information about a selected VLL in the fields below:

   - **Name** - The name of the VLL.
   - **VLL Mode** -
   - **Tagged**: A VLAN ID tag is added to the packets on the ingress router. When the packet arrives at the egress router, the tag is stripped off and the packet is forwarded.
   - **Raw**: The ingress router does not add a VLAN ID to the packets.
   - **Local VLL** - Both VLL endpoints are on the same device.
   - **Status** -

- All peers are up.
- All peers are down.
- Some peers are down.
- **VCID** - The VCID of the VLL.

Endpoint Settings display the following information about the A Endpoint and Z Endpoint of the selected VLL in the fields below:

- **Name** - The endpoint device name and IP address.
- **COS** - Class of Service associated with the endpoint.
- **VLL Mode** -
- **Tagged**: A VLAN ID tag is added to the packets on the ingress router. When the packet arrives at the egress router, the tag is stripped off and the packet is forwarded.
- **Raw**: The ingress router does not add a VLAN ID to the packets.
- **Tag Mode** -
- **Tagged**: If the endpoint is a tagged port, the device transmits the packet with the specified VLAN ID and forwards it out the specified interface.
- **Untagged**: If the endpoint is an untagged port, the device removes any VLAN ID before transmitting it out the specified interface.
- **L2 Status** - Layer 2 status (Up or Down).
- **Outer VLAN ID** - Present if the Tag Mode for the endpoint is Tagged. The service provider end point tag.
- **Inner VLAN ID** - Present if the Tag Mode for the endpoint is Tagged. The customer end point tag.

8. Right click any entry in the table to display the Print pop up menu. Select Print from the menu to print the table.

Viewing Saved VLL configurations

To view current saved VLL configurations, do the following:

1. Select **Configure > MPLS > VLL.**
2. Select the **Saved Configurations** tab (Figure 350).

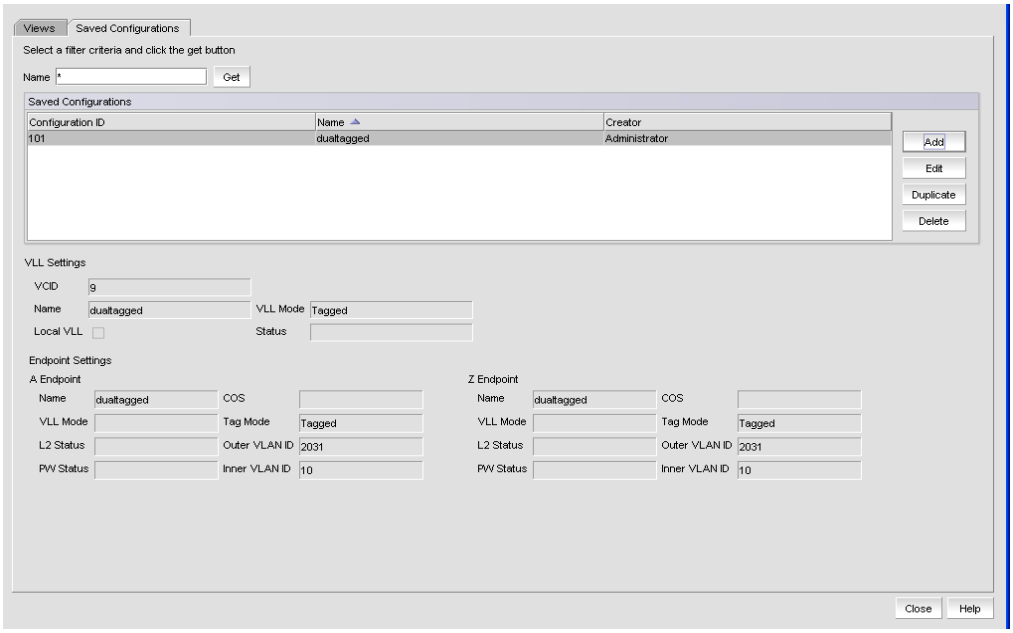


FIGURE 350 VLL Manager Saved Configurations tab

3. You can use the **Name** field to filter output by configuration name. You can use an Asterisk (*) as a wild card character.
4. Click the **Get** button to begin the search.

   Configurations that match the filter criteria display under **Saved Configurations**, showing the configuration ID, the configuration name, and the RBAC user name that created the configuration.
5. When you select a configuration, the following information displays in the fields below **Saved Configurations**:
6. Right click any entry in the table to display the Print pop up menu. Select Print from the menu to print the table.

Adding or editing a VLL instance

To add a new VLL instance do the following:

1. Select **Configure > MPLS > VLL**.
2. Select either the **Views** tab or the **Saved Configurations** tab.
3. Click the **Add** button.

   The VLL Configuration wizard **Target Selector** dialog box displays (Figure 351).

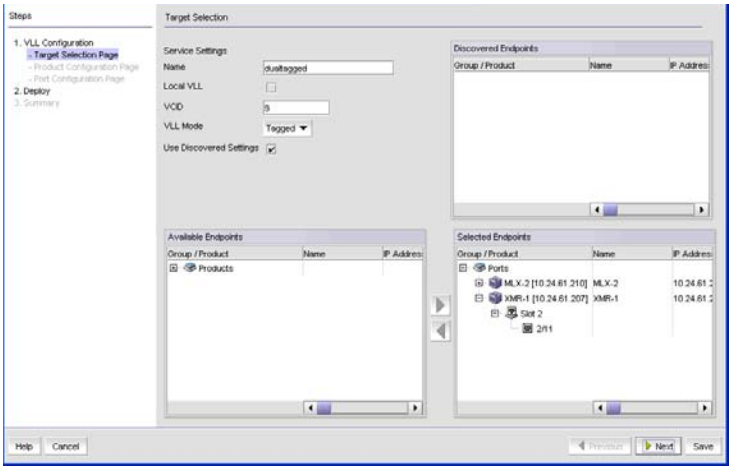


FIGURE 351 VLL Manager Target Selector dialog box

4. Enter a name for the endpoint in the **Name** field. The name must be unique on each product and cannot contain spaces, asterisks (*), or question marks (?).
5. Select the **Local VLL** check mark box if both VLL endpoints are on the same product.
6. If you want to use a specific VCID, enter the VCID. If you do not specify a VCID, the next available VCID in the VCID pool is assigned.
7. VLL Mode is disabled if the **Local VLL** check mark box is selected indicating that both VLL endpoints are on the same product. If the VLL endpoint is on different product (a remote VLL), use the **VLL Mode** selector to choose one of the following for the endpoint:
   - **Tagged**: A VLAN ID tag is added to the packets on the ingress router. When the packet arrives at the egress router, the tag is stripped off and the packet is forwarded.
   - **Raw**: The ingress router does not add a VLAN ID to the packets.
8. If you want to copy the VLL configurations for one or more products or ports under **Discovered Endpoints**, select the product or port and then select the **Use Discovered Settings** check box.
9. Under **Available Endpoints**, expand the **Devices** folder to display the available devices. Then expand the device folder, and slot folder to select a port for an endpoint. Ports that run FDP or CDP protocol are filtered out because they cannot be a VLL or VPLS endpoint. For a remote VLL the two endpoints must come from different devices. For a Local VLL, the ports selected must be from the same device.
10. Use the right arrow button to move the port to the **Selected Endpoints** box. Make sure you select two endpoints from two different devices.

11. Click **Next**.

The VLL Configuration wizard **Product Configuration** dialog box displays (Figure 352).

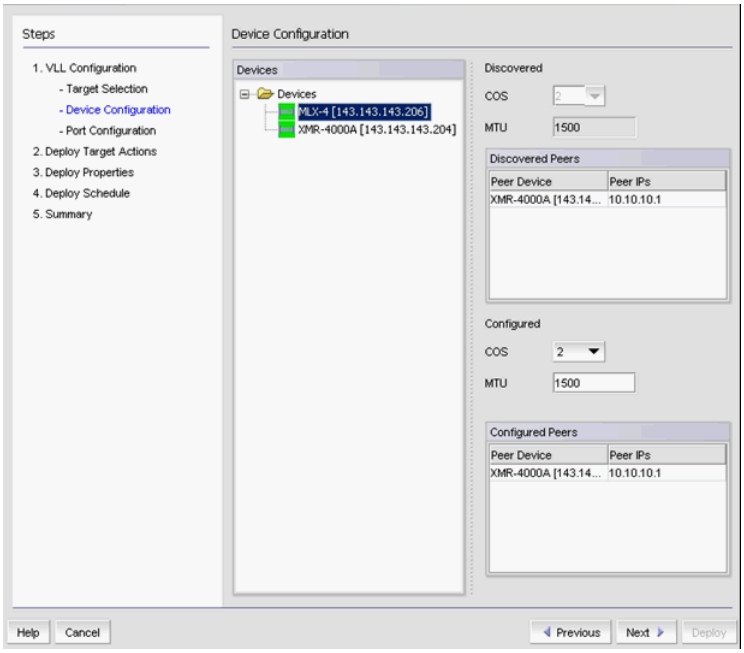


FIGURE 352 VLL Configuration wizard Device Configuration dialog box

NOTE
If you are configuring a local VLL, you cannot make changes to this dialog box. If you are configuring a non-local VLL, select a device from the device list.

Configuring devices using the VLL Manager

1. From the **Product Configuration** pane of the **VLL Configuration Wizard**, click each device entry. The last discovered CoS and MTU settings for the device are displayed in the **Discovered** area. You can modify the settings under the **Configured** area.
2. Enter values for the following:
   - COS - From the drop down list, select the Class of Service (COS) you want to assign to this instance. Packets that go through this instance are assigned this instance. Select 0 - 7.
   - MTU - Enter a Maximum Transmission Unit (MTU) for the device. MTU is the size of the largest data packet that can pass along a device. MTU must be 64 - 90.
   - Configured Peers - The Peers table shows the peer of the selected device. You can select the IP address of the peer by clicking the drop down arrow for Peer IP address. By default, the ingress IP address of a tunnel is selected.

3. Click **Next**.

   The VLL Configuration wizard **Port Configuration** dialog box displays (Figure 353).

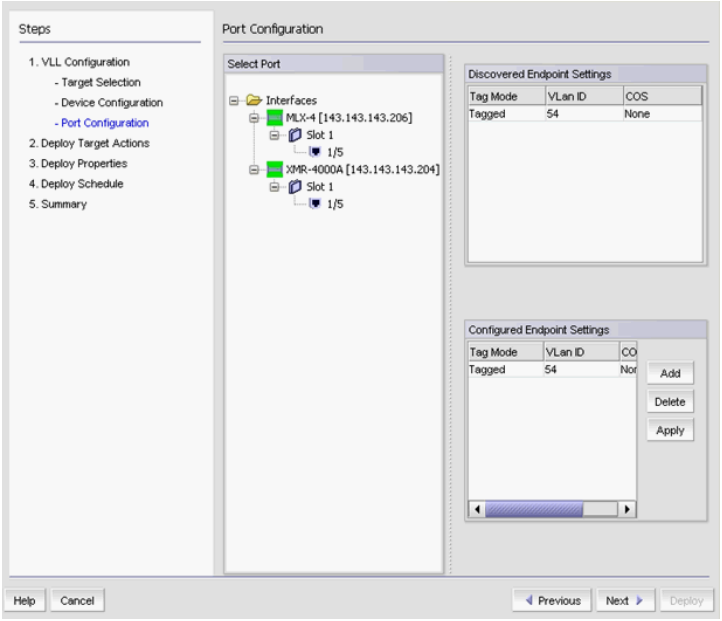


FIGURE 353 VLL Configuration wizard Port Configuration dialog box

The last discovered port settings for VLLs are displayed in the **Discovered Endpoint Settings** table. You can make changes to the settings in the **Configured Endpoint Settings** table.

4. To configure port settings for a port that has not been configured, select a port from the interfaces tree and click **Add** to add a row to the **Configured Endpoint Settings** table.

NOTE
You must configure two endpoints.

Provide the following information:

a. From the **Tag Mode** list, select one of the following:

   - **Tagged**: If the endpoint is a tagged port, the device transmits the packet with the specified VLAN ID and forwards it out the specified interface.
   - **Untagged**: If the endpoint is an untagged port, the device removes any VLAN ID before transmitting it out the specified interface.

b. For tagged ports only, enter a VLAN ID for the service provider end point tag in the **Outer VLAN ID** field.

   Packets with this VLAN ID are transmitted out the specified interface. If you configure dual tagged (inner and outer VLAN ID) endpoints, make sure you meet the following requirements:

   - Requires an Ethernet router, Core router, or Backbone router with firmware version 5.0 and later.
   - You can only define a specific Inner VLAN ID/Outer VLAN ID combination once for all VLL or VPLS instances.

- You can only define one dual tagged endpoint per port.
- You cannot define a dual tagged endpoint on a port if there is a 802.1ag configuration defined on the port.

c. For tagged ports only, enter a VLAN ID for the customer end point in the **Inner VLAN ID** field.

Packets with this VLAN ID are transmitted out the specified interface.

d. From the **COS** list, select a COS for the port.

This field applies only to local VLLs.

5. Click **Apply**.

If any of the endpoints

6. Click **Next**.

The VLL Configuration wizard **Deploy Target Actions** dialog box displays (Figure 354).

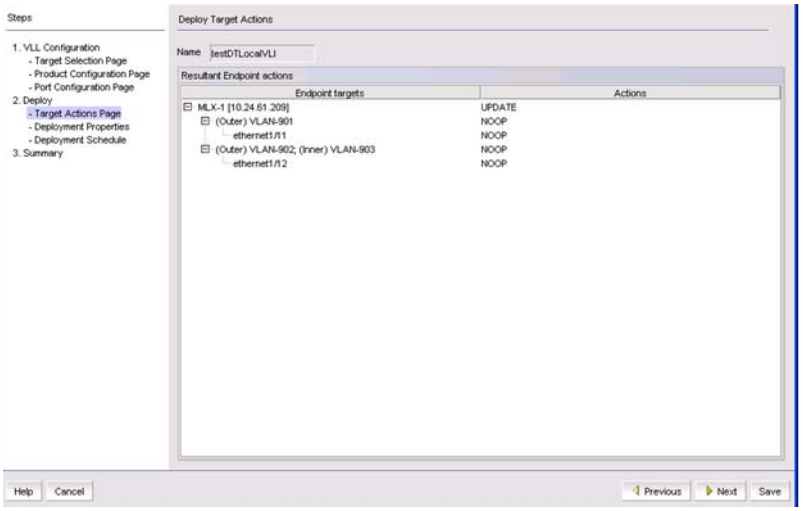


FIGURE 354 VLL Configuration wizard Deploy Target Actions dialog box

Deploying target actions using the VLL Manager

1. From the **Deploy Target Actions** pane, under the **Resultant Endpoint Actions**, **Endpoint Targets** column, select the device, or expand the folder for the device to display the VLAN ID (if the Tagged is configured for the port's tag mode) and the port on which the VLL is to be assigned.
2. The Actions column displays the action to take when the VLL is deployed to the devices. An action is displayed for the device, the VLAN, and the port to which the VLL will be deployed. Possible actions are:
   - **CREATE**: Adds the configuration to the device.
   - **DELETE**: Removes the configuration from the device.
   - **UPDATE**: Modifies the configuration on the device if the configuration is being edited.
3. Click **Next.**

The VLL configuration wizard **Deployment Properties** dialog box displays (Figure 355).

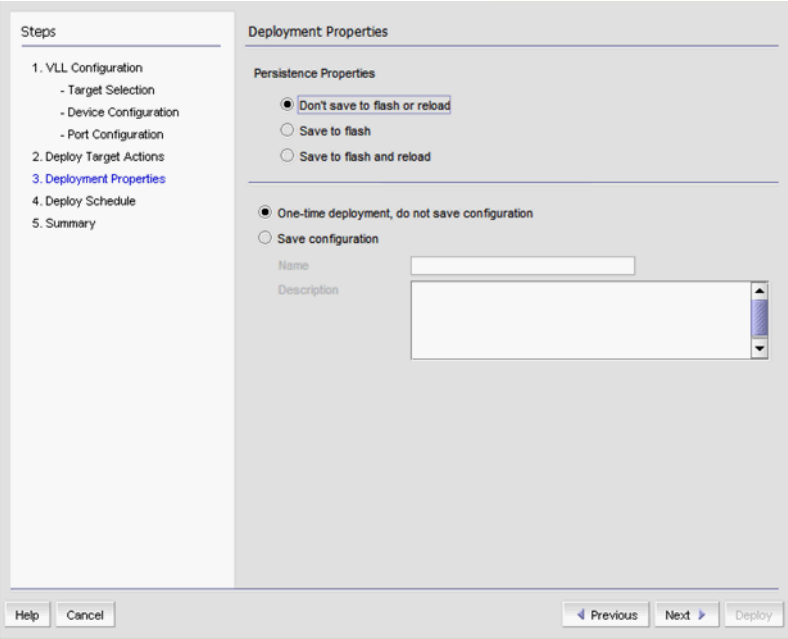


FIGURE 355 VLL configuration wizard Deployment Properties

Deploying VLL properties using the VLL Manager

1. From the **Deployment Properties** pane of the **VLL Configuration Wizard**, under **Persistence Properties**, chose one of the following:
   - **Do not Save to Flash or Reload** - Use this option if you want to update the running configuration. The payload configuration is not saved to the device flash memory, nor is the device rebooted when the VLL configuration is deployed.
   - **Save to Flash** - Use this option if you want to make the payload configuration permanent in the device flash memory and saved to the running configuration. This is equivalent to entering a write memory command. The payload configuration is applied to the device when the device reboots.
   - **Save to Flash and Reload** - Use this option if you want to save the payload configuration to the device flash memory and reboot the device. This is equivalent to entering the write memory and reload commands. The availability of this option depends on your user privileges.
2. Determine if you want to save the payload configuration in the Management application. If this is a one-time deployment, select **One time deployment, do not save configuration**. If you want to save the configuration for future deployment, select **Save configuration**, and enter a configuration name and description.

3. Click **Next**.

   If you did not select **Save configuration** on the **Deployment Properties** dialog box, the **Summary** dialog box displays (Figure 357), and you may skip to step 1.

   If you selected **Save configuration** on the **Deployment Properties** dialog box, the **Deployment Schedule** dialog box displays (Figure 356). Refer to "Scheduling deployment using the VLL Manager" on page 878.

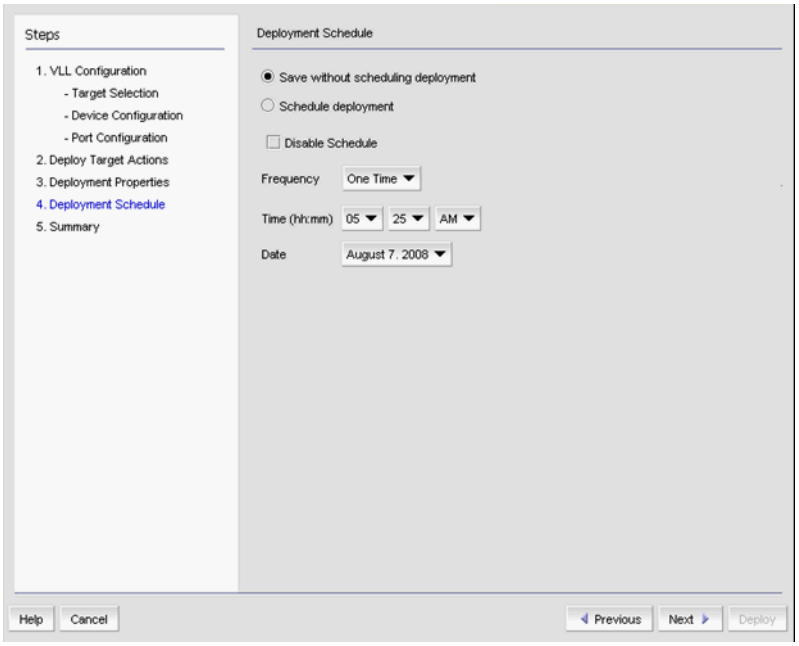


FIGURE 356 VLL configuration wizard Deployment Schedule dialog box

Scheduling deployment using the VLL Manager

1. From the **Deployment Schedule** pane of the **VLL Configuration Wizard**, select from the following deployment options:

   - **Save without scheduling deployment** - saves the payload configuration without a deployment schedule.
   - **Schedule Deployment** - enables you to schedule a time for deployment using the **Frequency**, **Time (hh:mm)**, and **Date** selectors.
   - **Disable Schedule** - Checkbox for disabling a scheduled deployment.

2. Click **Next**.

   The VLL configuration wizard **Summary** dialog box displays (Figure 357).

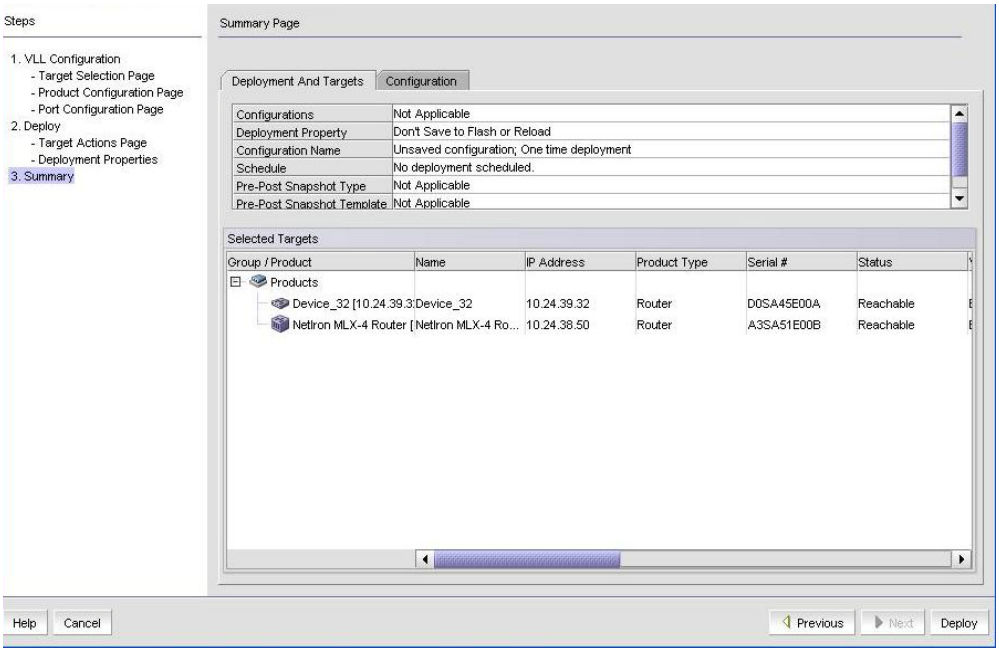


FIGURE 357 VLL configuration wizard Summary dialog box

Reviewing the VLL Manager summary

1. From the **Summary** pane of the **VLL Configuration Wizard**, review the VLL configuration wizard **Summary** information.

   The **Deployment and Targets** tab displays the information you entered on the previous pages. The **Configuration** tab displays the configuration in CLI format.

Reviewing the VLL Manager configuration

1. From the Summary pane of the VLL Configuration Wizard, review the information on the page.

   The **Configuration** tab displays the configuration in CLI format.

2. Click the **Previous** to return to pages that you want to modify. Click **Cancel** to cancel the configuration. When you have finished, click **Next**.

   The configuration is assigned a Configuration ID. The name you assigned the configuration is displayed and the administrator who created the configuration is identified.

3. Click the **Previous** to return to pages that you want to modify. Click **Cancel** to cancel the configuration.

4. When you have finished, click **Next**.

The configuration is assigned a Configuration ID. The name you assigned the configuration is displayed and the administrator who created the configuration is identified.

Creating a new VLL instance using duplicate

To create a new VLL instance using duplicate, do the following.

1. Select **Configure > MPLS > VLL**.
2. Select either the **Views** tab or the **Saved Configurations** tab.
3. Select the instance you want to duplicate from the list of VLL instances.
4. Click the **Duplicate** button.

   The **Target Selection** dialog box displays.
5. The text *Source_Name*_Copy is displayed for Name. Enter a unique name for the new instance. Name cannot contain spaces, asterisks (*), or question marks (?).
6. Also, the Management application automatically fills in the VCID for the new instance. It obtains the next available VCID from the VCID pool. You can change the VCID if desired as long as it is not used in a current VLL instance.
7. Modify any of the remaining values in the instance by following the procedure presented in "Adding or editing a VLL instance" on page 873.

NOTE
If you are modifying the selected endpoints, the device folder under the Available Endpoints lists all MPLS capable devices, whether or not they are covered by your MPLS license. If you select an MPLS capable device that is not covered by your MPLS license, and if you are adding an endpoint that would exceed the device license limit, you will not be able to configure VLL services for that device.

Editing a VLL instance

To edit a VLL instance, do the following:

1. Select **Configure > MPLS > VLL**.
2. Select either the **Views** tab or the **Saved Configurations** tab.
3. Select the instance you want to edit from the list of VLL instances.
4. Click the **Edit** button.

   The **Target Selection** dialog box displays.

Deleting VLL instances

You can delete a VLL configuration from a device, whether or not it is on a device covered by your MPLS license. Do the following.

1. Select the VLL instance you want to delete from the VLL Configuration list. You can select more than one by pressing CTRL + click to select the instances.
2. Click **Delete**.
3. Click **Next** to go to the next step.
4. Click **Deploy** to launch the **Deployment Properties** dialog box.

Filtering VLL traffic monitoring

The VLL Manager Monitor dialog box allows you to monitor traffic on VLLs.

1. Select **Monitor > MPLS > VLL**.

   The **VLL Monitor** Dialog box displays (Figure 358).

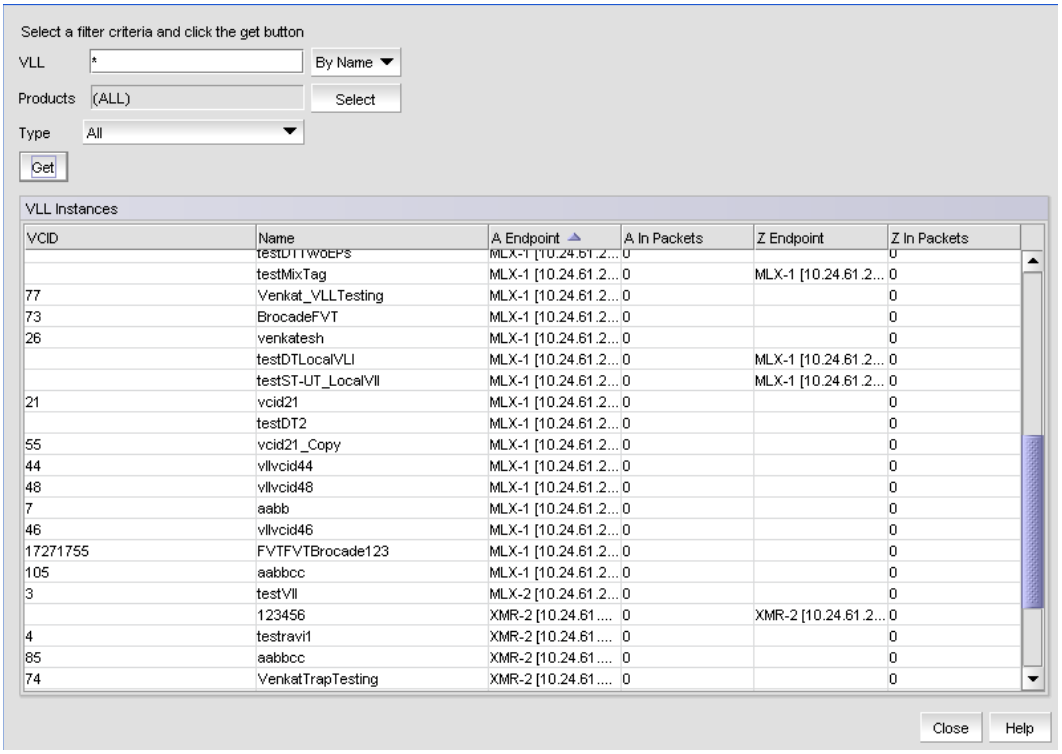


FIGURE 358 VLL Monitor dialog box

2. You can filter output by name or by VCID by using the selector next to the VLL field.
   - You can use an Asterisk (*), as a wildcard character if you select **By Name**.
   - You can enter individual VCIDs or a range of VCIDs if you select **By VCID**.

NOTE
If you choose **By VCID** you can search only for non-local VLLs (VLLs whose endpoints are on two different devices), but not for local VLLs (VLLs whose endpoints are in the same device).

3. Enter a product name or click the **Select** button to launch the **Select Products** dialog box to select a product.
4. Select **Type**.

5. Click the **Get** button to begin the search.

   VLLs that match the filter criteria display under **VLL Instances**.

NOTE
If a VLL is from a device that is not covered by the MPLS license, the row is grayed out. You will not be able to edit that VLL, but you can delete it from the device.

The **VLL Instances** table shows the following information:

- VCID of the VLL
- Name of the VLL
- A Endpoint - Name and IP address of the device that serves as the first endpoint for the VLL
- In Packets - Number of packets received by the A Endpoint. This data is not available in the NetIron CER and NetIron CES
- Z Endpoint - Name and IP address of the device that serves as the last endpoint for the VLL
- In Packets - Number of packets transmitted through the Z Endpoint. This data is not available in the NetIron CER and NetIron CES.

Virtual Private LAN Services (VPLS) overview

Virtual Private LAN Services (VPLS) is a method for carrying Layer 2 frames between customer edge (CE) devices across an MPLS domain. VPLS provides point-to-multipoint connectivity across the MPLS domain, allowing traffic to flow between remotely connected sites as if the sites were connected by a Layer 2 switch.

Figure 359 shows two separate VPLS instances have been created, one for Customer A's VPN and one for Customer B's VPN. Customer A's VPLS instance consists of virtual Circuit (VC) LSPs between PE devices R1, R2, and R3. Customer B's VPLS instance consists of VC LSPs between PE devices R3 and R4. Since VC LSPs are unidirectional, separate VC LSPs exist in each direction between each of the PE devices. When Label Distribution Protocol (LDP) is enabled on the MPLS interfaces on the PE devices, the VC LSPs are established automatically through LDP when you specify the VPLS peers on the PE devices.

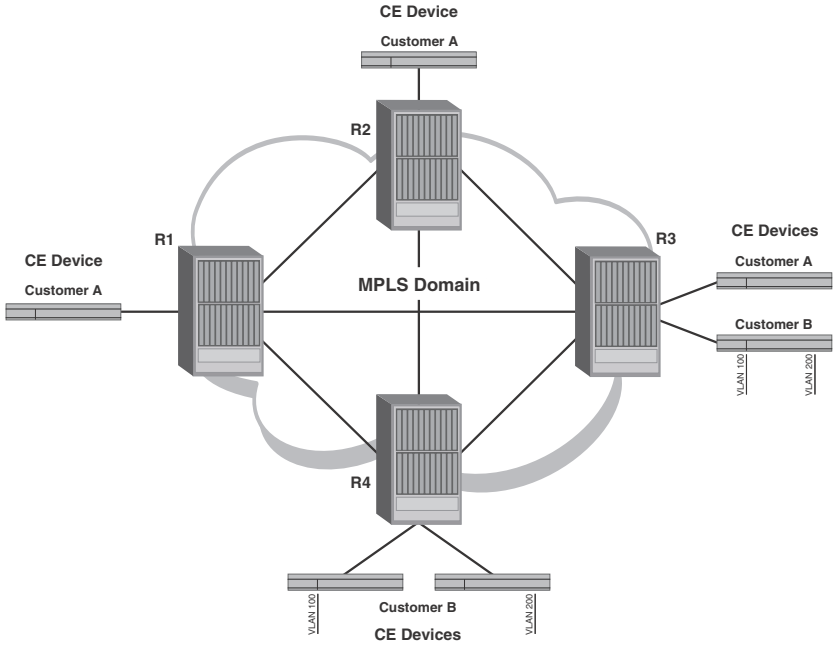


FIGURE 359 VPLS configuration with two customer VPNs

Unlike a Virtual Leased Line (VLL), a VPLS instance can have multiple endpoints. The PE device performs local and remote VLAN tag translation, so that multiple VLANs can be specified under a single VPLS instance. A VPLS instance consists of a full mesh of VC LSPs between the customer's Provider Edge (PE) devices. The full mesh of PE devices in a VPLS configuration allows one PE device to reach any other PE device in the VPN in exactly one hop, with no transit PE devices in between.

A PE device performs MAC address learning, flooding, and forwarding for the CE devices in each VPLS instance. For example, when PE device R1 receives a Layer 2 frame with a given MAC destination address from Customer A's CE device, it looks up the MAC address in a Layer 2 forwarding table that records associations between MAC addresses and VC LSPs. This forwarding table is known as the VPLS MAC database.

The PE device uses MAC address found in the VPLS MAC database to find the associated VC LSP. The PE device then encapsulates the frame as an MPLS packet and pushes an inner VC label and outer tunnel label onto the packet. The packet is then sent over a tunnel LSP to the VC peer.

VPLS Manager

The VPLS Manager allows you to manage VPLS instances. You can perform the following tasks from the VLL manager:

- View current VPLS instances and peer topologies.
- View VPLS configurations.
- Add, edit, duplicate, or delete VPLS instances.

NOTE
When configuring VPLS, a check is made to determine if there are LSPs configured for the target products. You may proceed with configuration, but an LSP is needed for a working connection.

Viewing VPLS instances and peer topologies

To view currently defined VPLS instances and peer topologies, do the following:

1. Select **Configure > MPLS > VPLS.**
2. To view information about current VPLS instances, select the **Views** tab and the **Details** tab (Figure 360).

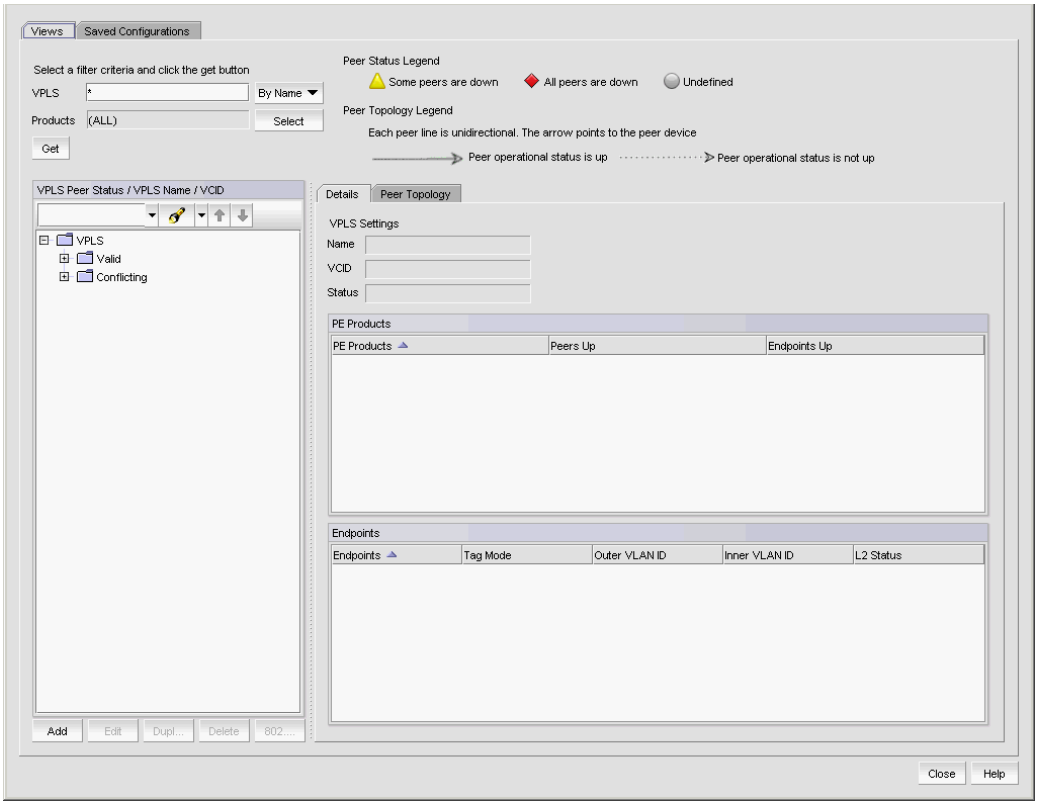


FIGURE 360 VPLS Manager Views tab

3. To specify new filter criteria, select **By Name** or **By VCID** from the VPLS list. You can use the following to filter the VPLS instances:
   - Asterisk (*) as a wildcard character if you select **By Name**.
   - Individual VCIDs or a range of VCIDs, separating each entry with a comma if you selected **By VCID**.
4. Click **Get** to begin the search.

   Information about products that match the search criteria displays under **VPLS Settings**, **PE Products**, and **Endpoints** on the **Details** tab.

   VPLS settings

   - VCID of the VPLS
   - Name of the VPLS
   - Current status of the VPLS. This status is derived from the state of all PE devices for a VPLS.

   Endpoint settings

   - PE Devices
     - PE Devices: Name and IP address of the PE device on which the VPLS is configured.
     - Peer up: Shows the number of peers that are up.
     - Endpoint up: Shows the number of endpoints that are up.
   - Endpoints
     - Endpoint: Names and IP addresses of the endpoint devices.
     - Tag Mode: Tagged if a VLAN tag is used. Untagged if a VLAN tag is not used.
     - Outer VLAN ID - Present if the Tag Mode for the endpoint is Tagged. The service provider end point tag.
     - Inner VLAN ID - Present if the Tag Mode for the endpoint is Tagged. The customer end point tag.
     - L2 Status: Layer 2 status - Up or Down.
5. To view VPLS peer topologies, select the **Peer Topology** tab.

   A topology map displays (Figure 361).

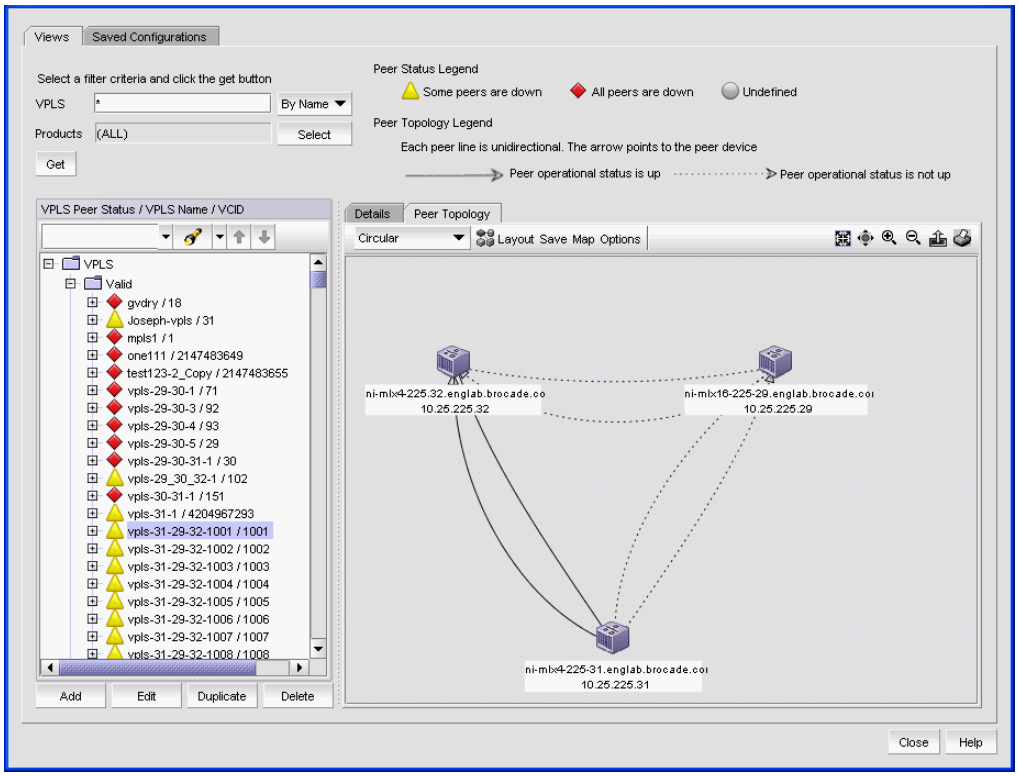


FIGURE 361 VPLS Manager Peer Topology tab

Viewing Saved VPLS configurations

To view current VPLS configurations, do the following:

1. Select **Configure > MPLS > VPLS.**
2. Select the **Saved Configurations** tab (Figure 362).

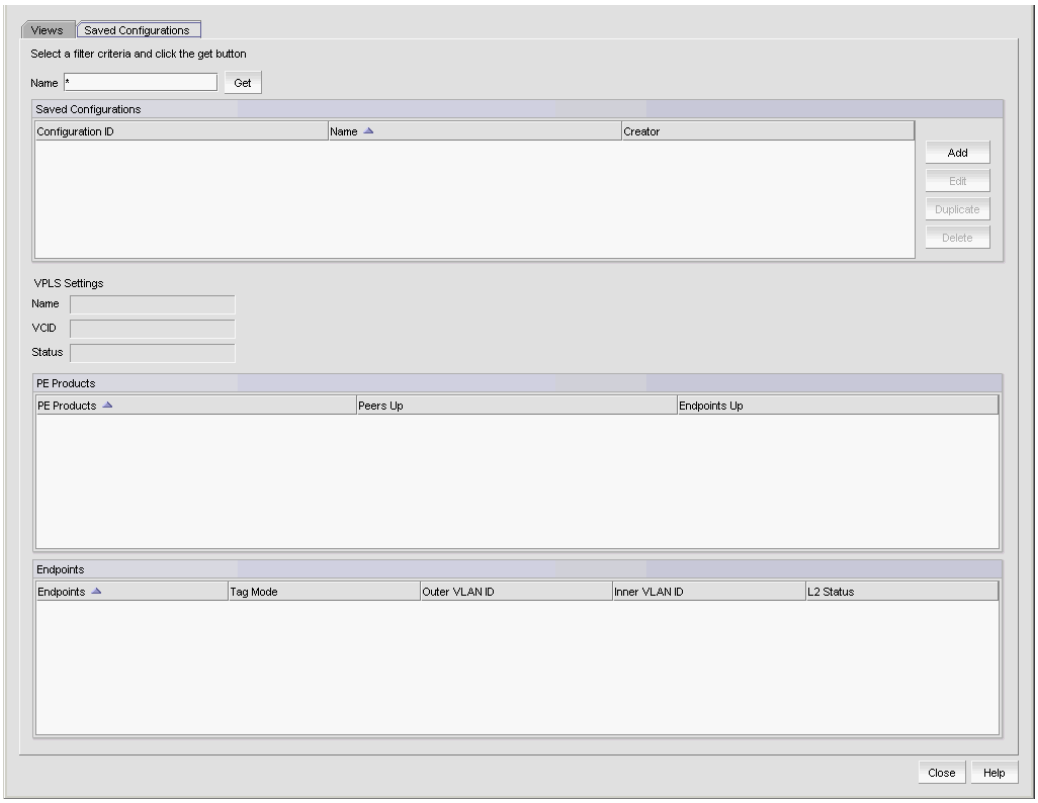


FIGURE 362 VPLS Manager Saved Configurations tab

3. You can use the **Name** field to filter output by configuration name.

   You can use an Asterisk (*) as a wild card character.

4. Click **Get** to begin the search.

   Configurations that match the filter criteria display under **Saved Configurations**, showing the configuration ID, the configuration name, and the name of the user that created the configuration.

   When you select a configuration, configuration information displays in the fields below **Saved Configurations**.

   - **VPLS Settings** — Displays the following information about a selected VLL in the fields below:
     - **Configuration ID —** The VCID of the VPLS.
     - **Name** — The name of the VPLS.
     - **Status** — Current status of the VPLS. This status is derived from the state of all PE devices for a VPLS.

- **PE Products** table — Displays the following information:
  - **PE Devices** — Names and IP addresses of the endpoint devices.
  - **Peers Up** — The number of peers that are up.
  - **Endpoints Up** — The number of endpoints that are up.
- **Endpoints** table — Displays the following information:
  - **Endpoints** — Names and IP addresses of the endpoint devices.
  - **Tag Mode** — Tagged if a VLAN tag is used. Untagged if a VLAN tag is not used.
  - **Outer VLAN ID** — Present if the Tag Mode for the endpoint is Tagged. The service provider end point tag.
  - **Inner VLAN ID** — Present if the Tag Mode for the endpoint is Tagged. The customer end point tag.
  - **L2 Status** — Displays whether L2 is up or down.

5. Right-click any entry in the table to display the Print pop up menu. Select Print from the menu to print the table.
6. Click **Close** to close the **VPLS Manager** dialog box.

Adding or editing a VPLS instance

To add a VPLS Instance, do the following.

1. From the **Saved Configurations** tab of the **VPLS Manager**, click the **Add** button.

   The **Target Selector** dialog box of the VPLS configuration wizard displays (Figure 363).

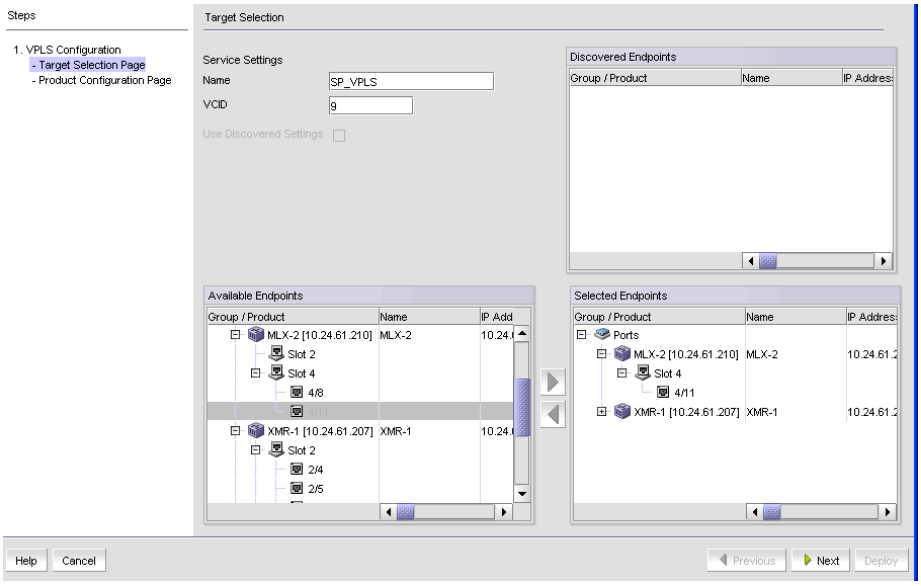


FIGURE 363 VPLS Configuration wizard Target Selector dialog box

2. Enter a name for the VPLS. The name must be unique on each device and cannot contain spaces, asterisks (*), or question marks (?).
3. If you want to use a specific VCID, enter the VCID. If you do not specify a VCID, the next available VCID in the VCID pool is assigned.

4. If you want to copy the VPLS configurations for one or more products or ports under **Discovered Endpoints**, select the product or port and then select the **Use Discovered Settings** check box.
5. Under **Available Endpoints**, expand the **Devices** folder to display the available devices. Then expand the device folder, and slot folder to select a port for an endpoint.
6. Use the right arrow button to move the port to the **Selected Endpoints** box. Make sure you select two endpoints from two different devices.

NOTE
The device folder lists all MPLS capable devices, whether or not they are covered by your MPLS license. If you select an MPLS capable device that in not covered by your MPLS license, you will not be able to configure VPLS services for that device. If you select an endpoint on a device that is not covered by your MPLS license and the device is not in the All MPLS Licensed and Configured Devices group, you see an error message saying that the MPLS device limit will be exceeded.

7. Click **Next**.

The **Device Configuration** dialog box displays (Figure 364).

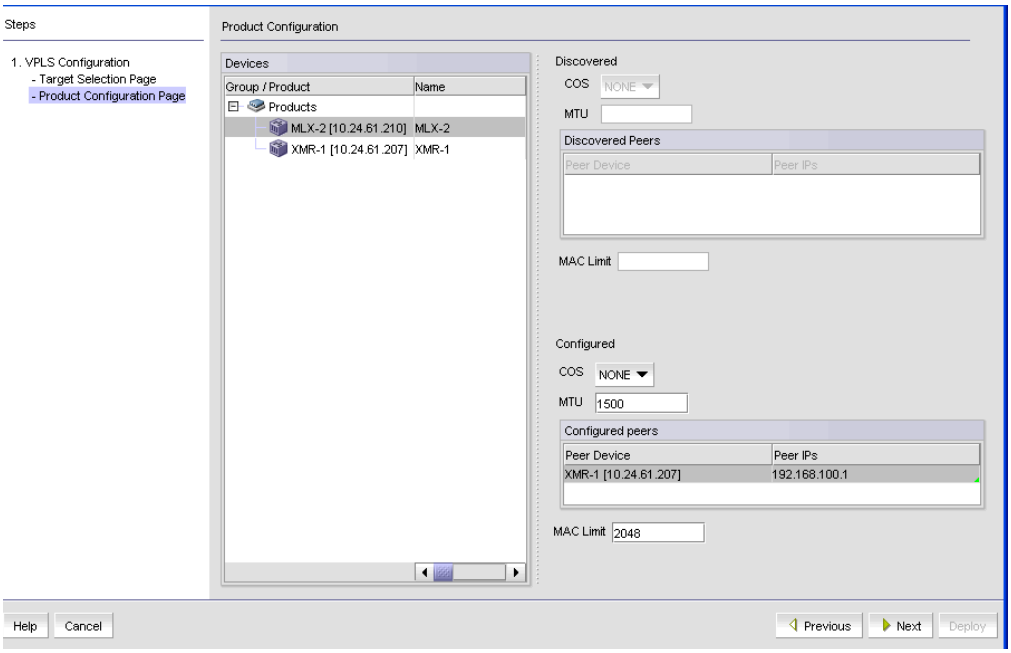


FIGURE 364 VPLS Configuration wizard Device Configuration dialog box

Configuring devices using the VPLS Manager

1. Click each device entry under **Devices** to determine if there are discovered settings for that device. The last discovered settings for the device are displayed in the **Discovered** area.
2. Under the **Configured** area, enter values for the following:

a. From the drop down list, select the Class of Service (COS) you want to assign to this instance.

b. Enter a Maximum Transmission Unit (MTU) for a VPLS instance. MTU is the size of the largest data packet that can pass along a device. Determine the range of values you can enter by checking the configuration guide for your device.

The Peers table shows the peer of the selected device.

c. You can select the IP address of the peer by clicking the drop down arrow for Peer IP address. By default, the ingress IP address of a tunnel is selected.

d. Enter the maximum number of MAC entries that the VPLS instance is allowed to learn. Determine the range of values you can enter by checking the configuration guide for your device.

3. Click **Next**.

The **Port Configuration** page displays (Figure 365).

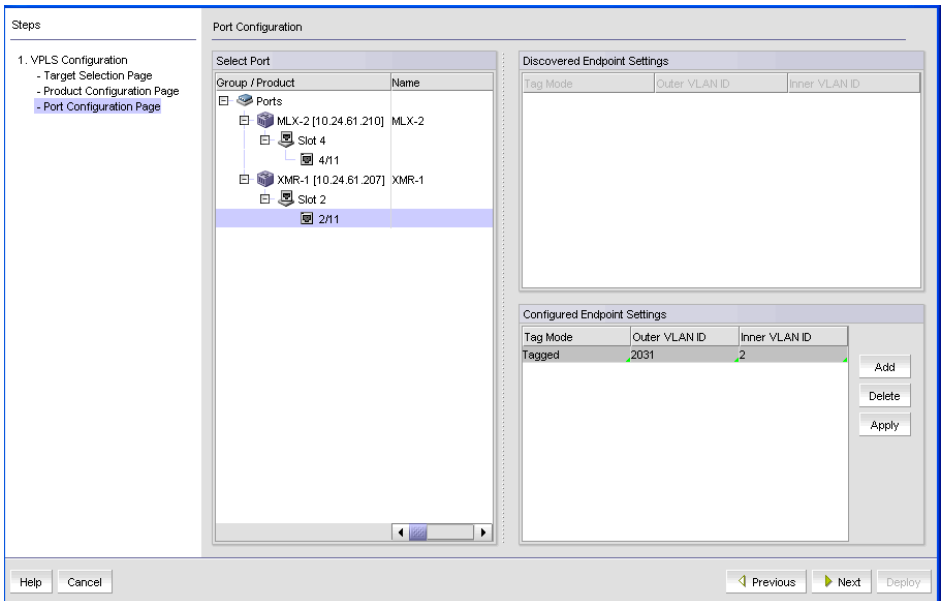


FIGURE 365 VPLS Configuration wizard Port Configuration dialog box

Discovered VPLS port settings appear under **Discovered Endpoint Settings**.

Configuring endpoint settings

1. From the Port Configuration page of the VPLS Configuration wizard, select a port from the **Interfaces** tree and click the **Add** button under **Configured Endpoint Settings**.

A row is added to the **Configured Endpoint Settings** list.

2. Click the empty **Tag Mode** field and select one of the following:

- **Tagged** if you want packets transmitted with a specified VLAN ID.
- **Untagged** if you want any VLAN ID removed before transmitting the packet.

3. If you chose **Tagged** mode, complete the following steps.

a. Click the empty **Outer VLAN ID** field and enter the VLAN ID you want to use.

b. Click the empty **Inner VLAN ID** field and enter the VLAN ID you want to use. Skip this step if you are using single tagging.

4. Click **Next**.

The **Deploy Target Actions** dialog box displays (Figure 366).

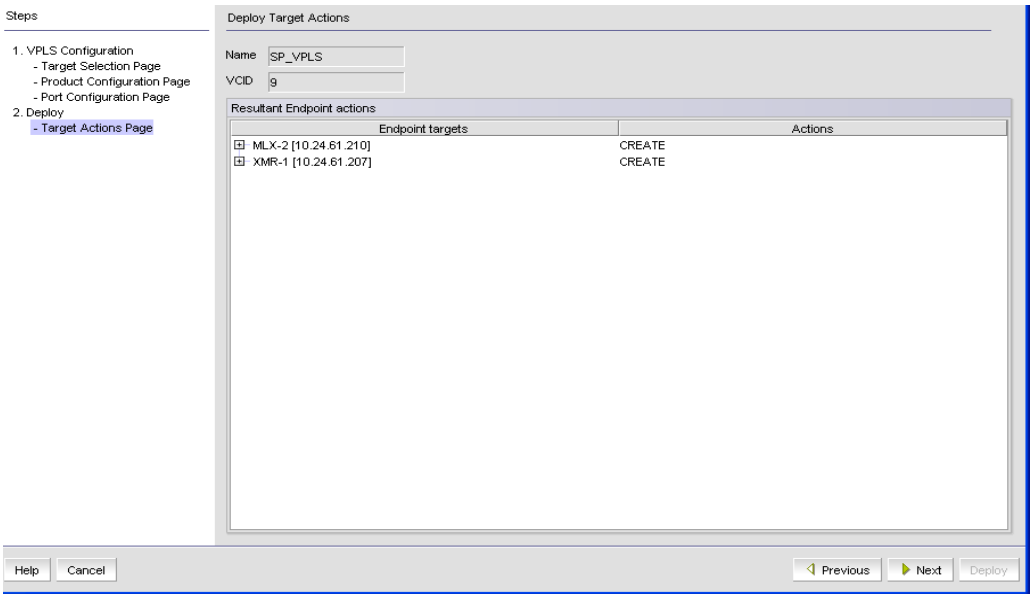


FIGURE 366 VPLS Configuration wizard Deploy Target Action dialog box

The VPLS instance name and VCID are shown in the **Name** and **VCID** fields.

Deploying target actions using VPLS Manager

1. From the **Deploy Target Actions** pane, the **Endpoint Targets** column lists the names and IP addresses of the devices to which the VPLS instance will be deployed. Expand the folder for a device to display any VLANs and ports to which the VPLS instance will be deployed.

   The **Actions** column displays the action that will be taken when the VPLS instance is deployed to the devices. Possible actions are:

   - **CREATE**: Adds the configuration to the device.
   - **DELETE**: Removes the configuration from the device.
   - **UPDATE**: Modifies the configuration on the device if the configuration is being edited.
   - **NOOP**: No change is required.

2. Click **Next**.

   The **Deployment Properties** page displays (Figure 367).

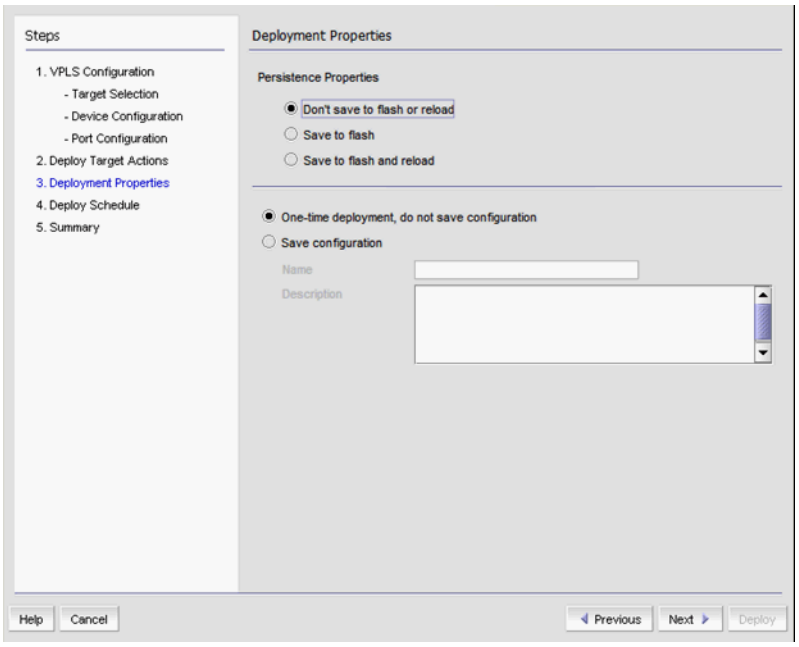


FIGURE 367 VPLS Configuration wizard Deployment Properties dialog box

Deploying VPLS properties using VPLS Manager

1. From the **Deployment Properties** pane, choose one of the following persistence properties:
   - **Do not Save to Flash or Reload** - Use this option if you want to update the running configuration. The payload configuration is not saved to the device flash memory, nor is the device rebooted when the payload configuration is deployed.
   - **Save to Flash** - Use this option if you want to make the payload configuration permanent in the device flash memory and saved to the running configuration. This is equivalent to entering a write memory command. The payload configuration is applied to the device when the device reboots.
   - **Save to Flash and Reload** - Use this option if you want to save the payload configuration to the device flash memory and reboot the device. This is equivalent to entering the write memory and reload commands. The availability of this option depends on your user privileges.
2. Determine if you want to save the payload configuration in the Management application. If this is a one-time deployment, select **One time deployment, do not save configuration**. If you want to save the configuration for future deployment, select **Save configuration**, and enter a configuration name and description.
3. Click **Next**.

   If you did not select **Save configuration** on the **Deployment Properties** dialog box, the **Summary** dialog box displays (Figure 369), and you may skip to step 1.

   If you selected **Save configuration** on the **Deployment Properties** dialog box, the **Deployment Schedule** dialog box displays (Figure 368). Proceed with step 1.

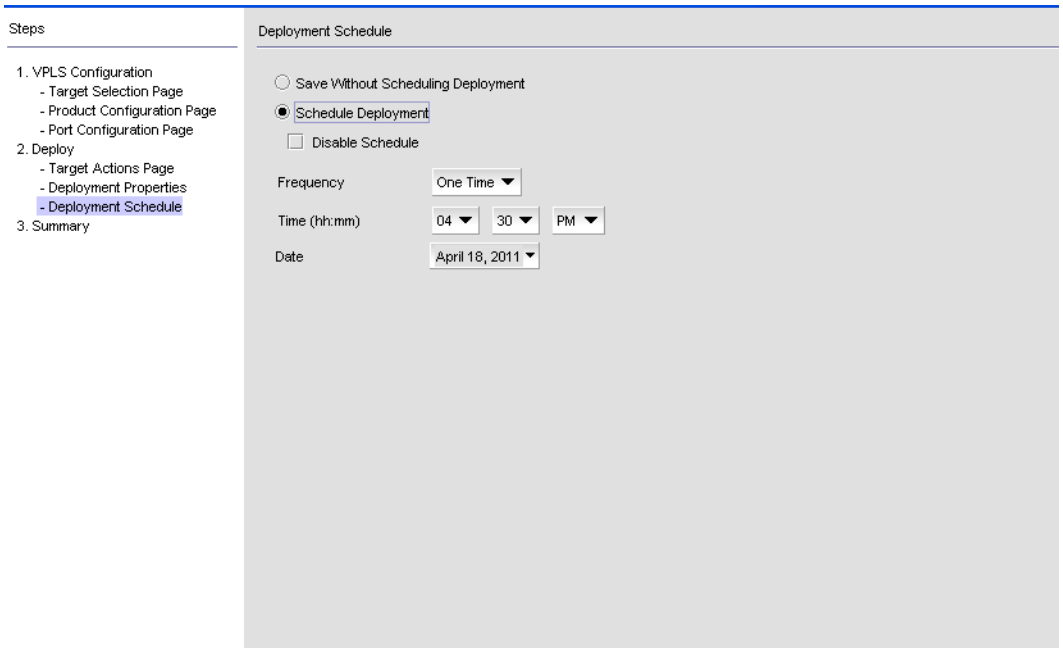


FIGURE 368 VPLS Configuration wizard Deployment Schedule dialog box

Scheduling deployment using VPLS Manager

1. If the **Deployment Schedule** dialog box displays, select from the following deployment options:
   - **Save without scheduling deployment** - saves the payload configuration without a deployment schedule.
   - **Schedule Deployment** - enables you to schedule a time for deployment using the **Frequency**, **Time (hh:mm)**, and **Date** selectors.
2. Click **Disable Schedule** to disable a schedule. If you clear the check box, the schedule is enabled.
3. Click **Next.**

   The **Summary** dialog box displays (Figure 369).

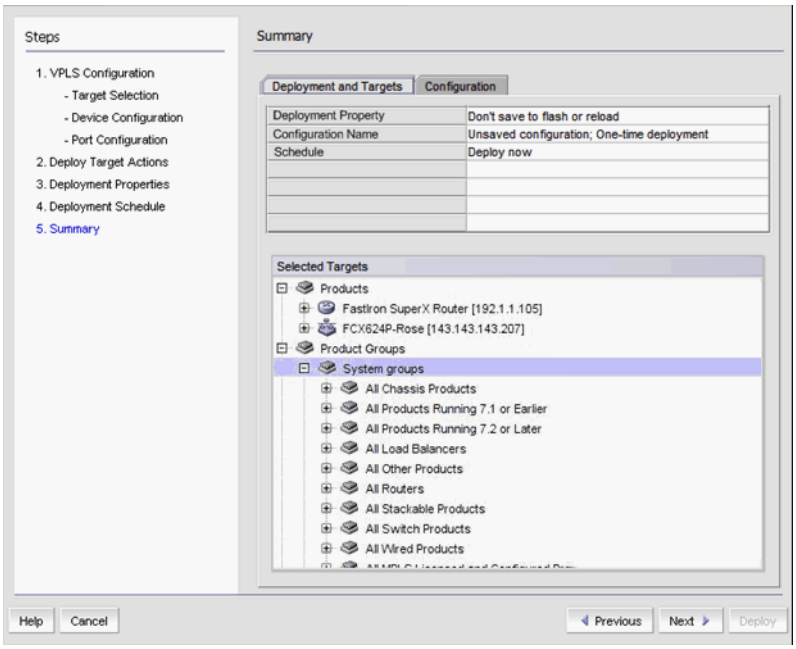


FIGURE 369 VPLS Configuration wizard Deployment Summary dialog box

Reviewing the VPLS Manager summary

1. On the Deployment and Targets **Summary** pane, review the summary information.

   The **Deployment and Targets** tab displays the information you entered on the previous pages. The **Configuration** tab displays the configuration in CLI format.

2. Click the **Previous** to return to pages that you want to modify. Click **Cancel** to cancel the configuration. When you have finished, click **Next**.

The configuration is assigned a Configuration ID. The name you assigned the configuration is displayed and the administrator who created the configuration is identified.

Creating a new VPLS instance from a duplicate

To create a new VPLS instance from a duplicate, do the following.

1. Select the instance you want to duplicate from the list of VPLS instances.
2. Click the **Duplicate** button. The text *Source_VPLS_Name*_Copy is displayed in the **Name** field.
3. Enter a unique name for the new instance. The name cannot contain spaces, asterisks (*), or question marks (?).

4. The next available VCID in the VCID pool is automatically placed in the **VCID** field. You can change the VCID if desired as long as it is not used in a current VLL instance.
5. Modify any of the remaining values in the instance by following the procedure presented in "Adding or editing a VPLS instance" on page 888.

NOTE
The device folder under Available Endpoints lists all MPLS capable devices, whether or not they are in the All MPLS Licensed and Configured Devices group. If they are not and if adding the device endpoints in the VPLS configuration would exceed the license limit, then you will not be able to deploy the configurations.

Editing a VPLS instance

To edit a VPLS instance, do the following:

1. Select **Configure > MPLS > VPLS**.
2. Select either the **Views** tab or the **Saved Configurations** tab.
3. Select the instance you want to edit from the list of VLL instances.
4. Click the **Edit** button.

   The **Target Selection** dialog box displays.

   NOTE
   The device folder under Available Endpoints lists all MPLS capable devices, whether or not they are in the All MPLS Licensed and Configured Devices group. If they are not and if adding the device endpoints in the VPLS configuration would exceed the license limit, then you will not be able to deploy the configurations.

Deleting a VPLS instance

You can delete a VPLS configuration from a device, whether or not it is covered by your MPLS license. Do the following.

1. Select the VPLS instance you want to delete from the VPLS list. You can select more than one by pressing CTRL + click to select the instances.
2. Click the **Delete** button on the tool bar.

   The **VPLS Configuration** box appears.
3. Review the VCIDs and names listed to make sure you want to delete those configurations.
4. Click the **Configuration tab** to view the list of VPLS instances to be deleted.
5. Click **Save** to save the configuration, or **Cancel** if you changed your mind.

   The saved configuration appears under the Saved Configuration tab. The VPLS configuration is deleted from the devices only if they are deployed successfully. the Management application will resynch the devices from which the VPLS instance was deleted and remove the VPLS configuration for those devices from its database.

Filtering for VPLS traffic monitoring

The VPLS Manager Monitor allows you to filter and monitor VPLS traffic.

1. Select **Monitor > MPLS > VPLS**.

   The **VPLS Monitor** dialog box displays (Figure 370).

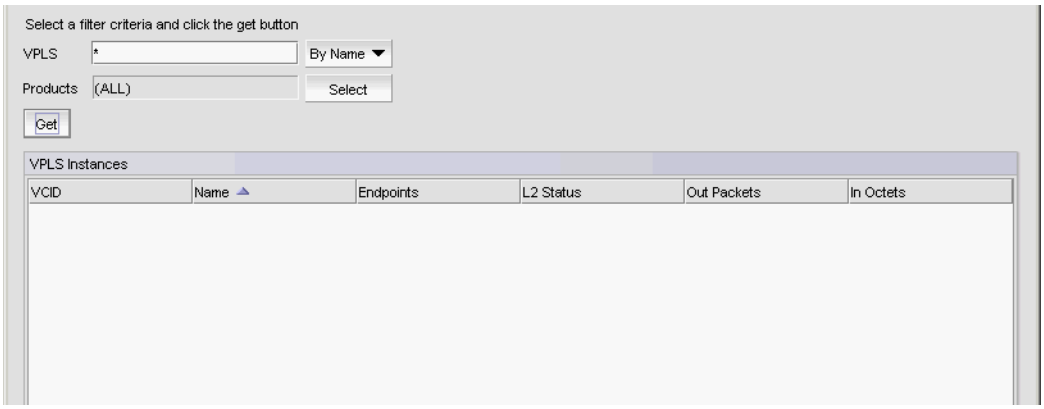


FIGURE 370 VPLS Monitor dialog box

2. You can filter output by name or by VCID by using the selector next to the **VPLS** field.
   - You can use an Asterisk (*), as a wildcard character if you select **By Name**.
   - You can enter individual VCIDs or a range of VCIDs if you select **By VCID**.
3. Enter a product name or click the **Select** button to launch the **Select Products** dialog box to select a product.
4. Select **Type**.
5. Click the **Get** button to begin the search.

NOTE
VPIf a VPLS instance is from a device that is not covered by the MPLS license, the row is grayed out. You will not be able to edit that instance, but you can delete it from the device.

The **VPLS Instances** table shows the following information:

- VCID — VCID of the instance.
- Name — Name of the instance.
- A Endpoint — Name and IP address of the devices that serve as VPLS endpoints.
- L2 Status — Layer 2 status - Up or Down.
- Out Packets — Number of packets transmitted out of the Endpoint. Only available for Ethernet Core and Backbone routers.
- In Octets — Number of octets received in the Endpoint. Only available for Ethernet Carrier and Edge routers.

VCID pools

VCID pools contain VCID that can be used in a VLL or VPLS instance. You may create a combined VCID pool containing VCIDs that are shared by VLL and VPLS, or you may create a segmented VCID pool that provides separate VCID pools for VLL and VPLS configurations.

Viewing, creating, and deleting VCID pools

To view a VCID Pool and to create or delete VCID pools, do the following:

1. Select **Configure > MPLS > VCID Pool**.

   The **VCID Pool** dialog box displays (Figure 371).

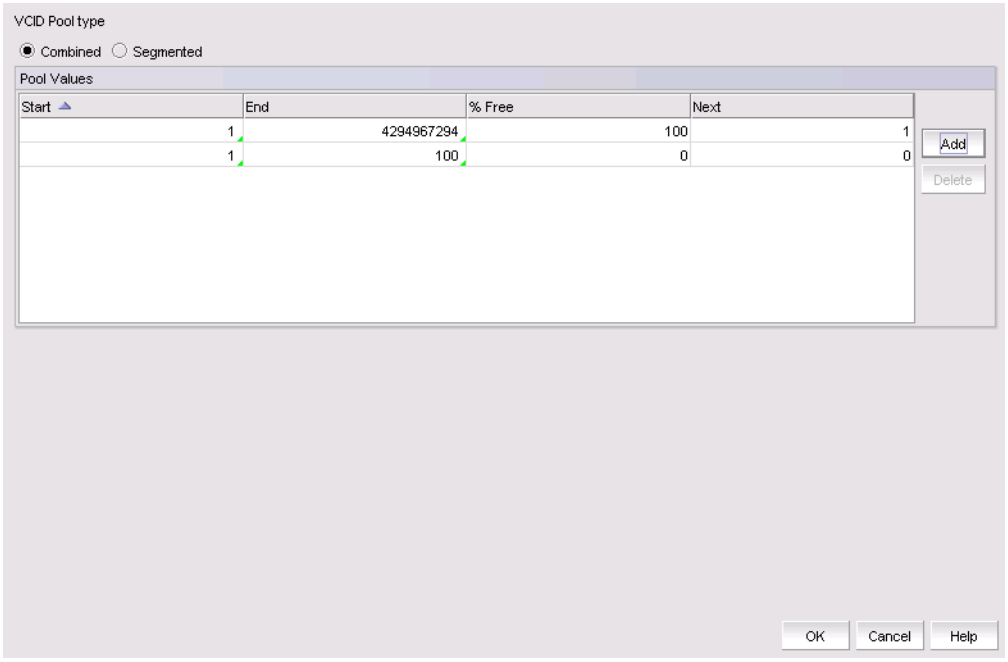


FIGURE 371 VCID Pool dialog box

2. For **VCID Pool Type**, select **Combined** if you want to create a combined VCID pool containing VCIDs that are shared by VLL and VPLS, or **Segmented** if you want to create a segmented VCID pool that provides separate VCID pools for VLL and VPLS configurations.

   If you select **Combined**, and single **Pool Values** list is displayed. If you select **Segmented**, a **VPLS Pool** list and a **VLL Pool** list are displayed.

   The **Pool Values** list displays starting and ending numbers in the pool, the percentage of VCIDs available in the pool, and the next available VCID.

3. Click the **Add** button to add an empty entry to the table.
4. Click the **Delete** button to delete a selected entry.

5. Edit the **Start** and **End** fields to specify the desired range of VCIDs. You can use any numbers between 1 to 4294967294. If you are creating a segmented pool, be sure the VLL and VPLS VCIDs do not overlap.

6. Click **OK**.

802.1ag Connectivity Fault Management

802.1ag Connectivity Fault Management (CFM) is an IEEE standard used to define protocols and practices for Ethernet Operations, Administration, and Maintenance (OAM). 802.1ag CFM enables you to manage your network infrastructure remotely. Once you configure a maintenance association and its associated end points, you can perform the following fault management checks:

- Fault detection using connectivity status
- Fault verification using loopback messages
- Fault isolation using linktrace messages
- Fault isolation using frame delay

NOTE
802.1ag CFM is only supported on IronWare Ethernet Routers devices running firmware release 5.2 or later.

NOTE
You cannot configure an 802.1ag CFM on a maintenance end point (MEP) configured with dual tagged VLANs.

Configuring a maintenance association

You can access 802.1ag CFM from the following features:

- VPLS Manager
- VLL Manager
- VLAN Manager

NOTE
802.1ag CFM is only supported on IronWare Ethernet Routers devices running firmware release 5.2 or later.

NOTE
You cannot configure an 802.1ag CFM on a maintenance end point (MEP) configured with dual tagged VLANs.

To configure a maintenance association, complete the following steps.

1. Choose one of the following options:
   - From the **VPLS Manager** dialog box, **Views** tab, choose one of the following options:
     - Select a device from the **VPLS Peer Status/VPLS Name/VCID** list and click **802.1ag CFM**.
     - Select the **Peer Topology** tab and right-click a device in the topology and select **802.1ag CFM.**
   - From the **VLL Manager** dialog box, **Views** tab, select an instance from the **VLL Instances** table and click **802.1ag CFM.**
   - From the **VLAN Manager** dialog box - **VLAN View** or **Product View**, select a VLAN from list and click **802.1ag CFM.**

   The **Configure 802.1ag CFM** dialog box displays.
2. Click **Add**.

   The **Add Maintenance Association** dialog box displays.
3. Select a maintenance domain from the list or enter a new maintenance domain name in the **Domain** field/list.

   The maintenance domain name must be less than 21 characters with no spaces.
4. If you selected a new maintenance domain name from the **Domain** list, select a level (1 through 7) for the maintenance domain from the **Level** list.

   If you selected a maintenance domain from the **Domain** list, the **Level** automatically displays.
5. Enter a name for the maintenance association in the **Association Name** field.

   The maintenance association name must be less than 21 characters with no spaces.
6. Enter an interval for the Continuity Check Messages (CCM) from the **CCM Interval** list.

   The default value is 10 seconds. Options include: 1 sec, 1 minute, 10 second, 10 minutes, 3.3 ms, 10 ms, and 100 ms.
7. Select a maintenance intermediate point (MIP) policy from the **MIP Policy** list.

   Options include:
   - **Default** — Creates MIPs in all service ports for a particular maintenance domain.
   - **Explicit** — Only creates a MIP when there is a MEP on the port at a lower level maintenance domain.
8. Select a product from the **Product** list.

   The list contains all products that are part of the VPLS.
9. Select a VLAN ID from the **VLAN ID** list.

   The list contains all VLAN IDs in the VPLS.
10. Select a port from the **Port** list.

    The list contains all VPLS end-points for the selected VLAN ID.
11. Enter a unique identifier for the end-point in the End Point ID field.

    Valid values include 1 through 8191.

12. Select the MEP direction from the **Direction** list.

    Options include:

    - **Up** — Select to set the MEP direction away from the monitored VLAN.
    - **Down** — Select to set the MEP direction towards the monitored VLAN.

13. Click the right arrow button to move the defined MEP to the **Selected Maintenance End Points** table.

    The **Selected Maintenance End Points** table lists the following configured MEP parameters:

    - The product on which the MEP is located
    - The VLAN ID of the MEP
    - The port of the MEP
    - The user-defined end-point identifier of the MEP
    - The direction (up or down) of the MEP

14. Click **OK** on the **Add Maintenance Association** dialog box.

    The **Deploy to Products** dialog box displays.

15. Select one of the following options:

    - **Save to running** — Select to update the running configuration; however, the deployment is not saved to the product's flash memory.
    - **Save to running and startup** — Select to update the running configuration as well as save the deployment configuration to the product's flash memory. Selecting this option is the equivalent to a write memory command on the product CLI.
    - **Save to running and startup then reboot** — Select to update the running configuration, save the deployment configuration to the product's flash memory, and reboot the product. Selecting this option is the equivalent to entering a write memory and a reload command on the product CLI.

16. Click **OK** on the **Deploy to Products** dialog box.

    The **Deployment Status** dialog box displays.

    While deployment is in progress, you can do the following:

    - Click **Abort** to stop deployment of the entire configuration.

      NOTE
      The abort action does not stop the tasks that have already started.

    - Click **Close** to close the **Deployment Status** dialog box.

      NOTE
      Closing the Deployment Status dialog box does not stop deployment of the configuration.

    After deployment is complete, you can select an entry in the **Deployment Status** list to display details about the deployment in the **Status Details** field.

17. Click **Close** on the **Deployment Status** dialog box.

    The **Configure 802.1ag CFM** dialog box displays with the new association in the **Maintenance Association Details** table.

18. Click **Close** on the **Configure 802.1ag CFM** dialog box.

Editing a maintenance association

You can access 802.1ag CFM from the following features:

- VPLS Manager (requires the IP - MPLS – VLL prvilege with read-write or read-only permission)
- VLL Manager (requires the IP - MPLS – VPLS prvilege with read-write or read-only permission)
- VLAN Manager (requires the VLAN Manager prvilege with read-write or read-only permission)

NOTE
802.1ag CFM is only supported on IronWare Ethernet Routers devices running firmware release 5.2 or later.

NOTE
You cannot configure an 802.1ag CFM on a maintenance end point (MEP) configured with dual tagged VLANs.

To Edit a maintenance association, complete the following steps.

1. Click **802.1ag CFM**.

   The **Configure 802.1ag CFM** dialog box displays.

2. Select the maintenance association you want to edit in the **Maintenance Association Details** table.

3. Click **Edit**.

   The **Edit Maintenance Association** dialog box displays.

4. Select a maintenance domain from the list or enter a new maintenance domain name in the **Domain** field/list.

   The maintenance domain name must be less than 21 characters with no spaces.

5. If you entered a new maintenance domain name in the **Domain** list, select a level (1 through 7) for the maintenance domain from the **Level** list.

   If you selected a maintenance domain from the **Domain** list, the **Level** automatically displays.

6. Enter a name for the maintenance association in the **Association Name** field.

   The maintenance association name must be less than 21 characters with no spaces.

7. Enter an interval for the Continuity Check Messages (CCM) from the **CCM Interval** list.

   The default value is 10 seconds. Options include: 1 sec, 1 minute, 10 second, 10 minutes, 3.3 ms, 10 ms, and 100 ms.

8. Select a maintenance intermediate point (MIP) policy from the **MIP Policy** list.

   Options include:

   - **Default** — Creates MIPs in all service ports for a particular maintenance domain.
   - **Explicit** — Only creates a MIP when there is a MEP on the port at a lower level maintenance domain.

9. To add a MEP, complete the following steps.
    a. Select a product from the **Product** list.

       The list contains all products that are part of the VPLS.

    b. Select a VLAN ID from the **VLAN ID** list.

       The list contains all VLAN IDs in the VPLS.

    c. Select a port from the **Port** list.

       The list contains all VPLS end-points for the selected VLAN ID.

    d. Enter a unique identifier for the end-point in the End Point ID field.

       Valid values include 1 through 8191.

    e. Select the MEP direction from the **Direction** list.

       Options include:

       - **Up** — Select to set the MEP direction away from the monitored VLAN.
       - **Down** — Select to set the MEP direction towards the monitored VLAN.

    f. Click the right arrow button to move the defined MEP to the **Selected Maintenance End Points** table.

       The **Selected Maintenance End Points** table lists the configured MEPs. Repeat step 9 for each MEP you want to add.

10. To edit a MEP, complete the following steps.
    a. Select a MEP in the **Selected Maintenance End Points** table and click the left arrow button to edit it in the **Available Maintenance End Points** area.

    b. Select a product from the **Product** list.

       The list contains all products that are part of the VPLS.

    c. Select a VLAN ID from the **VLAN ID** list.

       The list contains all VLAN IDs in the VPLS.

    d. Select a port from the **Port** list.

       The list contains all VPLS end-points for the selected VLAN ID.

    e. Enter a unique identifier for the end-point in the End Point ID field.

       Valid values include 1 through 8191.

    f. Select the MEP direction from the **Direction** list.

       Options include:

       - **Up** — Select to set the MEP direction away from the monitored VLAN.
       - **Down** — Select to set the MEP direction towards the monitored VLAN.

    g. Click the right arrow button to move the defined MEP to the **Selected Maintenance End Points** table.

       The **Selected Maintenance End Points** table lists the configured MEPs. Repeat step 10 for each MEP you want to edit.

11. Click **OK** on the **Edit Maintenance Association** dialog box.

    The **Deploy to Products** dialog box displays.

12. Select one of the following options:

    - **Save to running** — Select to update the running configuration; however, the deployment is not saved to the product's flash memory.
    - **Save to running and startup** — Select to update the running configuration as well as save the deployment configuration to the product's flash memory. Selecting this option is the equivalent to a write memory command on the product CLI.
    - **Save to running and startup then reboot** — Select to update the running configuration, save the deployment configuration to the product's flash memory, and reboot the product. Selecting this option is the equivalent to entering a write memory and a reload command on the product CLI.

13. Click **OK** on the **Deploy to Products** dialog box.

    The **Deployment Status** dialog box displays.

    While deployment is in progress, you can do the following:

    - Click **Abort** to stop deployment of the entire configuration.

      NOTE
      The abort action does not stop the tasks that have already started.

    - Click **Close** to close the **Deployment Status** dialog box.

      NOTE
      Closing the Deployment Status dialog box does not stop deployment of the configuration.

    After deployment is complete, you can select an entry in the **Deployment Status** list to display details about the deployment in the **Status Details** field.

14. Click **Close** on the **Deployment Status** dialog box.

    The **Configure 802.1ag CFM** dialog box displays with the new association in the **Maintenance Association Details** table.

15. Click **Close** on the **Configure 802.1ag CFM** dialog box.

Adding a MEP to a maintenance association

You can access 802.1ag CFM from the following features:

- VPLS Manager (requires the IP - MPLS – VLL prvilege with read-write or read-only permission)
- VLL Manager (requires the IP - MPLS – VPLS prvilege with read-write or read-only permission)
- VLAN Manager (requires the VLAN Manager prvilege with read-write or read-only permission)

NOTE
802.1ag CFM is only supported on IronWare Ethernet Routers devices running firmware release 5.2 or later.

NOTE
You cannot configure an 802.1ag CFM on a maintenance end point (MEP) configured with dual tagged VLANs.

To add a MEP to an existing maintenance association, complete the following steps.

1. Click **802.1ag CFM**.

   The **Configure 802.1ag CFM** dialog box displays.

2. Select the maintenance association you want to edit in the **Maintenance Association Details** table.

3. Click **Edit**.

   The **Edit Maintenance Association** dialog box displays.

4. In the **Available Maintenance End Points** area, select a product from the **Product** list .

   The list contains all products that are part of the VPLS.

5. Select a VLAN ID from the **VLAN ID** list.

   The list contains all VLAN IDs in the VPLS.

6. Select a port from the **Port** list.

   The list contains all VPLS end-points for the selected VLAN ID.

7. Enter a unique identifier for the end-point in the End Point ID field.

   Valid values include 1 through 8191.

8. Select the MEP direction from the **Direction** list.

   Options include:

   - **Up** — Select to set the MEP direction away from the monitored VLAN.
   - **Down** — Select to set the MEP direction towards the monitored VLAN.

9. Click the right arrow button to move the defined MEP to the **Selected Maintenance End Points** table.

   The **Selected Maintenance End Points** table lists the configured MEPs. Repeat step 4 through step 10 for each MEP you want to add.

10. Click **OK** on the **Edit Maintenance Association** dialog box.

    The **Deploy to Products** dialog box displays.

11. Select one of the following options:

    - **Save to running** — Select to update the running configuration; however, the deployment is not saved to the product's flash memory.
    - **Save to running and startup** — Select to update the running configuration as well as save the deployment configuration to the product's flash memory. Selecting this option is the equivalent to a write memory command on the product CLI.
    - **Save to running and startup then reboot** — Select to update the running configuration, save the deployment configuration to the product's flash memory, and reboot the product. Selecting this option is the equivalent to entering a write memory and a reload command on the product CLI.

12. Click **OK** on the **Deploy to Products** dialog box.

    The **Deployment Status** dialog box displays.

    While deployment is in progress, you can do the following:

    - Click **Abort** to stop deployment of the entire configuration.

      NOTE
      The abort action does not stop the tasks that have already started.

    - Click **Close** to close the **Deployment Status** dialog box.

      NOTE
      Closing the Deployment Status dialog box does not stop deployment of the configuration.

    After deployment is complete, you can select an entry in the **Deployment Status** list to display details about the deployment in the **Status Details** field.

13. Click **Close** on the **Deployment Status** dialog box.

    The **Configure 802.1ag CFM** dialog box displays with the updated details in the **Maintenance Association Details** table.

14. Click **Close** on the **Configure 802.1ag CFM** dialog box.

Editing a MEP

You can access 802.1ag CFM from the following features:

- VPLS Manager (requires the IP - MPLS – VLL prvilege with read-write or read-only permission)
- VLL Manager (requires the IP - MPLS – VPLS prvilege with read-write or read-only permission)
- VLAN Manager (requires the VLAN Manager prvilege with read-write or read-only permission)

NOTE
802.1ag CFM is only supported on IronWare Ethernet Routers devices running firmware release 5.2 or later.

NOTE
You cannot configure an 802.1ag CFM on a maintenance end point (MEP) configured with dual tagged VLANs.

To edit a MEP in an existing maintenance association, complete the following steps.

1. Click **802.1ag CFM**.

   The **Configure 802.1ag CFM** dialog box displays.

2. Select the maintenance association you want to edit in the **Maintenance Association Details** table.

3. Click **Edit**.

   The **Edit Maintenance Association** dialog box displays.

4. Select the MEP that you want to edit in the **Selected Maintenance End Points** table and click the left arrow button to edit it in the **Available Maintenance End Points** area.

5. Select a product from the **Product** list.

   The list contains all products that are part of the VPLS.

6. Select a VLAN ID from the **VLAN ID** list.

   The list contains all VLAN IDs in the VPLS.

7. Select a port from the **Port** list.

   The list contains all VPLS end-points for the selected VLAN ID.

8. Enter a unique identifier for the end-point in the End Point ID field.

   Valid values include 1 through 8191.

9. Select the MEP direction from the **Direction** list.

   Options include:

   - **Up** — Select to set the MEP direction away from the monitored VLAN.
   - **Down** — Select to set the MEP direction towards the monitored VLAN.

10. Click the right arrow button to move the updated MEP to the **Selected Maintenance End Points** table.

    The **Selected Maintenance End Points** table lists the configured MEPs. Repeat step 4 through step 10 for each MEP you want to edit.

11. Click **OK** on the **Edit Maintenance Association** dialog box.

    The **Deploy to Products** dialog box displays.

12. Select one of the following options:

    - **Save to running** — Select to update the running configuration; however, the deployment is not saved to the product's flash memory.
    - **Save to running and startup** — Select to update the running configuration as well as save the deployment configuration to the product's flash memory. Selecting this option is the equivalent to a write memory command on the product CLI.
    - **Save to running and startup then reboot** — Select to update the running configuration, save the deployment configuration to the product's flash memory, and reboot the product. Selecting this option is the equivalent to entering a write memory and a reload command on the product CLI.

13. Click **OK** on the **Deploy to Products** dialog box.

    The **Deployment Status** dialog box displays.

    While deployment is in progress, you can do the following:

    - Click **Abort** to stop deployment of the entire configuration.

      NOTE
      The abort action does not stop the tasks that have already started.

    - Click **Close** to close the **Deployment Status** dialog box.

      NOTE
      Closing the Deployment Status dialog box does not stop deployment of the configuration.

    After deployment is complete, you can select an entry in the **Deployment Status** list to display details about the deployment in the **Status Details** field.

14. Click **Close** on the **Deployment Status** dialog box.

    The **Configure 802.1ag CFM** dialog box displays with the updated details in the **Maintenance Association Details** table.

15. Click **Close** on the **Configure 802.1ag CFM** dialog box.

Viewing the MEPs in a maintenance association

You can access 802.1ag CFM from the following features:

- VPLS Manager (requires the IP - MPLS – VLL prvilege with read-write or read-only permission)
- VLL Manager (requires the IP - MPLS – VPLS prvilege with read-write or read-only permission)
- VLAN Manager (requires the VLAN Manager prvilege with read-write or read-only permission)

NOTE
802.1ag CFM is only supported on IronWare Ethernet Routers devices running firmware release 5.2 or later.

NOTE
You cannot configure an 802.1ag CFM on a maintenance end point (MEP) configured with dual tagged VLANs.

To view the MEPs in a maintenance association, complete the following steps.

1. Choose one of the following options:
   - From the **VPLS Manager** dialog box, **Views** tab, choose one of the following options:
     - Select a device from the **VPLS Peer Status/VPLS Name/VCID** list and click **802.1ag CFM**.
     - Select the **Peer Topology** tab and right-click a device in the topology and select **802.1ag CFM.**
   - From the **VLL Manager** dialog box, **Views** tab, select an instance from the **VLL Instances** table and click **802.1ag CFM.**
   - From the **VLAN Manager** dialog box - **VLAN View** or **Product View**, select a VLAN from list and click **802.1ag CFM.**

   The **Configure 802.1ag CFM** dialog box displays.
2. Select the maintenance association in the **Maintenance Association Details** list.

   The MEPs associated with the maintenance association display in the **Maintenance End Points (MEP)** table:
   - The product on which the MEP is located
   - The VLAN ID of the MEP
   - The port of the MEP
   - The user-defined end-point identifier of the MEP
   - The direction (up or down) of the MEP
3. Use the dialog box to perform any of the following tasks:
   - To add a MEP to a maintenance association, refer to “Adding a MEP to a maintenance association” on page 904.
   - To edit a MEP, refer to “Editing a MEP” on page 906.
   - To delete a MEP to a maintenance association, refer to “Deleting a maintenance association” on page 909.
   - To check the status of all remote MEPs for the selected MEP, refer to “Checking the connectivity status of remote MEPs” on page 910.

- To send a loopback message to a specific MEP or MIP in the domain, refer to "Sending a loopback message" on page 911.
- To send a linktrace message to a specific MEP or MIP in the domain, refer to "Sending a linktrace message" on page 912..

4. Click **Close** on the **Configure 802.1ag CFM** dialog box.

Deleting a maintenance association

You can access 802.1ag CFM from the following features:

- VPLS Manager (requires the IP - MPLS – VLL prvilege with read-write or read-only permission)
- VLL Manager (requires the IP - MPLS – VPLS prvilege with read-write or read-only permission)
- VLAN Manager (requires the VLAN Manager prvilege with read-write or read-only permission)

NOTE
802.1ag CFM is only supported on IronWare Ethernet Routers devices running firmware release 5.2 or later.

NOTE
Only maintenance domains that are not linked to other associations will be deleted.

To delete a maintenance association, complete the following steps.

1. Right-click a device and select **802.1ag CFM**.

   The **Configure 802.1ag CFM** dialog box displays.

2. Select one or more maintenance associations you want to delete in the **Maintenance Association Details** table.
3. Click **Delete**.

   A confirmation message displays with a **Delete the maintenance domain?** check box. Make sure that the check box is selected.

4. Click **Yes** on the confirmation message.

Checking the connectivity status of remote MEPs

Use the **802.1ag CFM Connectivity** dialog box to check the status of all remote maintenance end points (MEP) for the selected MEP. You can access 802.1ag CFM from the following features:

- VPLS Manager (requires the IP - MPLS – VLL prvilege with read-write or read-only permission)
- VLL Manager (requires the IP - MPLS – VPLS prvilege with read-write or read-only permission)
- VLAN Manager (requires the VLAN Manager prvilege with read-write or read-only permission)

NOTE
802.1ag CFM is only supported on IronWare Ethernet Routers devices running firmware release 5.2 or later.

NOTE
You cannot configure an 802.1ag CFM on a maintenance end point (MEP) configured with dual tagged VLANs.

To check the status of all remote MEPs for the selected MEP, complete the following steps.

1. Choose one of the following options:
   - From the **VPLS Manager** dialog box, **Views** tab, choose one of the following options:
     - Select a device from the **VPLS Peer Status/VPLS Name/VCID** list and click **802.1ag CFM**.
     - Select the **Peer Topology** tab and right-click a device in the topology and select **802.1ag CFM.**
   - From the **VLL Manager** dialog box, **Views** tab, select an instance from the **VLL Instances** table and click **802.1ag CFM.**
   - From the **VLAN Manager** dialog box - **VLAN View** or **Product View**, select a VLAN from list and click **802.1ag CFM.**

   The **Configure 802.1ag CFM** dialog box displays.
2. Select the MEP for which you want to check the status of remote MEPs in the **Maintenance End Points (MEP)** table.
3. Click **Connectivity**.

   The **802.1ag CFM Connectivity** dialog box displays.
4. Select the MEP for which you want to check the status of remote MEPs in the **Maintenance End Points (MEP)** table.
5. Click **Connectivity**.

   The **802.1ag CFM Connectivity** dialog box displays.
6. Review the connectivity details:
   - Source Product - The product that contains the selected MEP.
   - Domain - The domain of the selected MEP.
   - Association - The maintenance association of the selected MEP.
   - Source MEP - The port number of the selected MEP.
   - Connectivity Status table - Lists the connectivity status for each remote end point.
   - Remote MEP - The remote MEP identifier.

- Product - The product containing the remote MEP.
- Port - The port of the remote MEP.
- MAC Address - The MAC address of the remote MEP.
- Operational State - The state of the port attached to the MEP. Valid values include: Unknown, Idle, Start, Failed, and OK.

7. Click **Close** on the **802.1ag CFM Connectivity** dialog box.
8. Click **Close** on the **Configure 802.1ag CFM** dialog box.

Sending a loopback message

Use this dialog box to send a loopback message to a specific maintenance end point (MEP) or maintenance intermediate point (MIP) in the domain.

You can access 802.1ag CFM from the following features:

- VPLS Manager (requires the IP - MPLS – VLL prvilege with read-write or read-only permission)
- VLL Manager (requires the IP - MPLS – VPLS prvilege with read-write or read-only permission)
- VLAN Manager (requires the VLAN Manager prvilege with read-write or read-only permission)

NOTE
802.1ag CFM is only supported on IronWare Ethernet Routers devices running firmware release 5.2 or later.

NOTE
You cannot configure an 802.1ag CFM on a maintenance end point (MEP) configured with dual tagged VLANs.

Use loopback messages to identify fault locations by sending a query to maintenance end points (MEP) or maintenance intermediate points (MIP) along the service path of the domain.

To send a loopback message to a specific MEP or MIP in the domain, complete the following steps.

1. Choose one of the following options:
   - From the **VPLS Manager** dialog box, **Views** tab, choose one of the following options:
     - Select a device from the **VPLS Peer Status/VPLS Name/VCID** list and click **802.1ag CFM**.
     - Select the **Peer Topology** tab and right-click a device in the topology and select **802.1ag CFM.**
   - From the **VLL Manager** dialog box, **Views** tab, select an instance from the **VLL Instances** table and click **802.1ag CFM.**
   - From the **VLAN Manager** dialog box - **VLAN View** or **Product View**, select a VLAN from list and click **802.1ag CFM.**

   The **Configure 802.1ag CFM** dialog box displays.
2. Select the MEP for which you want to send a loopback message to a specific maintenance end point (MEP) or maintenance intermediate point (MIP) in the domain in the **Maintenance End Points (MEP)** table.

3. Click **Loopback**.

   The **802.1ag CFM Loopback** dialog box displays the product that contains the selected MEP, the domain, the maintenance association, and the port number of the selected MEP.

4. Select the MEP for which you want to send a loopback message to a specific maintenance end point (MEP) or maintenance intermediate point (MIP) in the domain in the **Maintenance End Points (MEP)** table.

5. Click **Loopback**.

   The **802.1ag CFM Loopback** dialog box displays.

6. Select one of the following destination options:

   - **MEP ID** — Select this option to send the loopback message to a MEP and enter the MEP ID in the field. THe MEP ID value can be 1 through 8191.
   - **MIP** — Select this option to send the loopback message to a MIP and enter the MAC address for the MIP.

7. Enter a timeout value in seconds (from 1 through 30) in the **Timeout** field.

8. Enter the number of loopback messages to send in the **Loopback Message Count** field. The loopback message count value can be from 1 through 1024.

9. Click **Execute**.

   The status of the loopback message displays one of the following status types:

   - **Success** (*Messages_Sent*/*Messages_Received*)
   - **Failed**

10. Click **Close** on the **802.1ag CFM Loopback** dialog box.

11. Click **Close** on the **Configure 802.1ag CFM** dialog box.

Sending a linktrace message

You can access 802.1ag CFM from the following features:

- VPLS Manager (requires the IP - MPLS – VLL prvilege with read-write or read-only permission)
- VLL Manager (requires the IP - MPLS – VPLS prvilege with read-write or read-only permission)
- VLAN Manager (requires the VLAN Manager prvilege with read-write or read-only permission)

NOTE
802.1ag CFM is only supported on IronWare Ethernet Routers devices running firmware release 5.2 or later.

NOTE
You cannot configure an 802.1ag CFM on a maintenance end point (MEP) configured with dual tagged VLANs.

Use linktrace messages to identify fault locations by sending a query to maintenance end points (MEP) or maintenance intermediate points (MIP) along the service path of the domain.

To send a link trace message to a specific MEP or MIP in the domain, complete the following steps.

1. Choose one of the following options:
   - From the **VPLS Manager** dialog box, **Views** tab, choose one of the following options:
     - Select a device from the **VPLS Peer Status/VPLS Name/VCID** list and click **802.1ag CFM**.
     - Select the **Peer Topology** tab and right-click a device in the topology and select **802.1ag CFM.**
   - From the **VLL Manager** dialog box, **Views** tab, select an instance from the **VLL Instances** table and click **802.1ag CFM.**
   - From the **VLAN Manager** dialog box - **VLAN View** or **Product View**, select a VLAN from list and click **802.1ag CFM.**

   The **Configure 802.1ag CFM** dialog box displays the product that contains the selected MEP, the domain, the maintenance association, and the port number of the selected MEP.
2. Select the MEP for which you want to send a link trace message to a specific maintenance end point (MEP) or maintenance intermediate point (MIP) in the domain in the **Maintenance End Points (MEP)** table.
3. Click **Linktrace**.

   The **802.1ag CFM Linktrace** dialog box displays.
4. Select the MEP for which you want to send a linktrace message to a specific maintenance end point (MEP) or maintenance intermediate point (MIP) in the domain in the **Maintenance End Points (MEP)** table.
5. Click **Linktrace**.

   The **802.1ag CFM Linktrace** dialog box displays.
6. Select one of the following destination options:
   - **MEP ID** — Select this option to send the linktrace message to a MEP and enter the MEP ID in the field. THe MEP ID value can be 1 through 8191.
   - **MIP** — Select this option to send the linktrace message to a MIP and enter the MAC address for the MIP.
7. Enter a timeout value in seconds (from 1 through 30) in the **Timeout** field.
8. Enter the number of hops to allow before dropping the packet in the **Time to Live (TTL)** field. The time to live value is decremented by each router that forwards the message. The message is dropped if the time to live reaches zero. The time to live value can be from 1 through 64 hops.
9. Click **Execute** to send the linktrace message.

   The details of the hop display in the **Hop Details** table.

10. Review the hop details:

    - The **Hop Details** table lists the connectivity status for each remote MEP and MIP.
    - The hop number.
    - The MAC address of the remote MEP/MIP.
    - Whether the MEP or MIP forwarded the message.
    - The ingress or egress MEP and MIP.
        - For a linktrace on a VLAN service, displays the associated port name in the format of *Slot_Number/Port_Number*.
        - For a linktrace on a VLL or VPLS, displays the IPv4 address of the peer product.
    - The ingress or egress action, based on the MEP or MIP direction:
        - If direction is DOWN, displays **Ingress OK**.
        - If direction is UP, displays **Egress OK**.
    - Relay Action
        - If the linktrace message is forwarded, displays **FDB**.
        - If the linktrace message reaches the MEP or MIP, displays **HIT**.

11. Click **Close** on the **802.1ag CFM Linktrace** dialog box.
12. Click **Close** on the **Configure 802.1ag CFM** dialog box.

Configuring frame delay

You can access 802.1ag CFM from the following features:

- VPLS Manager (requires the IP - MPLS – VLL prvilege with read-write or read-only permission)
- VLL Manager (requires the IP - MPLS – VPLS prvilege with read-write or read-only permission)
- VLAN Manager (requires the VLAN Manager prvilege with read-write or read-only permission)

NOTE
802.1ag CFM Frame Delay is only supported on IronWare Ethernet Routers devices running firmware release 5.4 or later.

NOTE
You cannot configure an 802.1ag CFM on a maintenance end point (MEP) configured with dual tagged VLANs.

Use frame delay to identify fault locations by sending a query between maintenance end points (MEP) along the service path of the domain.

To determine frame delay between two MEPs, complete the following steps.

1. Choose one of the following options:
    - From the **VPLS Manager** dialog box, **Views** tab, choose one of the following options:
        - Select a device from the **VPLS Peer Status/VPLS Name/VCID** list and click **802.1ag CFM**.
        - Select the **Peer Topology** tab and right-click a device in the topology and select **802.1ag CFM.**

- From the **VLL Manager** dialog box, **Views** tab, select an instance from the **VLL Instances** table and click **802.1ag CFM.**
- From the **VLAN Manager** dialog box - **VLAN View** or **Product View**, select a VLAN from list and click **802.1ag CFM.**

The **Configure 802.1ag CFM** dialog box displays the product that contains the selected MEP, the domain, the maintenance association, and the port number of the selected MEP.

2. Select the MEP for which you want to configure frame delay in the **Maintenance End Points (MEP)** table.
3. Click **Delay**.

   The **802.1ag CFM Delay** dialog box displays with the following details:

   - **Source Product** - The product that contains the selected MEP.
   - **Domain Name** - The domain of the selected MEP.
   - **Association Name** - The maintenance association of the selected MEP.
   - **Source MEP** - The port number of the selected MEP.
4. Select one of the following destination options:

   - To configure the destiation by ID, select the **MEP ID** check box and select an ID from the list. The MEP ID list displays all available destination MEP IDs in the following format: *device_name - port_ID - destination_MEP_ID*.
   - To configure the destiation by MAC address, select the **MEP MAC Address** check box and select an address from the list.
5. Click **Execute** to determine the frame delay.

   The delay measurements between service end-points in the bottom of the dialog box:

   - Minimum: The minimum round trip frame delay time.
   - Maximum: The maximum round trip frame delay time.
   - Average: The average round trip frame delay time.

     If the average frame delay value is less than 1,000 microseconds, these values display in microseconds; otherwise, the frame delay value display in milliseconds.
6. Click **Close** on the **802.1ag CFM Delay** dialog box.
7. Click **Close** on the **Configure 802.1ag CFM** dialog box.

Chapter

VIP Servers

29

In this chapter

VIP Servers overview

The VIP Servers dialog box allows you to manage virtual IPs (VIPs) on a ServerIron device. A VIP is the virtual IP address or server name to which client browsers send requests. For detailed information on VIPs, refer to the *ServerIron Configuration Guide*.

The current version of the VIP Servers dialog box can be used to manage ServerIron devices running software version 09.5.02*n* or software release 10.2.01*c* or later.

No other software versions are supported.

VIP Server functions

Based on a Management application area of responsibility (AOR), the VIP Servers dialog box provides the following functions:

- Displays VIP addresses configured on a ServerIron device
- Displays virtual server and real server port bindings that have been configured on a ServerIron device
- Displays real server and virtual server port status
- Enables or disables real servers, real server ports, virtual servers, or virtual server ports

Viewing the VIP Servers

1. Click the **IP** tab on the Management application.
2. Select **Configure > Application Delivery > VIP Servers**.

   The **VIP Servers** dialog box displays, as shown in Figure 372.

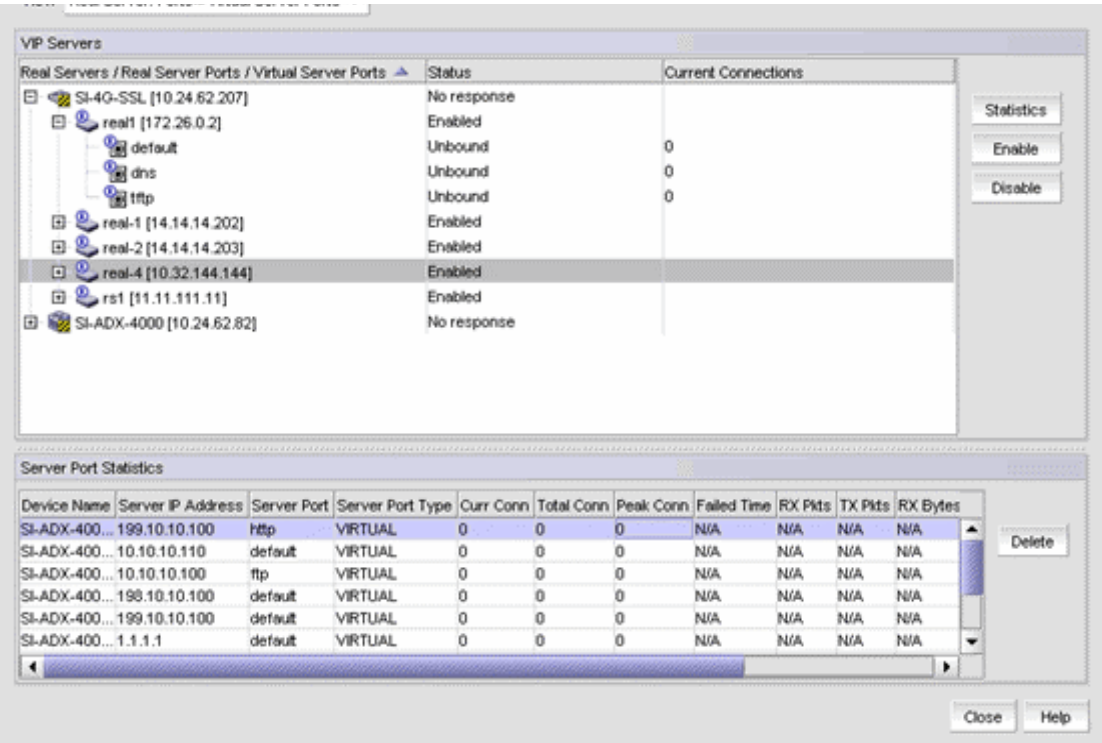


FIGURE 372 VIP Servers dialog box

The **View** list allows you to select which real server, real server port, virtual server, or virtual server ports you want to view. For detailed information, refer to "Viewing VIP Server information" on page 919.

The **VIP Servers** list displays the ServerIron devices that have been discovered by the Management application ports, and information about the real server or virtual server. Only the real servers and virtual servers in your area of responsibility (AOR) are displayed in this list.

The **VIP Servers** dialog box contains the following buttons:

- **Statistics** — Click to display the **Server Port Statistics** list, which shows statistics of the real server, virtual server, real server port, and virtual server port. For detailed information, refer to "Server port statistics" on page 921.
- **Enable** — Click to enable a real server, real server port, virtual server, or virtual server port using the **VIP Servers** dialog box. For step-by-step instructions, refer to "Enabling servers or server ports" on page 921.
- **Disable** — Click to disable a real server, real server port, virtual server, or virtual server port using the **VIP Servers** dialog box. For step-by-step instructions, refer to "Disabling servers or server ports" on page 921.
- **Delete** — Select a row in the **Server Port Statistics** list and click **Delete** to delete the statistics. For step-by-step instructions, refer to "Deleting a row from the Server Port Statistics list" on page 922.

Viewing VIP Server information

1. From the **View** list on the **VIP Servers** dialog box, select which ports you want to view from the following options:
   - Real server ports view of the virtual server, shown in Figure 373
   - Virtual server ports view of the real server, shown in Figure 374
   - Real server view of the virtual server, shown in Figure 375 on page 920
2. Click the plus sign (**+**) symbol next to an entry to expand all the real servers and virtual servers configured on the ServerIron device and port bindings between the real server ports and virtual server ports, or click the minus sign (**-**) symbol to collapse associated servers and ports.

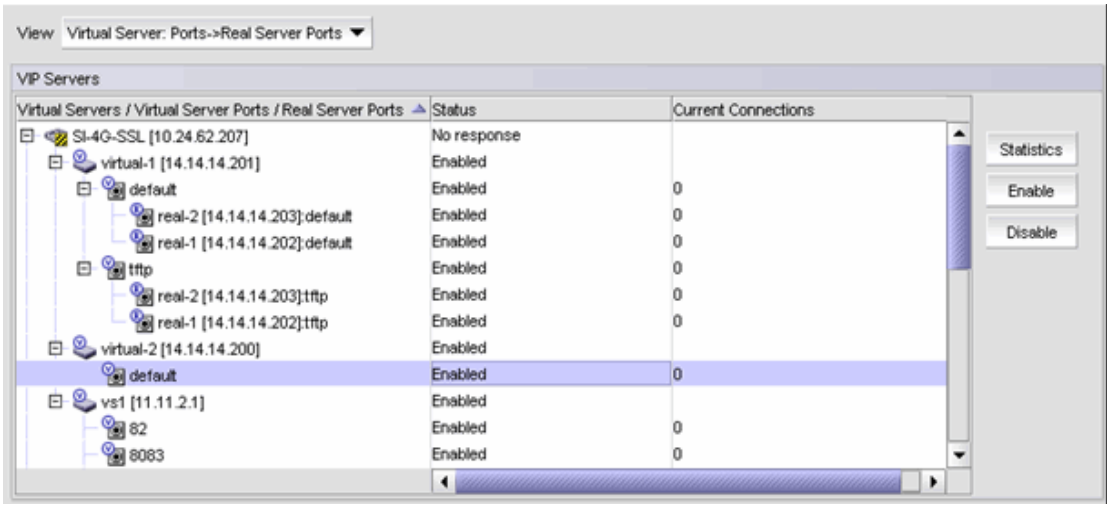


FIGURE 373 Real server ports view of the virtual server

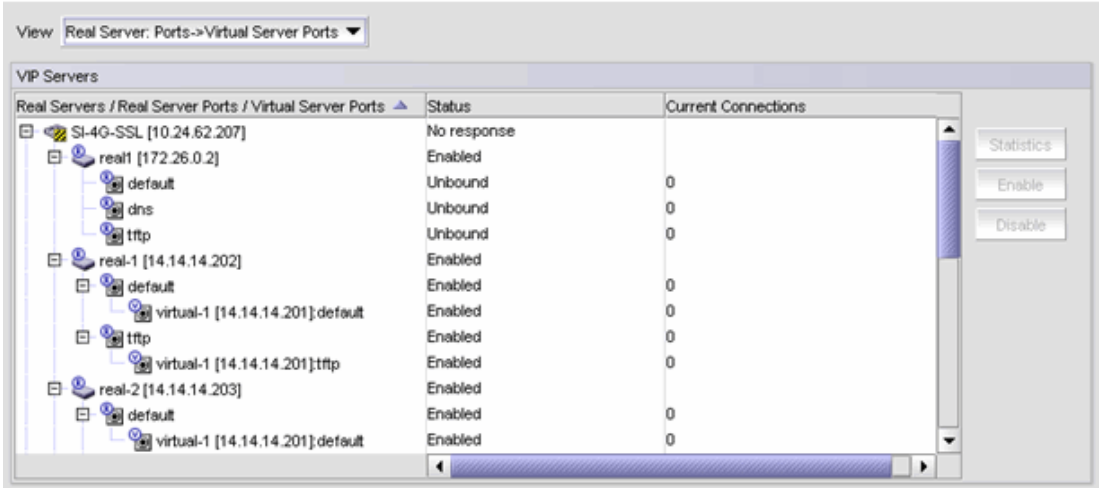


FIGURE 374 Virtual server ports view of the real server

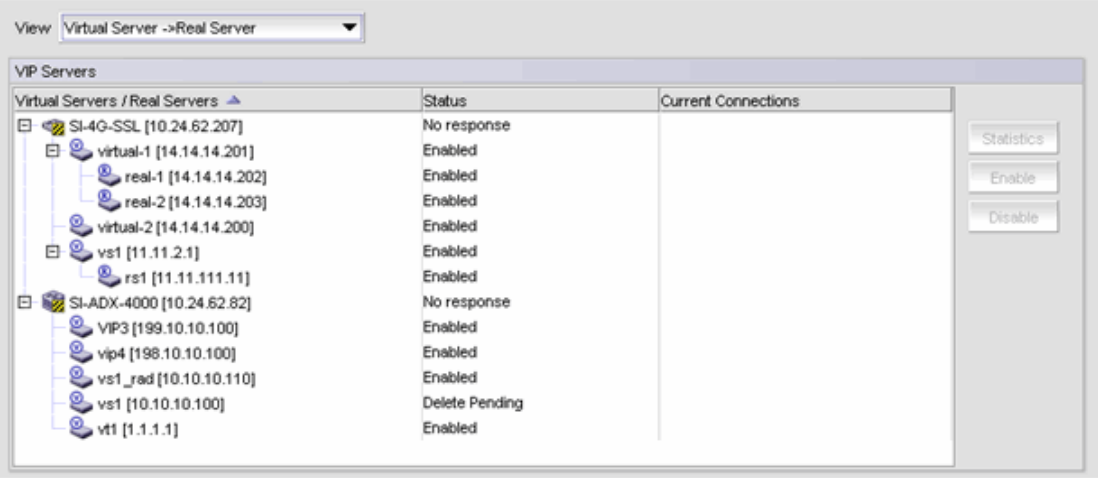


FIGURE 375 Real server view of the virtual server

The following fields describe the components in the **VIP Servers** list on the **VIP Servers** dialog box.

VIP Servers list

- The name and IP addresses of the real server or virtual server.
- The name or port numbers of the real server port or virtual server port.
- Only the servers in a Management application user's AOR are listed in the list. Also, if the server is down, that server is not listed in the list, even if it is in the user's AOR.
  - If you select **Virtual Server: Ports > Real Server Ports**, the display shows the virtual servers configured on a ServerIron device, and the virtual server ports configured under each virtual server.
  - You then see the real server ports to which the virtual server ports are bound.
  - If you select **Real Server: Ports > Virtual Server Ports**, the display shows the real servers configured on a ServerIron device, and the real server ports configured under each real server.
  - You then see the virtual server ports to which the real server ports are bound.
  - If you select **Virtual Server > Real Server**, you see the virtual servers and the real servers bound to them:
    - A **V** icon identifies the entry as a virtual server port.
    - An **R** icon indicates a real server port.

Status — The status of the real server, virtual server, or server port: Enabled, No response, or Delete Pending.

Current Connections — The number of current corrections on the real server port or virtual server port.

Enabling or disabling servers or server ports

If you have the **VIP Server Manager** privilege with read-write permission, you can enable and disable real servers, virtual servers, real server ports, and virtual server ports. If you have the **VIP Server Manager Leaf Node** privilege with read-write permission, you can enable and disable only the server leaf nodes. If you have both VIP-Server Mgr privilege and VIP-Server Mgr Leaf Node privilege with read-write permission, you can enable and disable on all levels.

Enabling servers or server ports

To enable a server or server port, complete the following steps:

1. Select the ServerIron device that has the servers or ports you want to enable and click the plus sign (**+**) symbol to expand its contents.
2. Select the server or port you want to enable, and click **Enable**.
3. When a confirmation message appears, click **Yes**.

Disabling servers or server ports

To disable a server or server port, complete the following steps.

1. Select the ServerIron device that has the server or port you want to disable and click the plus sign (**+**) symbol to expand its contents.
2. Select the server or port you want to disable, and click **Disable**.
3. When a confirmation message appears, click **Yes**.

Server port statistics

To monitor the statistics for real and virtual server ports on the **Server Port Statistics** list, shown in Figure 372 on page 918, complete the following steps.

1. Select one or more ServerIron devices, real servers, virtual servers, or server ports from the **VIP Servers** list.
2. Click **Statistics**.

   The **Server Port Statistics** list displays the following information:

   - Device Name — The name of the device and its IP address.
   - Server IP Address — The IP address of the server.
   - Server Port — The name of the server port.
   - Server Port Type — The type of server port: virtual or real.
   - Curr Conn — The number of current connections on the real or virtual server port.
   - Total Conn — The number of total connections on the real or virtual server port.
   - Peak Conn — The number of connections during peak time on the real or virtual server port.
   - Failed Time — The number of failed connections.

- RX Packets — The number of packets received by the port.
- TX Packets — The number of packets transmitted by the port.
- RX Bytes — The number of bytes received by the port.
- TX Bytes — The number of bytes transmitted by the port.
- Last Update — The date and time when information for the server was updated.

Deleting a row from the Server Port Statistics list

If you no longer need the statistics for a port, right-click the row of the port in the **Server Port Statistics** list and select **Delete**.

Chapter

Global Server Load Balancing 30

In this chapter

GSLB Manager

The Global Server Load Balancing (GSLB) Manager allows you to configure GSLB policies for a ServerIron ADX product. The ServerIron ADX product on which the GSLB protocol is enabled serves as a proxy to the Domain Name System (DNS) servers and evaluates the IP addresses in the DNS replies from the DNS server for which the ServerIron ADX product is a proxy. Based on the results of the evaluation, the GSLB ServerIron ADX product can change the order of the addresses in the reply so that the “best” host address for the client is on top.

The GSLB Manager feature is supported for ADP products (ServerIron version 09.0 and later and ADX version 12.0 or later) only. For more information on GSLB, refer to the ServerIron manuals.

Configuration requirements

Before using the GSLB Manager, confirm the following requirements:

- The GSLB Manager privilege is in your Management application user account or role.
- The ServerIron ADX products to which the policies, sites, and zones will be deployed are listed in the Network Object Manager tree. If they are not, make sure they are on the network that is being managed by the Management application. Then run discovery or add the ServerIron ADX products to the Management application using Network Object Manager.

Viewing the GSLB Manager

To view the GSLB Manager, perform the following steps.

Select **Configure > Application Delivery > GSLB**.

The **Policy Configuration** tab in the **GSLB** dialog box, shown in Figure 376, displays.

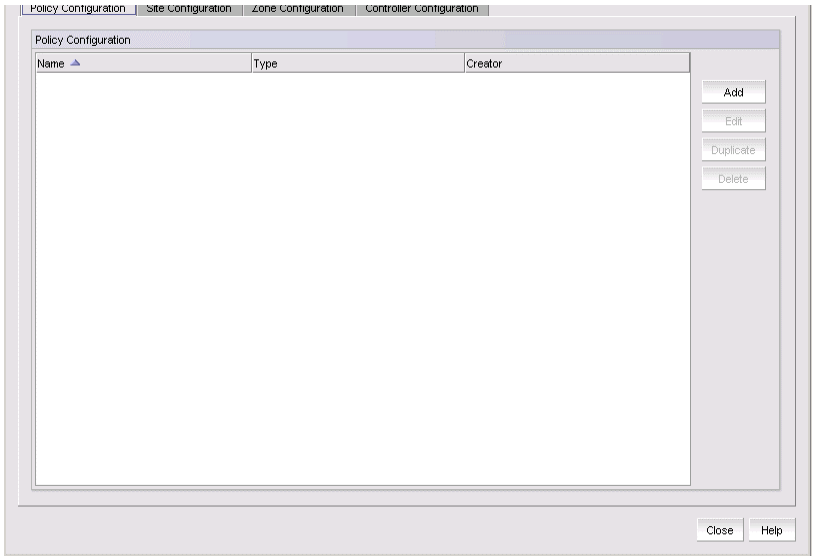


FIGURE 376 GSLB dialog box - Policy Configuration tab

The **GSLB** dialog box displays the following buttons:

- **Add —** Creates a new GSLB policy, site, or zone definition and a new controller configuration.
- **Edit** — Modifies existing GSLB Manager definitions and configurations.
- **Duplicate —** Creates a new definition or configuration by copying an existing one.
- **Delete —** Deletes a definition or configuration from GSLB Manager.

The **GSLB** dialog box contains the following tabs:

- **Policy Configuration —** GSLB policies are managed from this tab.
- **Site Configuration** — GSLB sites are managed from this tab.
- **Zone Configuration** — GSLB zones are managed from this tab.
- **Controller Configuration** — GSLB payloads are managed from this tab. GSLB payloads contain GSLB policies, sites, and zones and are deployed to GSLB controllers. Once deployed on the controller, DNS responses to GSLB zones are modified, based on the policies and site definitions.

GSLB policy management

A GSLB policy allows a GSLB ServerIron ADX product to evaluate each IP address in a DNS reply, based on defined criteria called *metrics*. The GSLB ServerIron ADX product can reorder the list of addresses and place the IP address for the best site at the top of the list.

Creating a GSLB policy

To create a GSLB policy, perform the following steps.

1. Select **Configure > Application Delivery > GSLB**.
2. Click the **Policy Configuration** tab.

   The **Policy Configuration** tab is displayed by default when you first launch GSLB Manager. The tab shows the name of the GSLB policies that have already been created in the Management application, and the Management application users who created them. The policy name and the user who created it uniquely identifies the GSLB policy.
3. Click **Add** to create a new GSLB policy.

   The **Policy Configuration** dialog box, shown in Figure 377, displays.

   There are two tabs on the **Policy Configuration** dialog box:

   - **Metrics** tab - The GSLB ServerIron ADX product evaluates each IP address in the DNS reply based on the metrics order. Based on the results, the GSLB ServerIron ADX product can reorder the list to place the IP address for the best site on the top of the list.
   - **Prefix** tab - The GSLB ServerIron ADX product keeps a list of prefixes in its cache that contains round-trip time (RTT) information. RTT is the amount of time it takes for a remote site to initiate a TCP connection from the client plus the amount of time until the remote site receives the client acknowledgment of the connection request.

     When the GSLB ServerIron ADX product receives RTT information, the IP address of the client is compared to the prefixes in the cache. If the address fits within the network of one of the prefixes, the GSLB ServerIron ADX product stores the RTT information for that site under the prefix entry.

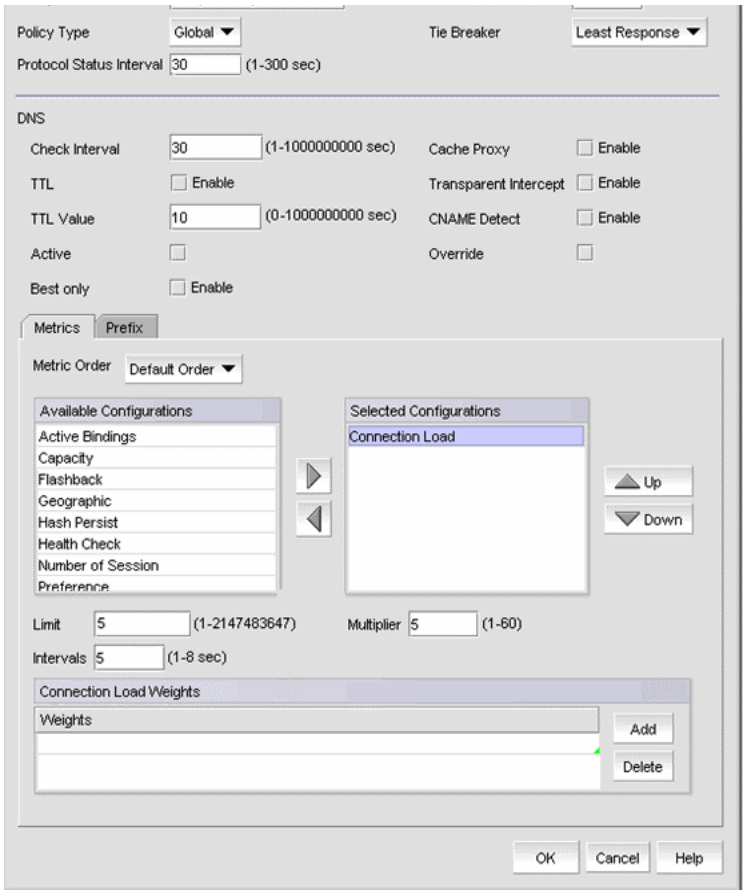


FIGURE 377 Policy Configuration dialog box - Metrics tab

4. Provide the following information on the **Policy Configuration** dialog box.
   a. Enter a policy name for the GSLB policy in the **Policy Name** field. The combination of a GSLB policy name and the Management application user who created it must be unique.
   b. Select the policy type from the **Policy Type** list. Options include the Global or Host policy types.
   c. In the **Protocol Status Interval** field, specify how often the site ADC/ADX products report their session list statistics and CPU utilization to the GSLB ServerIron ADX product.
   d. Specify the health status in the **Health Status Interval** field. This number determines the interval at which the ServerIron ADX products report the health check information to the GSLB ServerIron ADX product.

NOTE
If the health status interval is configured globally (that is, if the policy type is **Global**), the interval applies to all peer site ADC/ADX products that support the distributed health check feature.

e. Select the tie breaker method from the **Tie Breaker** list. This value is used in case multiple addresses pass the policy criteria without one address emerging as the best choice:

- **Least Response**: Selects the address of the site that has been selected least often in previous DNS responses.
  Note: ADX-type products do not support the **Least Response** tie-breaker method.
- **Round Robin**: Selects the first IP address in the DNS response for the first client request, then selects the next address for the next client request, and so on.

5. Provide the following additional information for Domain Name System (DNS) servers.

a. In the **Check Interval** field, indicate how often the GSLB ServerIron ADX product refreshes its zone and host information with DNS servers.

b. Select the **TTL** check box if you want the ServerIron ADX product to modify the Time to Live (TTL) value in DNS responses before sending the responses to the client DNS server.

c. If the **TTL** check box is selected, enter the number of seconds in the **TTL Value** field. The GSLB ServerIron ADX product changes the time to live (TTL) in each DNS record in the DNS responses before sending them to the client DNS server. If the **TTL** check box is not selected, the ServerIron ADX product does not change the TTLs, regardless of the value in this field.

d. Select the **Active** check box if you want the ServerIron ADX product to remove IP addresses obtained from DNS replies that fail a health check. The ServerIron ADX product removes these addresses as long as the DNS query contains at least one address that passes the health check.

By default, the GSLB ServerIron ADX product retains the same number of IP addresses in the DNS replies from the DNS server. The GSLB policy swaps the IP address on the top of the list with the best address selected by the GSLB policy.

e. If you do not want the default behavior, select the **Best only** check box to allow the ServerIron ADX product to remove all addresses except the one that the host-level GSLB policy selects as the best address.

f. Select the **Cache Proxy** check box if you want the ServerIron ADX product to act as a proxy for a DNS server, by responding directly to the client queries without forwarding them to the DNS server.

g. Select the **Transparent Intercept** check box if you want the ServerIron ADX product to either redirect or directly respond to client requests only for domains configured on the ServerIron ADX product. If the domain name requested by the client is not configured on the ServerIron ADX product, the query is forwarded to the DNS server without interception, and the reply is untouched by GSLB.

h. Select the **CNAME Detect** check box if you want the ServerIron ADX product to apply GSLB to Canonical Name (CNAME) records. A CNAME record refers to another domain name instead of an IP address.

i. Select the **Override** check box if you want the ServerIron ADX product to replace the IP address in the DNS reply with the IP address you configure for the proxy server.

Applying metrics on the Metrics tab

The GSLB ServerIron ADX product evaluates each IP address in the DNS reply based on the metrics order. Based on the results, the GSLB ServerIron ADX product can reorder the list to place the IP address for the best site on the top of the list.

To apply policy metrics, perform the following steps.

1. Click the **Metrics** tab on the **Policy Configuration** dial box.
2. Select the order from the **Metric Order** list. Metric order is the order in which the GSLB ServerIron ADX product applies the policy metrics:
   - **Default Order**: Metrics are applied in a fixed order as defined in the GSLB ServerIron ADX product.
   - **Select Order**: Metrics are applied in the order specified in this parameter.
3. Select the configuration you want from the **Available Configurations** list, and click the right arrow button to move it to the **Selected Configurations** list.

   If you want to remove the configuration from the **Selected Configurations** list, select the configuration, and click the left arrow button to move it back to the **Available Configurations** list.

   NOTE
   If **Select Order** is selected in the **Metric Order** list, metrics are applied in the order they appear in the **Selected Configurations** list. You can change the order of the configurations by selecting a configuration, and clicking the **Up** or **Down** button to move it up or down in the list.

4. If **Connection Load** is selected in the **Selected Configurations** list, enter values for the following options.

   NOTE
   If **Host** is selected as the policy type, these options are disabled.

   - **Limit** — Enter a load limit value for the connection. The valid limit range is from 1 through 2147483647 and the default value is 5.
   - **Multiplier** — Enter a multiplier value from 1 through 60. The default value is 5.
   - **Intervals** — Enter an interval value from 1 through 8. The default value is 5.
   - **Connection Load Weights**
     a. Click to add a row to the **Connection Load Weights** list, where you can add connection load weight values.
     b. Select a row and click to delete the row from the **Connection Load Weights** list.

Adding a prefix on the Prefix tab

1. Click the **Prefix** tab on the **Policy Configuration** dialog box, shown in Figure 378.
2. Click **Add**.

   A new row is added to the **Geo Prefix/Static Prefix** list.

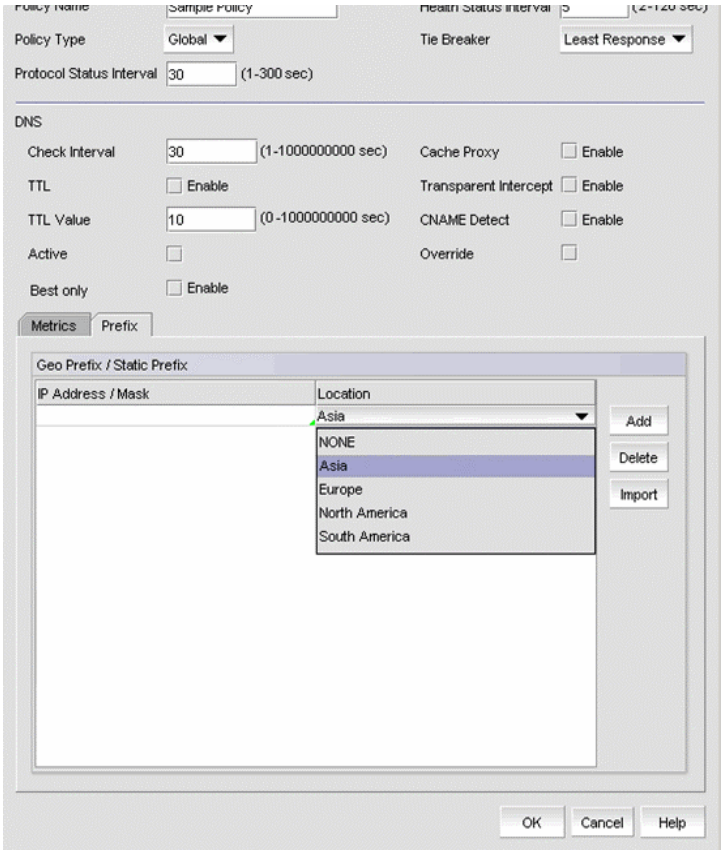


FIGURE 378 **Policy Configuration dialog box - Prefix tab**

3. Enter the IP address and select a location from the **Location** list.

   If you select **NONE** for the location, the prefix is considered static. If you select any other location, the prefix is considered geographical (Geo). Static prefixes never age out, but geographical prefixes are dynamic and can age out.

Deleting a prefix from the Prefix list

1. Click the **Prefix** tab on the **Policy Configuration** dialog box.
2. Select a row in the **Geo Prefix/Static Prefix** list.
3. Click **Delete**.

Importing IP addresses from a file

1. Select **Configure > Application Delivery > GSLB**.
2. Click the **Policy Configuration** tab.
3. In the **Geo Prefix/Static Prefix** list, click **Import**.

   The **List of Prefix Networks and Location** dialog box displays.
4. Click **Import** on the **Prefix** tab of the **Policy Configuration** dialog box.

   The **List of Prefix Networks and Locations** dialog box, shown in Figure 379, displays.

5. Enter a list of prefix networks and locations in the text box. Each entry should be on a separate line, and separate the prefix network and location with a comma. The location must be one of the following:
   - Asia
   - Europe
   - North America
   - South America
   - None

   If the location is **None**, it is added as a static prefix.
6. Select one of the following options:
   - **Overwrite:** Deletes and replaces any prefix in the list.
   - **Append**: Adds to the prefixes in the list.

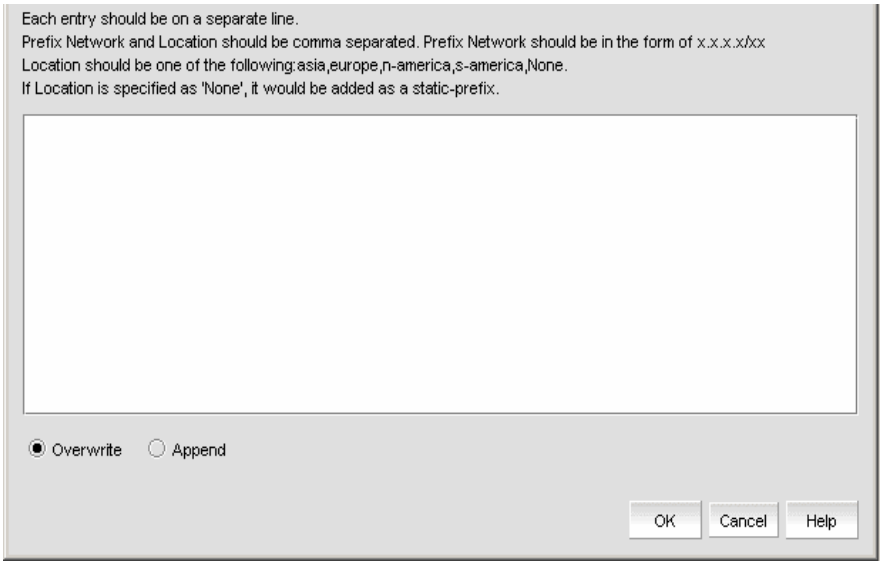


FIGURE 379 List of Prefix Networks and Location dialog box

7. Click **OK** to continue.

GSLB site management

The **Site Configuration** dialog box allows you to configure a GSLB ServerIron ADX product with site parameters. A GSLB site contains GSLB ServerIron ADX products that belong to that site.

Click the **Site Configuration** tab on the **GSLB** dialog box to view the GSLB sites that have been defined for the system, and perform one of the following tasks:

- Click **Add** to create a new GSLB site.
- Select an existing GSLB site, and click **Edit** if you want to modify it.
- Select an existing GSLB site, and click **Duplicate** if you want to create a new site by copying an existing site.

Adding a site configuration

1. Click **Add** on the **Site Configuration** tab on the **GSLB** dialog box.

   The **Site Configuration** dialog box displays, shown in Figure 380.

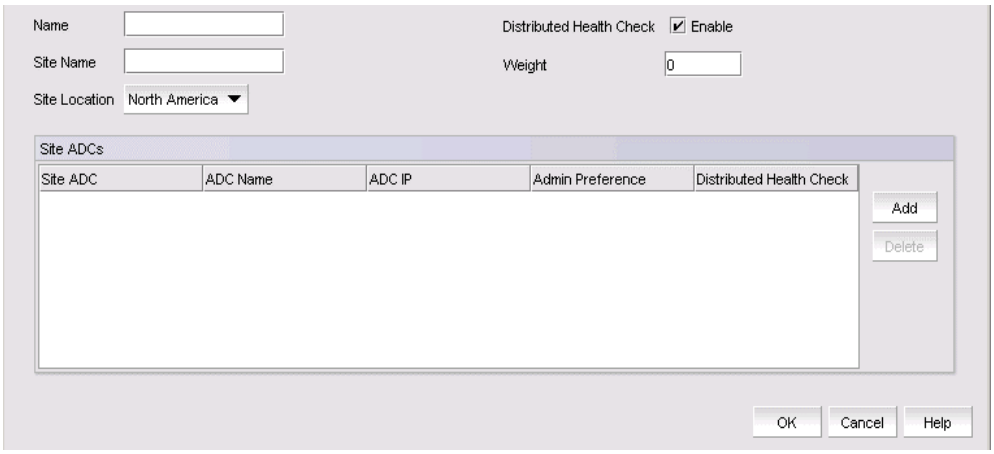


FIGURE 380 Site Configuration dialog box

2. Enter a name for the site configuration in the **Name** field and a site name in the **Site Name** field.
3. Select the location of the site from the **Site Location** list.
4. Select the **Distributed Health Check** check box if you want to enable health checks for all ServerIron ADX products at this site.
5. Enter the weight assigned to the ServerIron ADX product in the site in the **Weight** field. GSLB traffic can be distributed among GSLB sites based on weights configured for the sites. The weights determine the percentage of traffic each site receives in comparison with other sites, which may or may not have weights. Weight applies to all the ServerIron ADX products in the site.
   The weight can be from 0 through 100. The default is 0. If you want to use this weight, then do not enter IP weights in the zone configuration.

NOTE
The weight of the ServerIron ADX product displays in the **IP Weights** list of the **Add Hosts** dialog box.

Adding ServerIron ADX products to the site

You must add at least one site ADC/ADX product to create a site configuration.

1. Click the **Add** button.

   When you click **Add**, a row is added to the **Site ADCs** list. The ServerIron ADX products that the Management application has discovered appear in the **Site ADC** column. The name of the selected ServerIron ADX product displays in the **ADC Name** column. You can edit the ADC name.

2. Enter a value from 0 through 255 in the **Admin Preference** column to specify an administrative preference. The default is 128.

   The GSLB ServerIron ADX product prefers the site with the highest administrative preference. If you set the preference for a site ServerIron ADX product to 0, the site is administratively removed from GSLB selection.

   The GSLB ServerIron ADX product evaluates each IP address in the DNS reply based on a set of criteria. Depending on the results of this evaluation, the GSLB ServerIron ADX product reorders the list to place the best IP address on the top of the list. Usually, the GSLB ServerIron ADX product uses server health as one of the most important criteria to evaluate the server IP addresses in a DNS reply.

   The **Admin Preference** parameter overrides the setting for the **Distributed Health Check** parameter. You can select the type of health check that will be used. The site default uses the setting for the site **Distributed Health Check** parameter, described in step 4 of "Adding a site configuration" on page 931.

   - If enabled, the site default uses the health check for the ServerIron ADX product site instead of the health check for the GSLB site configured on the site **Distributed Health Check** parameter.
   - If disabled, the health check for this site ServerIron ADX product is disabled, even if the health check for the GSLB site is enabled.

3. Continue to add site ServerIron ADX products. When you have finished, click **OK** to save your changes.

   The new configuration is added to the **Site ADCs** products list.

NOTE
To delete a site ServerIron ADX product, select it from the **Site ADCs** list and click **Delete**.

GSLB zone configuration

When you manage GSLB zones, you specify the DNS zone name and the host information (applications) within each zone for which you want the GSLB ServerIron ADX product to provide GSLB. There are no defaults for zone parameters. As soon as you specify the hosts and applications, the GSLB ServerIron ADX product queries the DNS server (the one for which the GSLB ServerIron ADX product is a proxy) for the IP addresses associated with the hosts and begins sending health checks to the hosts.

Click the **Zone Configuration** tab on the **GSLB** dialog box to determine what zones have been configured for your system.

The **Hosts** list on the **Zone Configuration** dialog box shows the GSLB zones that have been defined and the Management application user who created the definition.

Managing zones

1. Select **Configure > Application Delivery > GSLB**.
2. Click the **Zone Configuration** tab on the **GSLB** dialog box and perform one of the following tasks:
   - Click **Add** to create a new GSLB zone.
   - Select an existing GSLB zone, and click **Edit** if you want to modify it.
   - Select an existing GSLB zone, and click **Duplicate** if you want to create a new zone by copying an existing zone.

Adding a zone configuration

You must add at least one host to create a zone configuration.

1. Click **Add** on the **Zone Configuration** dialog box on the **GSLB** dialog box.

   The **Zone Configuration** dialog box displays, as shown in Figure 381.

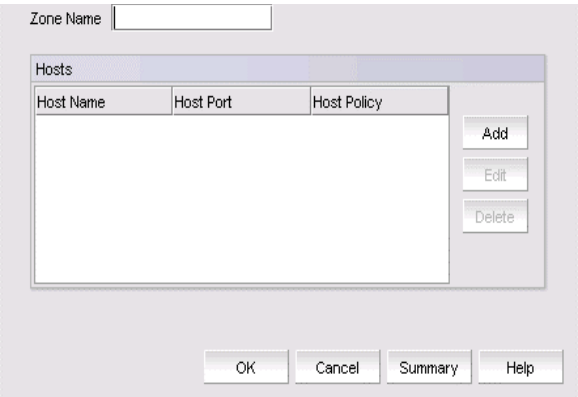


FIGURE 381 Zone Configuration dialog box

2. Enter a name for the zone in the **Zone Name** field.

   The combination of a GSLB zone name and the Management application user who created it must be unique.

3. Perform one of the following tasks:

   - Click the **Add** button to open the **Add Hosts** dialog box, where you can add hosts to a zone.
   - Select the host from the **Hosts** list, and click **Edit** to modify information for a host.
   - Select the host from the **Hosts** list, and click **Delete** to delete a host.

   When you click **Add** or **Edit**, the **Add Hosts** dialog box, shown in Figure 382, displays.

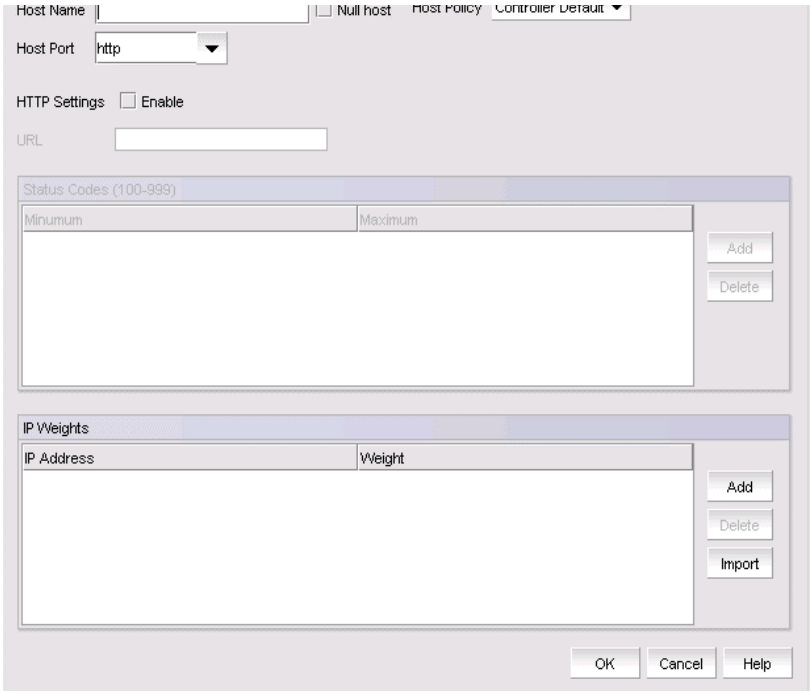


FIGURE 382 Add Hosts dialog box

Adding a host to a zone

The **Add Hosts** dialog box allows you to specify host information within each zone.

NOTE
When you specify the hosts and applications, the GSLB ServerIron queries the DNS server (the one for which the GSLB ServerIron is a proxy) for the IP addresses associated with the hosts and begins sending health checks to the hosts.

1. Enter the name of the host in the **Host Name** field. You do not need to enter the entire fully-qualified domain name (FQDN); you can enter only the host portion of the name. For example, if the FQDN is www.brocade.com, do not enter the entire name. Enter only “www”. The remainder of the name is already specified by the GSLB DNS zone name.

   When you configure a zone name in GSLB, you enter the zone name, then associate host applications with the zone name. For example, you might configure the following applications for the “brocade.com” zone:

   - www.brocade.com (HTTP application)
   - ftp.brocade.com (FTP application)

   Some e-commerce sites also accept just a zone name as an alias for a specific application within that zone. For example, a site might accept both “www.brocade.com” and “brocade.com” as valid names for the HTTP application on the web host. In this case, the second name has a null host name. No application is explicitly associated with the “brocade.com” zone, but the DNS server is configured to associate “foundyrnet.com” with the same IP addresses and application as “www.brocade.com” (for example, using address records or alias records).

2. Select the policy you want to deploy to the GSLB ServerIron ADX product from the **Host Policy** list. You can either select one of the policies defined under the **Host Policy** list or the policy that is the default for the controller.
3. Select the name of the well-known port or application from the **Host Port** list for which you want to provide GSLB.
4. Select the **HTTP Settings** check box to enable HTTP settings. For HTTP hosts, you can enable HTTP health checks.
   - If you enable HTTP settings, the **URL** field becomes available. Enter the URL that you want to use for HTTP health checks.
   - If you enable HTTP settings, the **Status Codes** list becomes available. When HTTP health checks are performed, the DNS server responds with a status code. If the status code is within a specified range, the server passes the health check. You can enter up to four ranges.
5. Enter the minimum status code number in the **Minimum** column and the maximum status code number in the **Maximum** column in the **Status Codes** list.
6. Click **Add** to add the status code ranges in the **Status Codes** list.

   NOTE
   To delete a range, select the range, then click **Delete** to remove it from the **Status Codes** list.

7. Click **Add** to add an IP address and weight in the **IP Weights** list.

The **IP Weights** list is used if IP Weights is specified in the selected policy (during site configuration using the **Site Configuration** dialog box). You assign a weight to an IP address so that the ServerIron ADX product distributes GSLB traffic among IP addresses in a DNS reply.

8. Enter the IP address to which you want to assign a weight in the **IP Address** column.
9. Enter a value from 0 through 100 in the **Weight** column. The default is 0.

NOTE
To delete an IP address and weight, select the entry, then click **Delete** to remove it from the **IP Weights** list.

10. Continue adding hosts to the **Add Hosts** dialog box. When you have finished, click **OK** to add the zone to the **Hosts** list of the **Zone Configuration** dialog box.

Deleting a zone configuration

To delete a zone configuration, complete the following steps.

1. Select the zone you want to delete from the **Hosts** list of the **Zone Configuration** dialog box.
2. Click **Delete**.
3. When the confirmation dialog box appears, click **Yes**.

Editing the list of IP addresses and weights

The **List of IP Addresses and Weights** dialog box allows you to import a list of IP addresses and weights by overwriting existing entries or appending to existing entries.

1. Select **Configure > Application Delivery > GSLB**.
2. Click the **Zone Configuration** tab.
3. Click **Add**.

   The **Zone Configuration** dialog box displays.
4. Click **Add**.

   The **Add Hosts** dialog box displays.
5. Click **Add** in the **IP Weights** list.

   The **List of IP Addresses and Weights** dialog box displays.
6. Enter a list of IP addresses into the **List of IP Addresses and Weights** text box. If a zone has IP weights, you can change the IP weights for a single host in a zone. Each entry must be on a separate line, separated by a comma.
7. Click the **Overwrite** option to select the option to overwrite existing IP addresses and weights.
8. Click the **Append** option to add new IP addresses and weights to the current list.

- "Adding a zone configuration" on page 933

Controller configuration

Once policies, sites, and zones are configured, you can assign and deploy a policy to a ServerIron ADX product that is the GSLB controller.

The **Controller Configuration** tab on the **GSLB** dialog box allows you to assign and deploy a policy to a ServerIron product that is the GSLB controller, after policies, sites, and zones are configured.

NOTE
All configuration options on the **Controller Configuration** tab are deployed to the selected GSLB controller. To site ServerIron ADX products, however, only the **GSLB Communication Port** and **Enable Logging** options are deployed.

1. Select **Configure > Application Delivery > GSLB**.
2. Click the **Controller Configuration** tab to view the controller definitions that have been defined for the system.

   The **Controller Configuration** tab displays.
3. Perform one of the following tasks:
   a. Click **Add** to launch the **Controller Configuration** dialog box, which you use to deploy a policy to a GSLB ServerIron ADX product that is the GSLB controller.
   b. Select an existing controller configuration and click **Edit** to modify an existing controller definition.
   c. Select an existing controller configuration and click **Duplicate** to create a controller configuration by copying an existing one.
   d. Select an existing controller configuration and click **Delete** to remove it from the **Controller Configuration** list.
   e. Click **Deploy** to deploy the selected controller configuration from the list.

NOTE
All configuration options on the **Controller Configuration** tab are deployed to the selected GSLB controller, but only the **GSLB Communication Port** and **Enable Logging** parameters are deployed to site GSLB ServerIron ADX products.

Creating a new GSLB controller configuration

1. Select **Configure > Application Delivery > GSLB**.

1. Click the **Controller Configuration** tab of the **GSLB** dialog box to view the controller definitions that have been defined for the system.

2. Click **Add** to create a new GSLB controller configuration, or select an existing GSLB controller configuration and click **Edit** or **Duplicate**.

   The **Controller Configuration** dialog box displays, as shown in Figure 383.

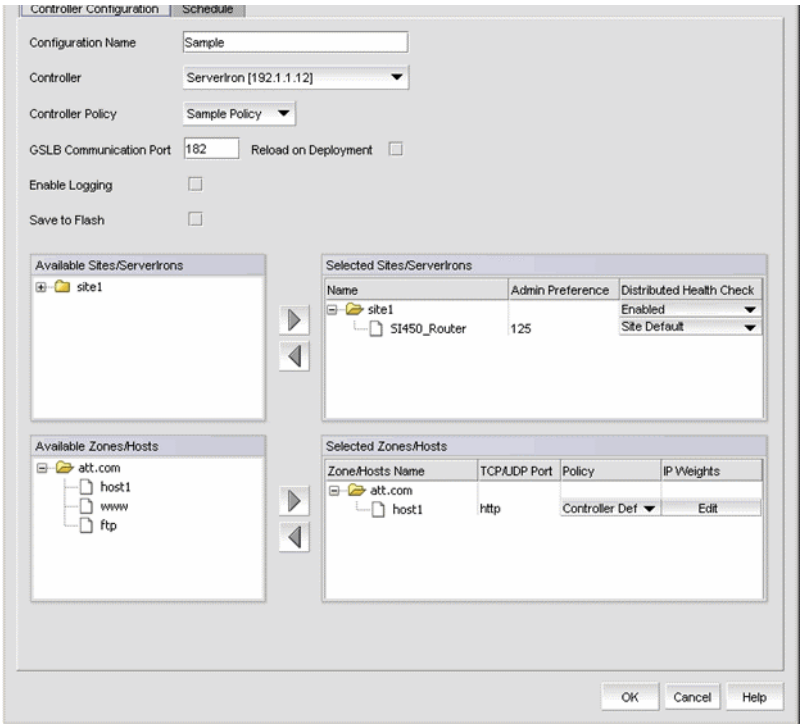


FIGURE 383 Controller Configuration dialog box

1. Enter a name for the configuration in the **Configuration Name** field. The combination of a GSLB controller name and the Management application user who created the definition must be unique.

2. Select the ServerIron ADX product from the **Controller** list that will be the GSLB controller.

3. Select the controller policy from the **Controller Policy** list that will be deployed to the controller. The list comes from the list on the **Policy Configuration** tab.

4. Enter the GSLB Communication Port number that the controller ServerIron ADX product will use for the GSLB protocol in the **GSLB Communication Port** field. This parameter setting is deployed to the controller and to site ServerIron ADX products specified in this configuration.

5. Select the **Reload on Deployment** check box if you want the ServerIron ADX product to perform a software reload when this configuration is deployed to the selected products.

6. Select the **Enable Logging** check box if you want to enable logging of the following information for DNS requests assisted by the GSLB ServerIron ADX product:

- Source IP address (the address of the client making the request)
- Best IP address (site address provided by the ServerIron ADX product)
- Host
- Zone
- Metric used

This parameter setting is deployed to the controller and to the site ServerIron ADX products specified in this configuration. When you enable logging of this information, the ServerIron ADX product generates a syslog message for each DNS request assisted by the ServerIron ADX product.

NOTE
The ServerIron ADX product sends the log messages only to the external syslog servers you have configured on the ServerIron ADX product. The messages do not appear in the ServerIron ADX product syslog buffer.

7. Select the **Save to Flash** check box if you want this configuration to be saved to the ServerIron ADX product memory when it is deployed to the product.
8. From the **Available Sites/ServerIrons** list, expand the site that contains the site ServerIron ADX product that will be under the controller ServerIron ADX control. The list of sites comes from the list on the **Site Configuration** tab.

   Select the site that you want to be controlled by the controller ServerIron ADX product and click the right arrow button to move it into the **Selected Sites/ServerIrons** list.

   The site name, administrative preference, and distributed health checks are listed in the list. Expand the entry for a site to display the individual ServerIron ADX products that belong to that site.

   If you want to overwrite the site administrative preference or distributed health check definition for one ServerIron ADX product, select the ServerIron ADX product, and enter new values for the **Administrative Preference** or **Distributed Health Check** parameters.
9. From the **Available Zones/Hosts** list, expand the zone that has the host that will be under the controller ServerIron ADX control. The list of zones comes from the list on the **Zone Configuration** tab.

   Select the host that you want and click the right arrow to move it into the **Selected Zones/Hosts** list. The zone or host name, TCP/UDP port, policy, and IP weights are listed in the list.
10. If a zone has IP weights, you can change the IP weights for a single host in a zone. Expand the zone, select the host, and click **Edit**.

    The **IP Weights** dialog box displays.

    a. Enter the IP address to which you want to assign an IP weight that is different from the one for the zone or host.

    b. Enter the IP weight in the **IP Weight** field.

    NOTE
    You can also add and delete IP addresses along with their IP weights.

11. When you have finished, click **OK** to add the configuration to the **Available Zones/Host** list on the **Controller Configuration** dialog box.

Deploying a controller configuration

Under GSLB Manager, only the entries under the **Controller Configuration** tab can be deployed to a ServerIron ADX product that will run the GSLB protocol. Controller configuration deployment can be scheduled or deployed on demand.

To schedule a controller configuration, refer to "Scheduling a deployment" on page 941.

To deploy a configuration on demand, complete the following steps.

1. Select **Configure > Application Delivery > GSLB**.
2. Click the **Controller Configuration** tab.
3. Select the configuration you want to deploy from the **Controller** list.
4. Click **Deploy**.

NOTE
When you deploy a controller configuration, the Management application deletes all GSLB configurations from the ServerIron ADX product to which the configuration is deployed, and then adds the configuration to the ServerIron ADX product. Therefore, make sure you deploy GSLB controller configurations when traffic is least likely to be affected.

The **Deployment status** progress indicator displays. Wait for the deployment to complete. The configuration remains under the **Configuration Controller** tab once it is deployed.

Scheduling a deployment

To schedule the deployment of a controller configuration, complete the following steps.

1. Select **Configure > Application Delivery > GSLB**.
2. Click **Add**, **Edit**, or **Duplicate** on the **Controller Configuration** tab.

   The **Controller Configuration** dialog box has two tabs: **Controller Configuration** and **Schedule**.
3. Click the **Schedule** tab of the **Controller Configuration** dialog box.

   The **Controller Configuration** dialog box - **Schedule** tab displays, as shown in Figure 384.

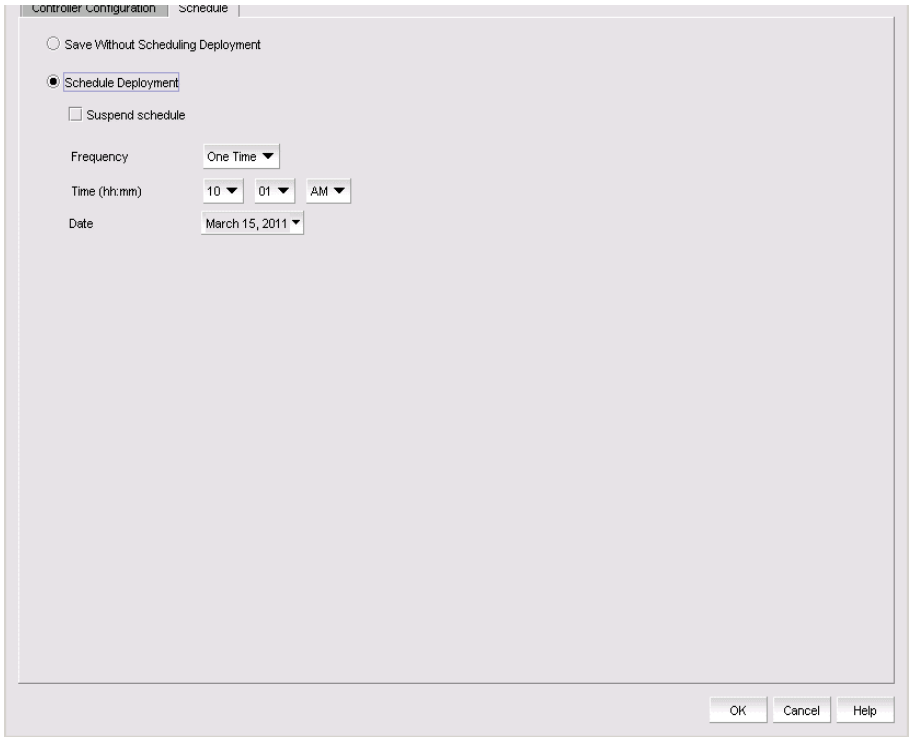


FIGURE 384 Controller Configuration dialog box - Schedule tab

4. Provide the following information.
   a. Click the **Save Without Scheduling Deployment** option if you want to save the deployment definition without scheduling it.
   b. Click the **Schedule Deployment** option if you want to schedule and save the deployment definition.

c. Select a schedule type from the **Frequency** list:

- **One Time**
- **Hourly**
- **Daily**
- **Weekly**
- **Monthly**
- **Yearly**

The **Time (hh:mm)** list appears if you select any schedule type except **Hourly**.

d. Select the time when the payload configuration will be deployed. Indicate the hour, minute, and whether it is AM or PM.

The **Minutes past the hour** list appears if you selected Hourly as the schedule type.

e. Select the minutes after the hour when the definition will be deployed.

The **Day of the Week** list appears if you select **Weekly** as the schedule type.

f. Select the day of the week when the definition will be deployed.

The **Day of the Month** list appears if you selected **Monthly** as the schedule type.

g. Select the day of the month when the definition will be deployed.

The **Date** list appears if you selected **One Time** or **Yearly** as the schedule type.

h. Indicate the date of the deployment.

i. Open the calendar and select the date.

ii. Select the **Suspend Scheduling** check box to disable the schedule.

Chapter

SSL Certificates for ServerIron Products

31

In this chapter

SSL certificates

SSL Certificates provides centralized Secure Sockets Layer (SSL) certificate and key management for ServerIron and ADX products that have the SSL capability. Use SSL Certificates to back up SSL certificates and keys from the ServerIron and ADX products, and restore them, as necessary. You can also add SSL certificates and keys to SSL certificates by cutting and pasting existing certificate and key file contents.

The SSL certificates and keys can only be deployed from the SSL Certificates dialog box to the following SSL-capable ServerIron devices:

- ServerIron with WSM6-SSL module, running software release 10.2.01c or later
- ServerIron with WSM6-SSL-Slave module, running software release 10.2.01c or later
- ServerIron 4G-SSL (Stackable), running software release 10.2.01c or later
- ADX running software release 12.1.00 or later

NOTE
If the ADX is running software release 12.3.00 or later, you can only view and manage SSL certificates that are bound to Virtual IP servers that are in your Area of Responsibility (AOR). To add a Virtual IP server to your AOR, refer to "Assigning products to an AOR" on page 197.

You must have the appropriate user privileges to access SSL Certificates.

NOTE
SSL Certificates does not generate signed certificates and keys. You can generate a certificate signing request (CSR), but the signed certificates and keys managed by SSL Certificates must be signed by a certificate authority (CA) and must be stored in an accessible location. Certificates and keys are added to SSL Certificates by cutting and pasting the certificate and key file contents obtained from a certificate authority into SSL Certificates.

You can configure SSL certificates preferences from the **Options** dialog box. For step-by-step instructions, refer to "Configuring SSL certificates preferences" on page 164.

You can import the SSL certificates and keys during discovery from SSL-capable products on the **Discover Setup - IP** dialog box. For step-by-step instructions, refer to "Defining global setting preferences" on page 60.

SSL certificate configuration

To access SSL Certificates, select **Configure > Application Delivery > SSL Certificates**.

The SSL Certificates dialog box has two tabs:

- The **Certificate View** tab (Figure 385).
- The **Product View** tab (Figure 386).

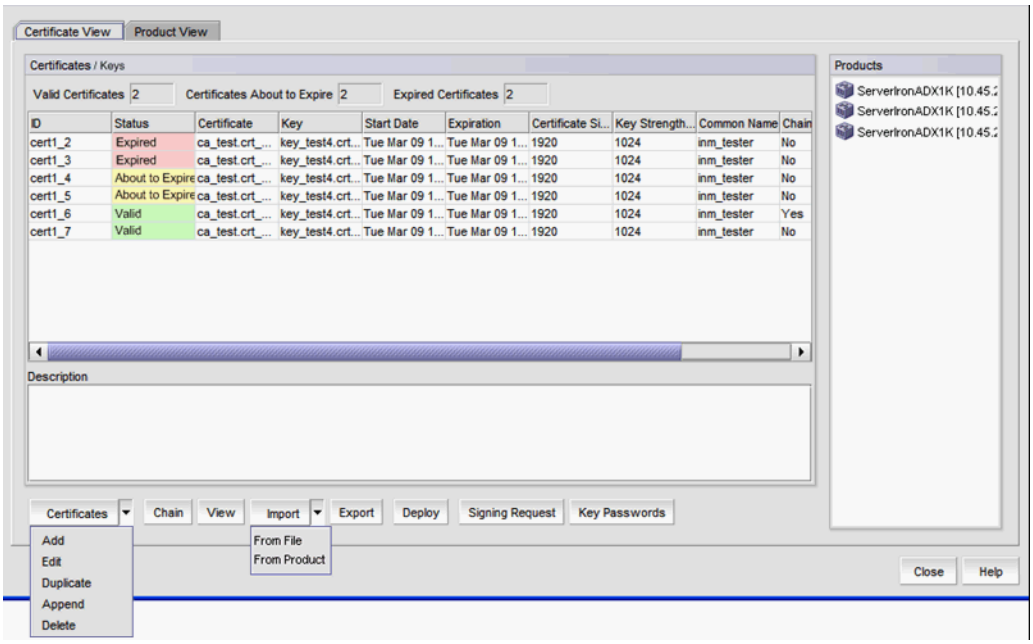


FIGURE 385 SSL Certificates dialog box - Certificate View tab

Accessing SSL certificates on the Certificate View tab

The **SSL Certificates** dialog box **Certificate View** tab allows you to view, add, edit, duplicate, append, delete, chain, import, export, and deploy SSL certificates. You can also create a certificate signing request (CSR) and create key passwords from this tab.

The SSL certificates and keys can only be deployed from SSL Certificate Manager to the following SSL-capable IronWare OS devices:

- ServerIron with WSM6-SSL module, running software release 10.2.01c or later
- ServerIron with WSM6-SSL-Slave module, running software release 10.2.01c or later
- ServerIron 4G-SSL (Stackable), running software release 10.2.01c or later
- ADX running software release 12.1.00 or later

NOTE
If the ADX is running software release 12.3.00 or later, you can only view and manage SSL certificates to Virtual IP servers that are in your Area of Responsibility (AOR). To add a Virtual IP server to your AOR, refer to "Assigning products to an AOR" on page 197

The **Certificate View** tab contains the following fields and components.

- Certificates/Keys — A table displaying certificates and certificate information.
- Products — A tree structure showing products that have certificates/keys. When you select a certificate/key, the product associated with that certificate/key is highlighted.
- Valid Certificates — The number of valid certificates.
- Certificates About to Expire — The number of certificates that are about to expire.
- Expired Certificates — The number of certificates that have expired.
- ID — A unique system-assigned ID for each certificate entry.
- Status — Possible values are Valid, About to Expire, or Expired.
- Certificate — The user-assigned certificate name. The same name may be used on different products.
- Key — The user-assigned key name. The same name may be used on different products.
- Start Date — The start date for the certificate. If only a key is present, this field is blank. For chained certificates, the date for the last certificate in the chain is displayed.
- Expiration — The expiration date for the certificate. If only a key is present, this field is blank. For chained certificates, the date for the last certificate in the chain is displayed.
- Certificate Size — The certificate size in bytes. If only a key is present, this field is blank.
- Key Strength — The key strength (size in bits). If only a certificate is present, this field is blank.
- Common Name — The common name for the certificate. For chained certificates, the name for the last certificate in the chain is displayed.
- Chain — Yes if certificates are chained, No if certificates are not chained. If only a key is present, this field is blank.
- Need Deploy — Yes if the certificate or key is not deployed to the product. No if the certificate or key is deployed to the product.
- Description — A text area that shows user comments and annotations.
- **Certificates** selector — Use this selector to Add, Edit, Duplicate, Append, or Delete certificates.
- **Chain** button — Use to chain certificates.
- **View** button — Use to view certificates.
- **Import** selector — Use this selector to import a certificate or key from a file or a product.

- **Export** button — Use to export a certificate.
- **Deploy** button — Use to deploy certificates.
- **Signing Request** button — Use to generate certificate signing request.
- **Key Passwords** button — Use to add or edit a key password.

Accessing SSL certificates on the Product View tab

The **SSL Certificates** dialog box **Certificate View** tab allows you to view, add, edit, duplicate, append, delete, chain, import, export, and deploy SSL certificates. You can also create a certificate signing request (CSR) and create key passwords from this tab.

The SSL certificates and keys can only be deployed from SSL Certificate Manager to the following SSL-capable IronWare devices:

- ServerIron with WSM6-SSL module, running software release 10.2.01c or later
- ServerIron with WSM6-SSL-Slave module, running software release 10.2.01c or later
- ServerIron 4G-SSL (Stackable), running software release 10.2.01c or later
- ADX running software release 12.1.00 or later

NOTE
If the ADX is running software release 12.3.00 or later, you can only view and manage SSL certificates that are bound to Virtual IP servers that are in your Area of Responsibility (AOR). To add a Virtual IP server to your AOR, refer to "Assigning products to an AOR" on page 197

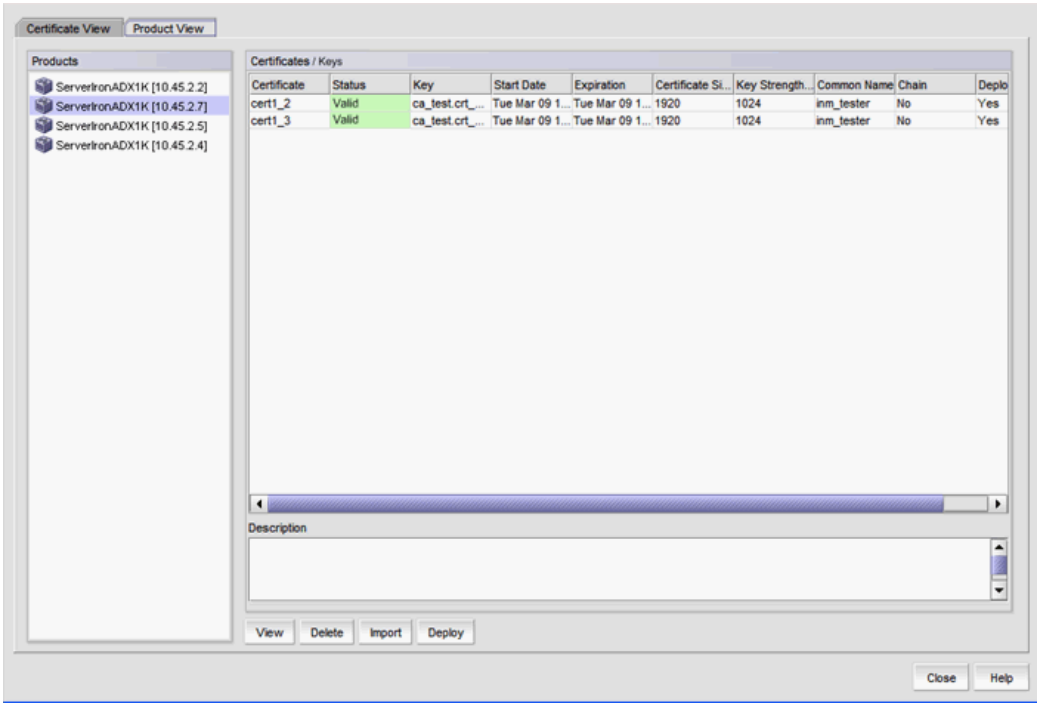


FIGURE 386 SSL Certificates dialog box - Product View tab

The **Product View** tab contains the following fields and components.

- Products — A product tree structure. When you select a product, certificates are displayed under Certificates.
  If the ADX is running software release 12.3.00 or later, you can only view and manage SSL certificates to Virtual IP servers that are in your Area of Responsibility (AOR). To add a Virtual IP server to your AOR, refer to "Assigning products to an AOR" on page 197
- Certificates/Keys — A list of certificates by product.
- Certificate — The user-assigned certificate name. The same name may be used on different products.
- Status — Possible values are Valid, About to Expire, or Expired.
- Key — The user-assigned key name. The same name may be used on different products.
- Start Date — The start date for the certificate. If only a key is present, this field is blank. For chained certificates, the date for the last certificate in the chain is displayed.
- Expiration — The expiration date for the certificate. If only a key is present, this field is blank. For chained certificates, the date for the last certificate in the chain is displayed.
- Certificate Size — The certificate size in bytes. If only a key is present, this field is blank.
- Key Strength — The key strength (size in bits). If only a certificate is present, this field is blank.
- Common Name — The common name for the certificate. For chained certificates, the name for the last certificate in the chain is displayed.
- Chain — Yes is certificates are chained, No if certificates are not chained. If only a key is present, this field is blank.
- Need Deploy — Yes if the certificate or key is not deployed to the product. No if the certificate or key is deployed to the product.
- **View** button — Launches the View Certificate dialog box.
- **Delete** button — Deletes a selected certificate.
- **Import** button — Import a certificate or key from a file.
- **Deploy** button — Launches the Deploy Certificate/Key dialog box.

Generating a certificate signing request

You can use SSL Certificates to generate a certificate signing request (CSR). The CSR must be submitted to a certificate authority (CA) for signing. The signed certificate is then exported from the CA to a secure location. It can then be imported into SSL Certificates.

1. Select **Configure > Application Delivery > SSL Certificates**.

   The **SSL Certificates** dialog box displays.

2. Click **Signing Request**.

   The **Certificate Signing Request** dialog box displays (Figure 387).

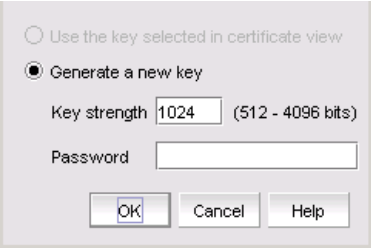


FIGURE 387 Certificate Signing Request dialog box

If the selected certificate key entry has a key, the **Use the key selected in certificate view** option is automatically selected.

If a key is not available for the selected entry, the **Generate a new key** option is automatically selected.

3. Choose one of the following options:
   - Select the **Use the key selected in certificate view** option to use the certificate key entry selected on the **Certificate View** tab of the **SSL Certificates** dialog box. Go to step 6.
   - Select the **Generate a new key** option to generate a new key. Continue with step 4.
4. Enter a number in the **Key strength** field.

   The key strength is from 512 through 4096 bits. The default is 1024 bits.
5. Enter the password in the **Password** field.

   The password is from 4 through 254 characters, case-sensitive, and allows all printable ASCII characters.
6. Click **OK**.

   The **Generate CSR Key** dialog box displays (Figure 388).

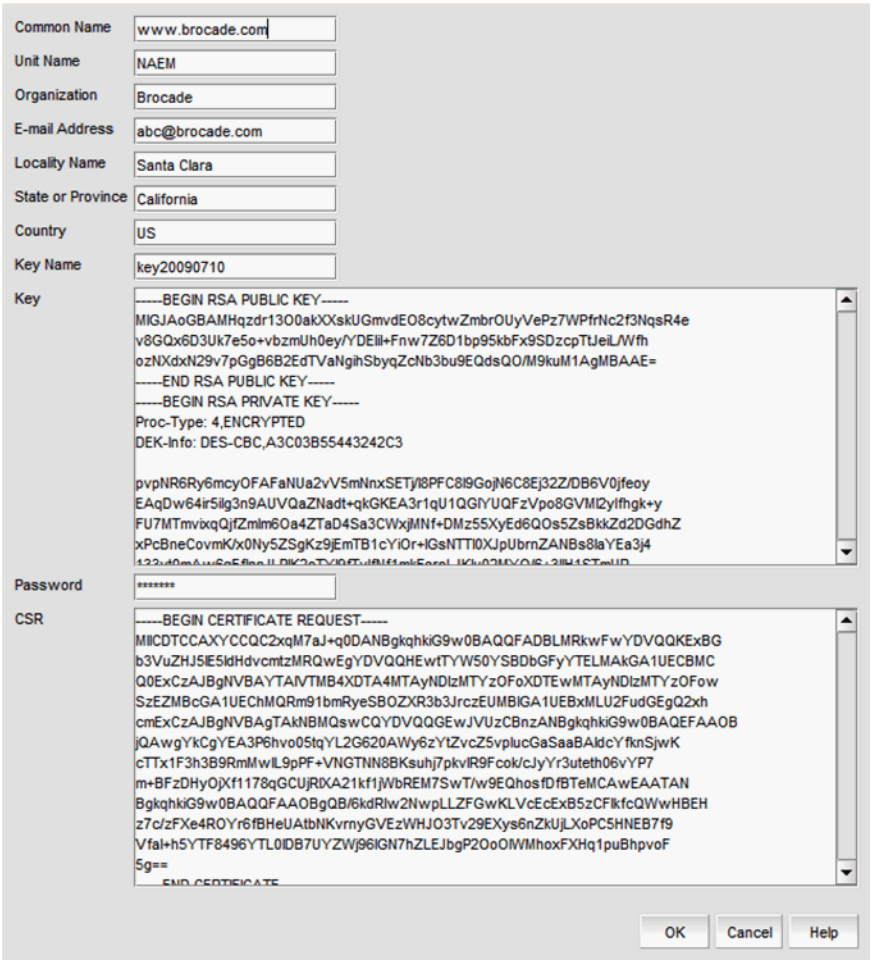


FIGURE 388 Generate CSR Key dialog box

7. Enter your organization's user data:
   - **Common Name** - A common name for the CSR (1 through 32 alphanumeric characters).
   - **Unit Name** - A unit name for the CSR (1 through 32 alphanumeric characters).
   - **Organization** - The name of your organization (1 through 64 alphanumeric characters).
   - **E-mail Address** - The e-mail address for the CSR. This is the From: address when the CSR is submitted for signing. It can be up to 64 characters long.
   - **Locality Name** - A name for your locality (1 through 64 alphanumeric characters).
   - **State or Province** - Your state or province (1 through 32 alphanumeric characters).
   - **Country** - A two-character country code.
8. Enter a name for the SSL key in the **Key Name** field (1 through 32 alphanumeric characters).
9. In the **Key** field, paste the newly generated SSL key, or a previously generated key that has been selected from the **Certificate View** tab.

10. Enter the key password in the **Password** field, if necessary.

    By default, the **Password** field displays the password (entered in the **Certificate Signing Request** dialog box) as asterisks (*).

11. Click **OK**.

    The generated CSR displays in the **CSR** field.

12. The CSR needs to be copied and pasted into a file. Obtain instructions from the CA for submitting the CSR for signing.

Related topic

"SSL certificate configuration"

Adding an SSL certificate and key file

To add an SSL certificate and key file, you must have received a signed certificate from an Certificate Authority (CA) and you must have a copy of a signed certificate ready to paste. If you want to include a certificate key, you must also have the key available.

1. Select **Configure > Application Delivery > SSL Certificates**.

   The **SSL Certificates** dialog box displays.

2. From the **Certificate View** tab, use the **Certificates** arrow to select **Add**.

   The **Add SSL Certificate** dialog box displays (Figure 389).

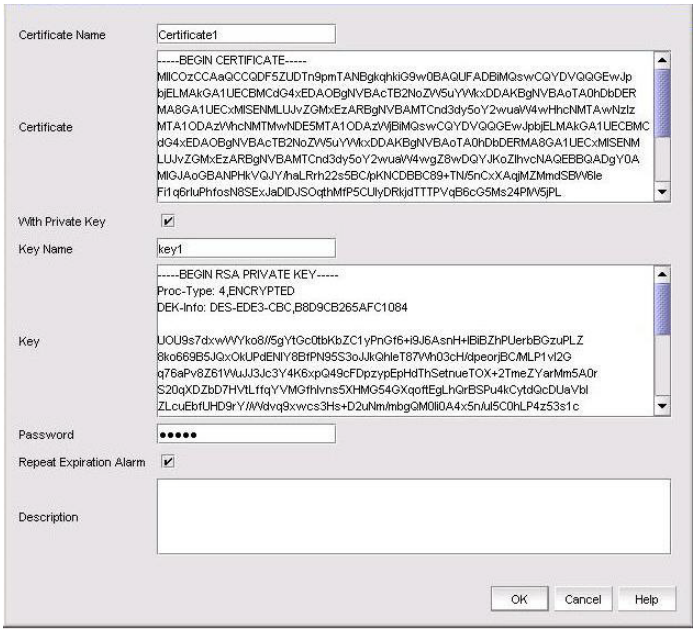


FIGURE 389 Add SSL Certificate dialog box

3. Enter a name in the **Certificate Name** field.

   The name can be from 1 through 32 characters in length.

4. Paste the signed certificate request into the **Certificate** field.

The certificate request must be in .PEM format, and must not be expired. No size limit is enforced.

5. If you want a key to accompany the certificate, select the **With Private Key** check box.

   This enables the **Key Name**, **Key**, and **Password** fields.

   If you select **With Private Key**, continue with step 6. If you do not select **With Private Key**, continue with step 9.

6. Enter a name in the **Key Name** field. Any alphanumeric character can be used except a space.

   The field is case-sensitive. The maximum number of characters is 24.

7. Paste the SSL key into the **Key** field. The key must be in .PEM format. No size limit is enforced.

8. Enter a password for the SSL key in the **Password** field.

   All printable ASCII characters are allowed. The field is case-sensitive. The maximum number of characters is 32.

9. Select the **Repeat Expiration Alarm** check box to repeat sending the certificate expiration trap.

10. Enter descriptive text for the certificate in the **Description** field.

    All printable ASCII characters are allowed. The field is case-sensitive. The maximum number of characters is 1024.

11. Click **OK** to create the certificate and key.

Related topic

"SSL certificate configuration"

Editing an SSL certificate and key file

You can only select to repeat sending a certificate expiration trap or edit the certificate key decription from the **Edit Certificate** dialog box.

NOTE
You cannot edit the **Certificate Name**, **Certificate**, **With Private Key**, **Key Name**, or **Key** fields.

1. Select **Configure > Application Delivery > SSL Certificates**.

   The **SSL Certificates** dialog box displays.

2. From the **Certificate View** tab, use the **Certificates** arrow to select **Edit** .

   The **Edit Certificate** dialog box displays.

3. Select the **Repeat Expiration Alarm** check box to repeat sending the certificate expiration trap.

4. Change the descriptive text for the certificate in the **Description** field.

   All printable ASCII characters are allowed. The field is case sensitive. The maximum number of characters is 1024.

5. Click **OK**.

Related topic

"SSL certificate configuration"

Duplicating an SSL certificate and key file

You can only edit the certificate name, the key name, and the certificate key decription from the **Duplicate Certificate** dialog box.

1. Select **Configure > Application Delivery > SSL Certificates**.

   The **SSL Certificates** dialog box displays.

2. From the **Certificate View** tab, use the **Certificates** arrow to select **Duplicate** .

   The **Duplicate Certificate** dialog box displays.

3. Change the name in the **Certificate Name** field.

   The name can be from 1 through 32 characters in length.

4. Change the name in the **Key Name** field.

   Only enabled when the **With Private Key** check box is selected.

   Any alphanumeric character may be used except a space. The field is case sensitive. The maximum number of characters is 24.

5. Change the descriptive text for the certificate in the **Description** field.

   All printable ASCII characters are allowed. The field is case sensitive. The maximum number of characters is 1024.

6. Click **OK**.

Related topic

"SSL certificate configuration"

Viewing SSL certificate details

NOTE
If the ADX is running software release 12.3.00 or later, you can only view and manage SSL certificates that are bound to Virtual IP servers that are in your Area of Responsibility (AOR). To add a Virtual IP server to your AOR, refer to "Assigning products to an AOR" on page 197

You can only select to repeat sending a certificate expiration trap or edit the certificate key decription from the **Edit Certificate** dialog box.

1. Select **Configure > Application Delivery > SSL Certificates**.

   The **SSL Certificates** dialog box displays.

2. From the **Certificate View** tab, select the certificate you want to view and click **View** .

   The **View Certificate Details** dialog box displays the selected certificate in a readable format. If the selected certificate is chained, a tree structure displays that allows you to select a chained certificate.

3. Click **Close**.

Importing certificates and keys from file locations

NOTE
If the ADX is running software release 12.3.00 or later, you can only view and manage SSL certificates that are bound to Virtual IP servers that are in your Area of Responsibility (AOR). To add a Virtual IP server to your AOR, refer to "Assigning products to an AOR" on page 197

The certificates and keys must already be stored in known locations before importing the certificates and keys from file locations. You must know the certificate or key name, and the password associated with the key.

1. Select **Configure > Application Delivery > SSL Certificates**.

   The **SSL Certificates** dialog box displays.

2. From the **Certificate View** tab, use the **Import** arrow to select **From File**.

   The **Import from File - SSL Certificates/Keys** dialog box displays (Figure 390).

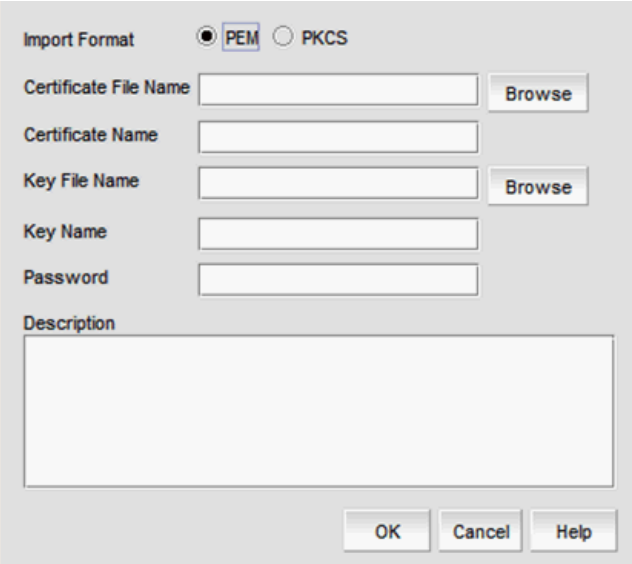


FIGURE 390 Import from File - SSL Certificates/Keys dialog box

3. Select the **Input Format**. Privacy Email (**PEM**) and RSA public-key cryptography standards (**PKCS**) formats are supported.
4. Enter the name of the file that contains the certificate in the **Certificate File Name** field or click **Browse** to browse to the location.
5. Enter the certificate name in the **Certificate Name** field.
6. If a key is to be associated with the certificate, enter the name of the file that contains the key in the **Key File Name** field or click **Browse** to browse to the location.

   If you selected **PKCS** as the **Input Format**, the **Browse** button is unavailable.

7. Enter the key name in the **Key Name** field.

8. Enter the password associated with the key in the **Password** field.
9. (Optional) Enter a description of the certificate in the **Description** field.
10. Click **OK** to import the certificate and key files.

Related topic

"SSL certificate configuration"

Importing certificates and keys from products

NOTE
If the ADX is running software release 12.3.00 or later, you can only view and manage SSL certificates that are bound to Virtual IP servers that are in your Area of Responsibility (AOR). To add a Virtual IP server to your AOR, refer to "Assigning products to an AOR" on page 197

You can import deployed certificates and keys from products to manage them from SSL certificates.

NOTE
To import keys from ADX devices, key passwords must be entered in the **Key Passwords** dialog box prior to import. If the key passwords are not entered in the **Key Passwords** dialog box, the keys from ADX devices are not imported. ADX software release 12.2 and later supports a master key password. Using the master key password feature, you can configure one master password on the product to import all keys from the device. Use the following commands to set and clear the master passwords on ADX devices.
ssl set export-master-pswd <*password*>
ssl clear export-master-pswd <*password*>

1. Select **Configure > Application Delivery > SSL Certificates**.

   The **SSL Certificates** dialog box displays.

2. From the **Certificate View** tab, click the **Import** arrow and select **From Product**.

   The **Import from Product - SSL Certificates/Keys** dialog box displays (Figure 391).

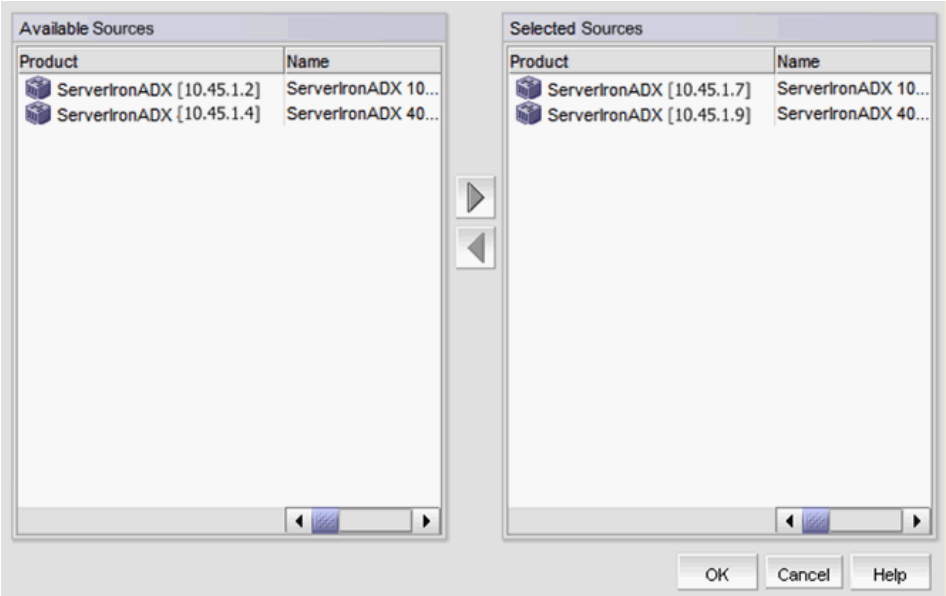


FIGURE 391 Import from Product - SSL Certificates/Keys dialog box

3. Select a product from the **Available Sources** list.
4. Use the right arrow button to move the selected product to the **Selected Sources** list.
5. Click **OK** to import certificates and keys for the selected products.

Related topic

"SSL certificate configuration"

Exporting certificates and keys

NOTE
If the ADX is running software release 12.3.00 or later, you can only view and manage SSL certificates that are bound to Virtual IP servers that are in your Area of Responsibility (AOR). To add a Virtual IP server to your AOR, refer to "Assigning products to an AOR" on page 197

You must know where you want to store the certificate or key before exporting the certificate or key. You also must know the certificate or key name.

1. Select **Configure > Application Delivery > SSL Certificates**.

   The **SSL Certificates** dialog box displays.

2. From the **Certificate View** tab, select a certificate and click **Export**.

   The **Export to File** dialog box displays.

3. Select the **Export Format** option.

   Privacy Email (**PEM**) and RSA public-key cryptography standards (**PKCS**) formats are supported.

   For the **PEM** format, two files, one certificate and one key, are exported.

   For the **PKCS** format, one file, which contains the certificate and key, is exported.

If you export the certificate file only (no key file), the **PKCS** option is not enabled.

4. Enter the location of the file in the **File Location** field or click **Browse** to browse to the location.
5. Enter the certificate name in the **Certificate Name** field.
6. Enter the key name in the **Key Name** field.

   If you export the certificate file only (no key file), the **Key Name** field is not enabled.

   If you select **PKCS** as the export format, the **Key Name** field is not enabled.
7. Click **OK** to export the certificate and key files.

Related topic

"SSL certificate configuration"

Deploying certificates and keys

NOTE
If the ADX is running software release 12.3.00 or later, you can only view and manage SSL certificates that are bound to Virtual IP servers that are in your Area of Responsibility (AOR). To add a Virtual IP server to your AOR, refer to "Assigning products to an AOR" on page 197

You can deploy an SSL certificate and key to a ServerIron or ADX product using the following procedure.

1. Select **Configure > Application Delivery > SSL Certificates**.

   The **SSL Certificates** dialog box displays.
2. Select a certificate from the **Certificate View** tab.
3. Click **Deploy**.

   The **Deploy Certificates/Keys** dialog box displays (Figure 392).

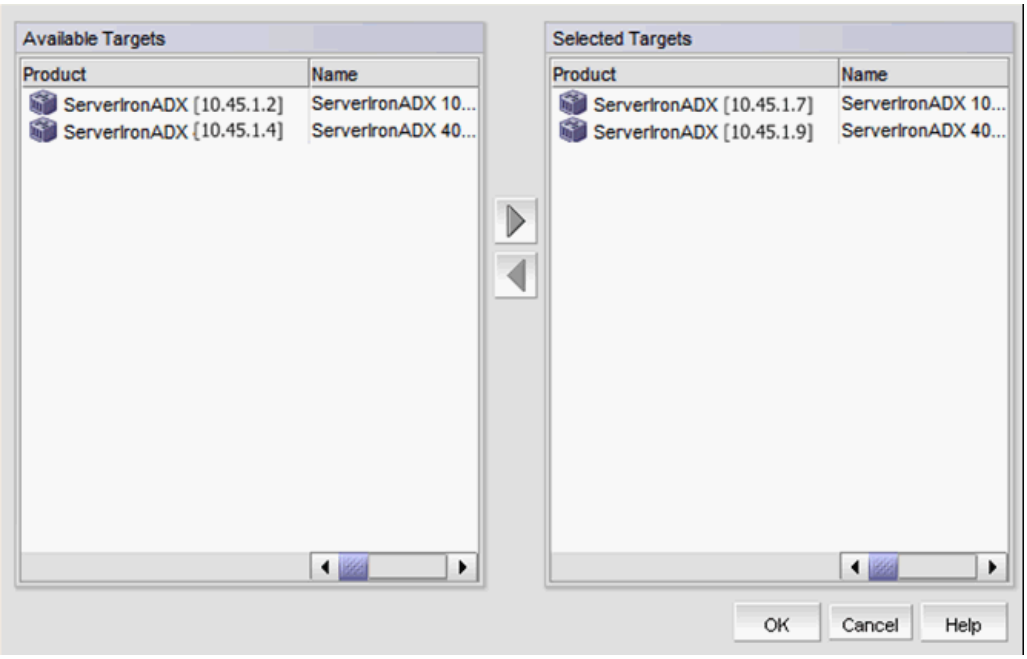


FIGURE 392 Deploy Certificates/Keys dialog box

4. Select a product from the **Available Targets** list.
5. Use the right arrow button to move the selected product to the **Selected Targets** list.
6. Click **OK**.

   The certificate and key selected from the **Certificate View** tab are deployed to the selected products.

Related topic

"SSL certificate configuration"

Creating key passwords

You can create candidate key passwords used when importing SSL keys from a ServerIron product using the following procedure.

1. Select **Configure > Application Delivery > SSL Certificates**.

   The **SSL Certificates** dialog box displays.
2. From the **Certificate View** tab, click **Key Passwords**.

   The **Key Passwords** dialog box displays (Figure 393).

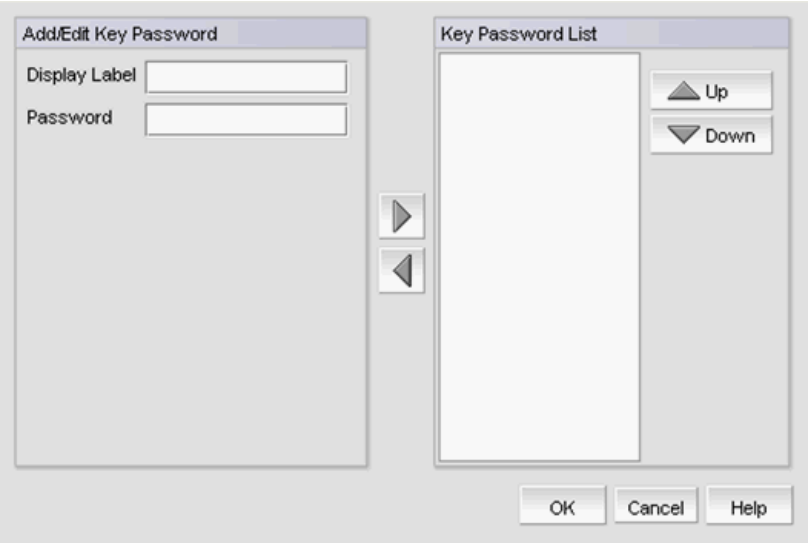


FIGURE 393 Key Passwords dialog box

3. Under **Add/Edit Key Password**, enter an ASCII character string (from 1 through 16 characters) in the **Display Label** field that identifies the password you enter in the **Password** field. Use the key name or a character string that is easy to identify with a specific key.

   The label provides a means for identifying the password. The password itself is not exposed.

4. Enter a password (4 through 254 ASCII characters) for the SSL encryption key in the **Password** field.

5. Use the right arrow key to move the password to the **Key Password List**.

   You can use the left arrow key to move a key back to **Add/Edit Key Password** to edit the **Display Label** and **Password** fields. Use the **Up** and **Down** buttons to rearrange the **Key Password List**.

6. Click **OK** to save your work.

Related topic

"SSL certificate configuration"

Appending SSL certificates

NOTE
If the ADX is running software release 12.3.00 or later, you can only view and manage SSL certificates that are bound to Virtual IP servers that are in your Area of Responsibility (AOR). To add a Virtual IP server to your AOR, refer to "Assigning products to an AOR" on page 197

You can append an SSL certificate with another certificate.

1. Select **Configure > Application Delivery > SSL Certificates**.

   The **SSL Certificates** dialog box displays.

2. From the **Certificate View** tab, select the certificate to which you want to append another certificate.

3. Use the **Certificates** arrow to select **Append**.

   The **Append Certificate** dialog box displays. The **Append Certificate** dialog box contains the same fields and components as the **Add Certificate** dialog box (Figure 389). For information about the fields and components, refer to "Adding an SSL certificate and key file" on page 950.

4. Add the certificate content you want to append to the certificate you selected in step 2 in the **Certificate** field.

5. Click **OK** to save changes.

Chaining SSL certificates

NOTE
If the ADX is running software release 12.3.00 or later, you can only view and manage SSL certificates that are bound to Virtual IP servers that are in your Area of Responsibility (AOR). To add a Virtual IP server to your AOR, refer to "Assigning products to an AOR" on page 197

You can chain a certificate to another certificate selected from the **Certificate View** tab.

NOTE
You cannot chain a key only entry.

1. Select **Configure > Application Delivery > SSL Certificates**.

   The **SSL Certificates** dialog box displays.

2. From the **Certificate View** tab, select the certificate to which you want to chain another certificate.

   Make sure the **Status** for the certificate to which you want to chain another certificate is **Valid.**

3. Click **Chain**.

   The **Chain Certificates** dialog box displays (Figure 394).

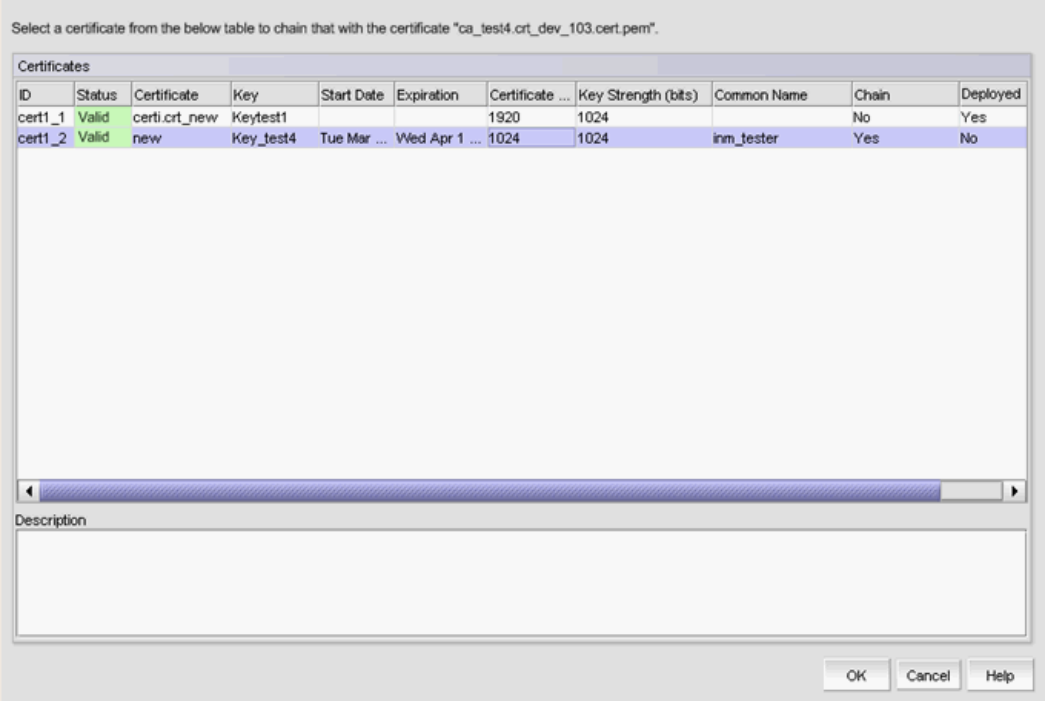


FIGURE 394 Chain Certificates dialog box

The **Certificates** table includes the following details:

- **ID** — A unique system-assigned ID for each certificate entry.
- **Status** — Possible values are Valid, About to Expire, or Expired.
- **Certificate** — The user-assigned certificate name. The same name may be used on different products.
- **Key** — The user-assigned key name. The same name may be used on different products.
- **Start Date** — The start date for the certificate. If only a key is present, this field is blank. For chained certificates, the date for the last certificate in the chain is displayed.
- **Expiration** — The expiration date for the certificate. If only a key is present, this field is blank. For chained certificates, the date for the last certificate in the chain is displayed.
- **Certificate Size** — The certificate size in bytes. If only a key is present, this field is blank.
- **Key Strength** — The key strength (size in bits). If only a certificate is present, this field is blank.
- **Common Name** — The common name for the certificate. For chained certificates, the name for the last certificate in the chain is displayed.
- **Chain** — Yes is certificates are chained, No if certificates are not chained. If only a key is present, this field is blank.
- **Deployed** — Yes if the certificate or key is not deployed to the product. No if the certificate or key is deployed to the product.
- **Summary** — An overall count of certificates.

4. Select the certificate you want to chain to the certificate you selected in step 2. The **Chain** status for the selected certificate must be **Yes.**

   Make sure the **Status** for the second certificate is **Yes.**

   The description of the certificate displays in the **Description** field, if a description was entered when the certificate was created.

5. Click **OK**.

   If the root certificate status has a **Chain** status of **Yes**, the certificate selected in the **Chain Certificates** dialog box is chained to the certificate selected from the **Certificate View** tab of the **SSL Certificates** dialog box.

Deleting SSL certificates

NOTE
If the ADX is running software release 12.3.00 or later, you can only view and manage SSL certificates that are bound to Virtual IP servers that are in your Area of Responsibility (AOR). To add a Virtual IP server to your AOR, refer to "Assigning products to an AOR" on page 197

NOTE
When certificates and keys are bound to devices, the delete operation deletes the certificates and keys from the SSL Certificates dialog box as well as the product.

To delete a selected SSL certificate , complete the following steps.

1. Select **Configure > Application Delivery > SSL Certificates**.

   The **SSL Certificates** dialog box displays.

2. Choose one of the following options:

   - From the **Certificate View** tab, select the SSL certificate that you want to delete and select **Certificates > Delete**.
   - From the **Product View** tab, select the SSL certificate that you want to delete and click **Delete**.

3. Click **Yes** on the confirmation message to delete the certificate.

Chapter

32

Deployment Manager

In this chapter

Introduction to the Deployment Manager

The Deployment Manager allows you to view, edit, duplicate, delete, deploy, and generate reports for the following types of deployment configurations:

- DCB
- VLAN
- STP
- Security

You cannot create configurations using the Deployment Manager. The deployment configurations must have been previously created and saved. Refer to the following sections for information about creating these types of configurations:

- "Fibre Channel over Ethernet" on page 481 (for DCB configurations)
- "VLAN Management" on page 819 (for VLAN and STP configurations)
- "Security Management" on page 561

Deployments that were created through the legacy Configuration Wizard are listed in the **Deployment Manager** dialog box, but cannot be modified, deployed, or deleted. You can only launch reports for these deployments.

Editing a deployment configuration

1. Select **Configure > Task Scheduler**.

   The **Task Scheduler** dialog box displays, as shown in Figure 395.

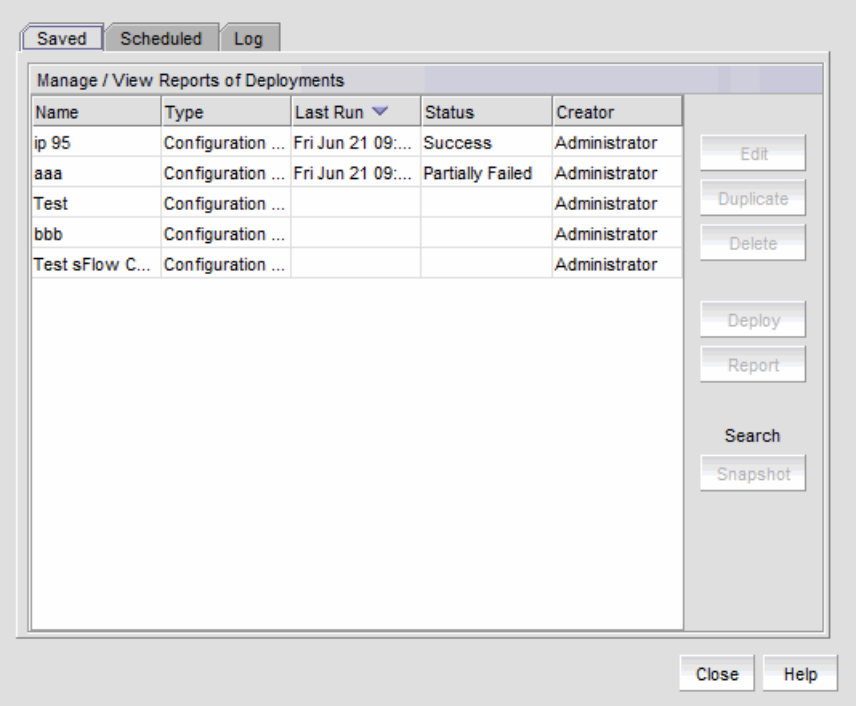


FIGURE 395 Task Scheduler dialog box

2. Select a deployment configuration in the **Saved** or **Scheduled** tab.

   Policy-based routing configurations cannot be edited.

3. Click **Edit**.

   A dialog box specific to the type of deployment displays. This is the same dialog box that was used when the deployment was created.

4. Update the dialog box with the information you want to change.

Duplicating a deployment configuration

1. Select **Configure > Task Scheduler**.

   The **Task Scheduler** dialog box displays.

2. Select a deployment configuration in the **Saved** or **Scheduled** tab.

   NOTE
   VLAN configurations and policy-based routing configurations cannot be duplicated.

3. Click **Duplicate**.

   A dialog box specific to the type of deployment displays. This is the same dialog box that was used when the original deployment was created.

4. Update the dialog box with any information you want to change.

A copy of the deployment configuration is created with the name "*originalName* **copy***n*". For example, if the original name is "test", the new name is "test copy1". If you duplicate "test" again, the name of the second duplicate is "test copy2".

Deleting a deployment configuration

1. Select **Configure > Task Scheduler**.

   The **Task Scheduler** dialog box displays.
2. Select a deployment configuration in the **Saved** or **Scheduled** tab.
3. Click **Delete**.
4. Click **Yes** in the confirmation dialog.

   The deployment configuration is deleted and removed from the **Task Scheduler** dialog box.

   If the deployment configuration is already in progress, it is not deleted.

Deploying a configuration

1. Select **Configure > Task Scheduler**.

   The **Task Scheduler** dialog box displays.
2. Select a deployment configuration in the **Saved** or **Scheduled** tab.
3. Click **Deploy**.

   The **Deployment Status** dialog box displays.
4. Click **Start**.

   The selected configuration is deployed.

   You cannot deploy configurations that are already in progress.

Viewing deployment logs

1. Select **Configure > Task Scheduler**.

   The **Task Scheduler** dialog box displays.
2. Click the **Log** tab.

   A list of deployment configurations that are executed and the status of each displays.

Generating a deployment report

1. Select **Configure > Task Scheduler**.

   The **Task Scheduler** dialog box displays.
2. Select a deployment in the **Saved**, **Scheduled**, or **Log** tab.

3. Click **Report**.

   An HTML report displays. You can click the Configuration Name or Deployment Time to see additional details.

Generating a deployment configuration snapshot report

1. Select **Configure > Task Scheduler**.

   The **Task Scheduler** dialog box displays.

2. Select a deployment in the **Saved** or **Scheduled** tab.

3. Click **Deploy**.

   The **Deployment Status** dialog box displays.

4. Click **Snapshot Report**.

   The **Configuration Snapshot Report** dialog box displays.

5. (*Optional*) If the configuration snapshot list is too long, you can filter the list.

   a. Select the start date and end date of the configuration snapshots you wish to view.

   b. Click **Find**.

      The Management application displays the list of snapshots that match the start date and end date you specified.

6. Select a product from the **Device Configuration** column to display the configuration snapshots that are available for that product.

7. Click **View** to display information for that deployment.

   The **View Pre/Post Configuration Snapshot** dialog box displays details of the selected configuration.

Searching the configuration snapshots

1. Select **Configure > Task Scheduler**.

   The **Task Scheduler** dialog box displays.

2. Select a deployment in the **Saved**, **Scheduled**, or **Log** tab.

3. Click **Snapshot**.

   The **Configuration Snapshot Search** dialog box displays.

4. Identify the targets you want to search.

   Select a target in the **Available Targets** list and click the right arrow to move the target to the **Selected Targets** list.

5. Define search criteria.

   You can specify whether the targets should contain or not contain specific text, and whether to display all configurations, the most recent configurations, or only those configurations that fall within a specific date range.

6. Click **Find**.

   The Management application displays the list of snapshots that match the search criteria you specified.

You can select configurations in the **Search Results** list to display details, view the snapshot report, and compare two configurations,

Chapter

Performance Data 33

In this chapter

SAN performance overview

NOTE
SAN performance is only supported on Fabric OS devices.

Performance monitoring provides details about the quantity of traffic and errors that a specific port or device generates on the fabric over a specific time. You can also use performance monitoring to indicate the devices that create the most traffic and identify the ports that are most congested.

Performance monitoring allows you to monitor your SAN using the following methods (requires a Licensed version):

- Gather and display real-time performance data (Switch Ports - FC, Switch Ports - GE, Switch Ports - 10 GE, ISL Ports, E_Port Trunks, end-to-end Monitors, FCIP Tunnels, device Ports, managed HBA Ports, and managed CNA Ports).

  The Professional version only allows you to monitor your SAN by gathering and displaying real-time performance data (Switch Ports - FC, Switch Ports - GE, Switch Ports - 10GE, ISL Ports, E_Port Trunks, end-to-end Monitors, FCIP Tunnels, device Ports, managed HBA Ports, managed CNA Ports).

- Create custom port and time data filters for historical performance data that can be saved as a favorite.
-
- Provide enhanced performance reports.

SAN performance measures

Performance measures enable you to select one or more measures to define the graph or report. The measures available to you depend on the object type from which you want to gather performance data.

NOTE
Devices with 10GE ports must be running Fabric OS 6.4.1 or later to obtain the correct TE_Port statistics (TX/RX).

NOTE
Devices with 10GE ports must have the RMON MIB enabled on the switch. For more information about the **rmon collection** command, refer to the *Fabric OS Converged Enhanced Ethernet Command Reference*.

You can define a report or graph for the following performance data:

- Current — Available in mAmps for installed SFPs.
- Rx Power — Available in dBm for installed SFPs.
- Tx Power — Available in dBm for installed SFPs.
- Temperature — Available in Centigrade for installed SFPs.
- Voltage — Available in mVolts for installed SFPs.
- Tx % Utilization — Available for FC, GE, managed HBA ports, managed CNA ports, E_port trunks, 10GE ports, and FCIP tunnels.
- Rx % Utilization — Available for FC, GE, managed HBA ports, managed CNA ports, 10GE ports, E_port trunks, and FCIP tunnels.
- Tx MB/Sec — Available for FC, GE, managed HBA ports, managed CNA ports, 10GE ports, E_port trunks, FCIP tunnels, and end-to-end monitors.
- Rx MB/Sec — Available for FC, GE, managed HBA ports, managed CNA ports, 10GE ports, E_port trunks, FCIP tunnels, and end-to-end monitors.
- CRC Errors — Available for FC, managed HBA ports, managed CNA ports, 10GE ports and end-to-end monitors.
- Signal Losses — Available for managed HBA ports, managed CNA ports, and FC ports.
- Sync Losses — Available for managed HBA ports, managed CNA ports, and FC ports.
- Link Failures — Available for managed HBA ports, managed CNA ports, and FC ports.
- Sequence Errors — Available for FC ports.
- Invalid Transmissions — Available for FC ports.
- Rx Link Resets — Available for FC ports.
- Tx Link Resets — Available for FC ports.
- C3 Discard — Available for FC ports.
- C3 Discard RX Timeout — Available for FC ports
- C3 Discard Tx Timeout — Available for FC ports
- C3 Discard Unreachable — Available for FC ports.
- C3 Discard Others — Available for FC ports.
- Encode Error out — Available for FC ports.

- BB Credit Zero — Available for FC ports.
- Truncated Frames — Available for FC ports.
- FEC Corrected Blocks — Available for FC ports.
- FEC Uncorrected Blocks — Available for FC ports.
- Dropped Packets — Available for FCIP tunnels only.
- Cumulative Compression Ratio — Available for FCIP tunnels only.
- Current Compression Ratio — Available for FCIP tunnels only.
- Latency — Available for FCIP tunnels only.
- Link Retransmits — Available for FCIP tunnels only.
- Timeout Retransmits — Available for FCIP tunnels only.
- Fast Retransmits — Available for FCIP tunnels only.
- Duplicate Ack Received — Available for FCIP tunnels only.
- Window Size RTT — Available for FCIP tunnels only.
- TCP Out of Order Segments — Available for FCIP tunnels only.
- Slow Start Status — Available for FCIP tunnels only.
- Uncompressed Tx/Rx MB/sec - Available for FCIP tunnels only.
- Overflow Errors — Available for 10GE ports only.
- Runtime Errors — Available for 10GE ports only.
- Receive EOF — Available for 10GE ports only.
- Too Long Errors — Available for 10GE ports only.
- Underflow Errors — Available for 10GE ports only.
- Alignment Errors — Available for 10GE ports only.
- NOS Count — Available for managed HBA ports and managed CNA ports.
- Error Frames — Available for managed HBA ports and managed CNA ports.
- Under Sized Frames — Available for managed HBA ports and managed CNA ports.
- Over Sized Frames — Available for managed HBA ports and managed CNA ports.
- Primitive Sequence Protocol Errors — Available for managed HBA ports and managed CNA ports.
- Dropped Frames — Available for managed HBA ports and managed CNA ports.
- Bad EOF Frames — Available for managed HBA ports and managed CNA ports.
- Invalid Ordered Sets — Available for managed HBA ports, managed CNA ports, and FC ports.
- Non Frame Coding Error — Available for managed HBA ports and managed CNA ports.

SAN performance management requirements

To collect performance data, make sure the following requirements have been met:

- Make sure the SNMP access control list for the device is empty or the Management application server IP is in the access control list.

  Example of default access control list

  ```
  FCRRouter:admin> snmpconfig --show accesscontrol
  SNMP access list configuration:
  ```

```
Entry 0:  No access host configured yet
Entry 1:  No access host configured yet
Entry 2:  No access host configured yet
Entry 3:  No access host configured yet
Entry 4:  No access host configured yet
Entry 5:  No access host configured yet
```

Example of Management application Server IP address included in access control list

```
FCRRouter:admin> snmpconfig --show accesscontrol
SNMP access list configuration:
Entry 0:  Access host subnet area 172.26.1.86 (rw)
Entry 1:  No access host configured yet
Entry 2:  No access host configured yet
Entry 3:  No access host configured yet
Entry 4:  No access host configured yet
Entry 5:  No access host configured yet
```

To add the Management application server IP address to the access control list, use the **snmpconfig –add accesscontrol** command.

To set the default access control, use the **snmpconfig –default accesscontrol** command.

- Make sure that the SNMP credentials in the Management application match the SNMP credentials on the device.
  - To check the SNMP v1 credentials on the device, use the **snmpconfig –show snmpv1** command.

    Example of SNMP v1

    ```
    HCLSwitch:admin> snmpconfig --show snmpv1
    SNMPv1 community and trap recipient configuration:
    Community 1: Secret C0de (rw)
    Trap recipient: 10.103.4.63
    Trap port: 162
    Trap recipient Severity level: 4
    Community 2: OrigEquipMfr (rw)
    Trap recipient: 10.1.12.240
    Trap port: 162
    Trap recipient Severity level: 4
    Community 3: private (rw)
    Trap recipient: 10.103.5.105
    Trap port: 162
    Trap recipient Severity level: 4
    Community 4: public (ro)
    Trap recipient: 2.168.102.41
    Trap port: 162
    Trap recipient Severity level: 4
    Community 5: common (ro)
    Trap recipient: 10.32.150.116
    Trap port: 162
    Trap recipient Severity level: 4
    Community 6: FibreChannel (ro)
    Trap recipient: 1001:0:0:0:0:0:0:172
    Trap port: 162
    Trap recipient Severity level: 4
    ```

  - To set the SNMP v1 credentials on the device, use the **snmpconfig –set snmpv1** command.

Example of setting SNMP v1

```
HCLSwitch:admin> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
Community (rw): [test]
Trap Recipient's IP address : [172.26.1.183]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address : [172.26.24.26]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Community (rw): [custom]
Trap Recipient's IP address : [172.26.1.158]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Community (ro): [custom]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [common]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [FibreChannel]
Trap Recipient's IP address : [172.26.1.145]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
```

- To check the SNMP v3 credentials on the device, use the **snmpconfig –show snmpv3** command.

Example of SNMP v3

```
sw1:FID128:admin> snmpconfig --show snmpv3
SNMPv3 USM configuration:
User 1 (rw): snmpadmin1
Auth Protocol: noAuth
Priv Protocol: noPriv
User 2 (rw): snmpadmin2
Auth Protocol: noAuth
Priv Protocol: noPriv
User 3 (rw): snmpadmin3
Auth Protocol: noAuth
Priv Protocol: noPriv
User 4 (ro): snmpuser1
Auth Protocol: noAuth
Priv Protocol: noPriv
User 5 (ro): snmpuser2
Auth Protocol: noAuth
Priv Protocol: noPriv
User 6 (ro): admin
Auth Protocol: noAuth
Priv Protocol: noPriv
```

- To set the SNMP v3 credentials on the device, use the **snmpconfig –set snmpv3** command.

```
FM_4100_21:admin> snmpconfig --set snmpv3
SNMPv3 user configuration(SNMP users not configured in Fabric OS user
database will have physical AD and admin role as the default):
User (rw): [snmpadmin1] admin
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3] 1
New Auth Passwd:
Verify Auth Passwd:
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES2(5)/AES256(6)]):
(1..6) [2] 1
New Priv Passwd:
```

```
Verify Priv Passwd:
User (rw): [snmpadmin2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES2(5)/AES256(6)]):
(2..2) [2]
User (rw): [snmpadmin3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES2(5)/AES256(6)]):
(2..2) [2]
User (ro): [snmpuser1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES2(5)/AES256(6)]):
(2..2) [2]
User (ro): [snmpuser2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES2(5)/AES256(6)]):
(2..2) [2]
User (ro): [snmpuser3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES2(5)/AES256(6)]):
(2..2) [2]
SNMPv3 trap recipient configuration:
Trap Recipient's IP address : [2.168.71.32]
UserIndex: (1..6) [1]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [1.1.1.1]
UserIndex: (1..6) [2]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [10.64.209.171]
UserIndex: (1..6) [1]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
```

- To check SNMP credentials in the Management application, complete the following steps.

    1. Select **Discover > Fabrics**.
    The **Discover Fabrics** dialog box displays.
    2. Select an IP address from the **Available Addresses** list.
    3. Click **Edit**.
    The **AddFabric Discovery** dialog box displays.
    4. Select the **Manual** option to view SNMP credentials.
    5. Click the **SNMP** tab.
    6. Select **v1** or **v3** from the **SNMP Version** list.
    7. Make sure SNMP credentials match those on the device.
    8. Click **OK** on the **AddFabric Discovery** dialog box.
    9. Click **Close** on the **Discover Fabrics** dialog box.

- To set SNMP credentials in the Management application, refer to "Discovery" on page 31.

- Make sure that the SNMP security level is set to the appropriate level for the switch.
  - To check the SNMP security level, use the snmpconfig **–show secLevel** command.

    Example of checking SNMP security level

    ```
    snmpconfig --show secLevel
    GET security level = 0, SET level = 0
    SNMP GET Security Level: No security
    SNMP SET Security Level: No security
    ```

  - To set the SNMP security level, use the **snmpconfig –set secLevel** command.

    Example of checking SNMP security level

    ```
    snmpconfig --set secLevel 0
    Select SNMP GET Security Level
    (0 = No security, 1 = Authentication only, 2 = Authentication and Privacy,
    3 = No Access): (0..3) [0]
    ```

- To collect performance data for GE ports and FCIP statistics, make sure that SNMP v3 credentials match and that FCIP-MIB capability is enabled.
  - To check FCIP-MIB capability, use the **snmpconfig –show mibcapability** command.

    Example of showing FCIP-MIB

    ```
    FCRRouter:admin> snmpconfig --show mibcapability
    FCIP-MIB: YES
    ```

  - To enable FCIP-MIB capability, use the **snmpconfig –set mibcapability** command.

    Example of enabling FCIP-MIB

    ```
    FCRRouter:admin> snmpconfig --set mibcapability
    FA-MIB (yes, y, no, n): [yes]
    FICON-MIB (yes, y, no, n): [yes]
    HA-MIB (yes, y, no, n): [yes]
    FCIP-MIB (yes, y, no, n): [yes]
    ISCSI-MIB (yes, y, no, n): [yes]
    ```

- To collect performance data on a Virtual Fabric-enabled device, use the **userconfig –show** command to make sure the Fabric OS user has access to all the Virtual Fabrics. Make sure that the SNMPv3 user name is the same as the Fabric OS user name. Otherwise, the data is not collected for virtual switches with a non-default Virtual Fabric ID. By default, the **admin** user has access to all Virtual Fabrics.

  Example of Fabric OS user verification

  ```
  sw1:FID128:admin> userconfig --show
  Account name: admin
  Description: Administrator
  Enabled: Yes
  Password Last Change Date: Unknown
  Password Expiration Date: Not Applicable
  Locked: No
  Home LF Role: admin
  Role-LF List: admin: 1-128
  Chassis Role: admin
  Home LF: 128
  ```

  - Make sure I/O is running on the switch to obtain real statistics. To view switch statistics, use the **portperfshow** (FC Ports) or **portshow fciptunnel** (FCIP tunnels) command.

Example for FC ports

```
Sprint-65:root> portperfshow 5
```

Example for FCIP tunnels

```
Sprint-65:root> portshow fciptunnel ge0 1 -perf
```

SAN real-time performance data

Real-time performance monitoring enables you to collect data from managed devices in your SAN. Real-time performance monitoring is only supported on the following managed objects: FC (E_Ports and F_Ports), GE_Ports, E_Port trunks, 10GE_Ports, managed HBA Ports, managed CNA Ports, and FCIP tunnels. You can use real-time performance monitoring to configure the following options:

- Select the polling rate from 10 seconds up to 1 minute.
- Select up to 100 ports total from a maximum of 20 devices for graphing performance.

  For E_Port trunks, you can select up to 25 trunks (the trunk member [port] count must be below 100) from a maximum of 20 devices for graphing performance.

  NOTE
  Virtual Fabric logical ISL ports are not included in performance collection.

- Choose to display the same Y-axis range for both the Tx MB/Sec and Rx MB/Sec measure types for easier comparison of graphs.

Generating a real-time performance graph

You can monitor a device's performance through a performance graph that displays transmit and receive data. The graphs can be sorted by the column headers. You can create multiple real-time performance graph instances.

NOTE
To make sure that statistics for a switch does not fail, you must configure SNMP credentials for the switch. For step-by-step instructions, refer to "Discovery" on page 31.

To generate a real-time performance graph for a device, complete the following steps.

1. Select the fabric, device, or port for which you want to generate a performance graph
2. Select **Monitor > Performance > Real-Time Graph**.

   If you selected a port, the **Real Time Performance Graphs** dialog box for the selected port displays. To filter real-time performance data from the **Real Time Performance Graphs** dialog box, refer to "Filtering real-time performance data" on page 977.

   If you selected a fabric or device, the **Realtime Port Selector** dialog box displays, as shown in Figure 396 on page 977. Continue with step 3.

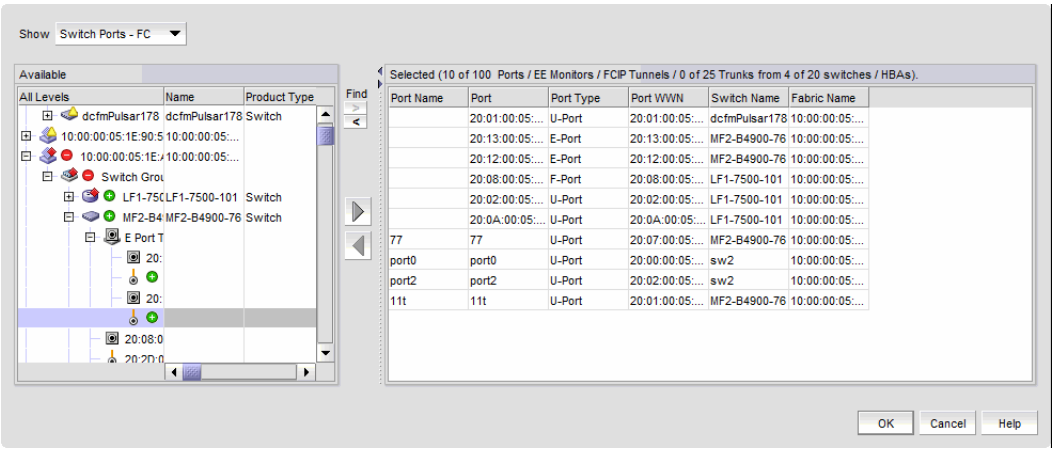


FIGURE 396 Realtime Port Selector dialog box

NOTE
You can set columns in right side of the dialog box for FICON display using **Server** > **Options** > **SAN Display**. The first eight columns will display FC Address, Serial #, Tag, Product Type, Model, Vendor, Port Name, Port Type, and Port WWN.

3. Select the object type from the **Show** list by which you want to graph performance.

NOTE
Devices with 10GE ports must be running Fabric OS 6.4.1 or later to obtain the correct TE_Port statistics (TX/RX).

NOTE
Devices with 10GE ports must have the RMON MIB enabled on the switch. For more information about the **rmon collection** command, refer to the *Fabric OS Converged Enhanced Ethernet Command Reference*.

4. Right-click anywhere in the **Available** list and select **Expand All** from the menu.
5. Select the ports or trunks you want to include in the performance graph in the **Available** list.

   Press **Ctrl** or **Shift** and then click to select more than one port.
6. Click the right arrow to move the selected ports to the **Selected** list.
7. Click **OK**.

   The **Real Time Performance Graphs** dialog box displays.

Filtering real-time performance data

To filter real-time performance data from the **Real Time Performance Graphs** dialog box, complete the following steps.

1. Open the **Real Time Performance Graphs** dialog box.

   For step-by-step instructions, refer to "Generating a real-time performance graph" on page 976.

2. Select how the data is measured, in received frames, transmitted frames, or CRC errors.

   For a list of possible performance measures, refer to "SAN performance measures" on page 970.

3. To select more than one measure, click the **Additional Measures** expand arrows and select the check box for each additional measure. If **Additional Measures** area is not shown, click the down arrow.

   For a list of possible performance measures, refer to "SAN performance measures" on page 970.

4. (Optional) Enter a value (percentage) in the **Reference Line** field to set a reference for the transmit and receive utilization.

   Note that this field is only available when you select **Tx % Utilization** or **Rx % Utilization** from the **Measures** list.

5. Select how detailed the data will display from the **Granularity** list. Options are in increments of 10 seconds, 15 seconds, 20 seconds, 25 seconds, 30 seconds, 45 seconds, or 1 minute.

6. Select **Plot Events** to display advanced monitoring service (AMS) violation events received during the chart time range and Master Log events logged on the same product as the measure being plotted.

7. Move the **Row Height** slider to the left to make the row height smaller or to the right to make it larger.

8. Select the **Display tabular data only** check box to show only text with no graphs or icons.

   The **Source** and **Destination** icons and the **Graph** column do not display.

9. Click **Apply**.

   The selected data automatically displays in the **Real Time Performance Graphs** dialog box.

10. Click the close button (**X**) to close the **Real Time Performance Graphs** dialog box.

Graph display

The columns in the graphical portion of the **Real Time Performance Graphs** dialog box display the following information:

- Source Fabric - The source fabric being monitored.
- Source - The source device being monitored.
- Source Port - The source port being monitored.
- Tunnel ID - The ID of the FCIP tunnel being monitored.
- Destination Fabric - The destination fabric.
- Description - Description of the FCIP tunnel.
- Port Type - Type of port being monitored.
- Graph - Graph of data over time.
- Destination - The destination device.
- Destination Port - The port through which the selected device is connected to the destination device.
- Destination Tunnel ID - The ID of the destination FCIP tunnel.

- Destination Port Type - The port type through which the selected device is connected to the destination device.
- Additional Measures columns - Displays each measure selected in the **Measures** list and **Additional Measures** area.
- Measures columns - A column for each selected measure in the **Measures** list or **Additional Measures** area.

Exporting real-time performance data

To export real-time performance data, complete the following steps.

1. Generate a performance graph.

   To generate a performance graph, refer to "Generating a real-time performance graph" on page 976.

2. Right-click anywhere in the graph table and select **Export Table**.

   The **Save table to a tab delimited file** dialog box displays.

3. Browse to the file location where you want to save the performance data.
4. Enter a name for the file and click **Save**.

Performance statistics counters

Table 86 details the formulas used to calculate performance statistics based on counter type and protocol.

To calculate FC, GE, FCIP and TE port statistics, the Management application uses SNMP to query the respective object identifiers (OID) (listed in Table 86).

To calculate HBA and CNA statistics, the Management application uses APIs provided by HCM.

To calculate end-to-end monitor (EE monitor) statistics, the Management application uses HTTP to obtain the TX, RX, and CRC error values.

The polling interval for historical graphs is 5 minutes. The polling interval for real-time graphs is based on the granularity value (configured in the Real Time Graph dialog box).

TABLE 86 Performance statistic counters

Counter name	Type	Protocol	Source OID value	Formula
TX	FC	SNMP	.1.3.6.1.3.94.4.5.1.6	TX = (delta value[1] / (1000 * 1000)) / (polling interval[2])
RX	FC	SNMP	.1.3.6.1.3.94.4.5.1.7	RX = (delta value[1] / (1000 * 1000)) / (polling interval[2])
TX	GE	SNMP	.1.3.6.1.2.1.31.1.1.1.10	TX = (delta value[1] / (1000 * 1000)) / (polling interval[2])
RX	GE	SNMP	.1.3.6.1.2.1.31.1.1.1.6	RX = (delta value[1] / (1000 * 1000)) / (polling interval[2])
TX	FCIP	SNMP	.1.3.6.1.2.1.31.1.1.1.10	TX = (delta value[1] / (1000 * 1000)) / (polling interval[2])

TABLE 86 Performance statistic counters

Counter name	Type	Protocol	Source OID value	Formula
RX	FCIP	SNMP	.1.3.6.1.2.1.31.1.1.1.6	RX = (delta value[1] / (1000 * 1000)) / (polling interval[2])
Uncompressed Tx/Rx MB/sec	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.6	(delta value[1] / (1000 * 1000)) / (polling interval[2])
TX	EE Monitors	HTTP	PortRX (variable from the return html file)	TX = (delta value[1] / (1000 * 1000)) / (polling interval[2])
RX	EE Monitors	HTTP	PortTX (variable from the return html file)	RX = (delta value[1] / (1000 * 1000)) / (polling interval[2])
TX	HBA, CNA	HCM API	N/A	TX = (delta value[1] / (1000 * 1000)) / (polling interval[2])
RX	HBA, CNA	HCM API	N/A	RX = (delta value[1] / (1000 * 1000)) / (polling interval[2])
TX	TE	SNMP	.1.3.6.1.2.1.31.1.1.1.6	TX = (delta value[1] / (1000 * 1000)) / (polling interval[2])
RX	TE	SNMP	.1.3.6.1.2.1.31.1.1.1.10	RX = (delta value[1] / (1000 * 1000)) / (polling interval[2])
TX% / RX%	FC, GE, HBA, CNA	N/A	N/A	TX% or RX% = ((TX or RX) / ((105000000 * port speed)* (polling interval[2])) * 100 If utilization is less than 1, the value is 0.0.
TX% / RX%	FCIP	N/A	N/A	TX% or RX% = ((bytes transferred) / (maximum bytes transmitted))*100 where maximum bytes transmitted = tunnel speed * 134217728 (maximum bytes transmitted 1 Gbps). If utilization is less than 1, the value is 0.0.
TX% / RX% (Pre-Fabric OS 6.4.1 release)	TE	N/A	N/A	TX% or RX% = ((TX or RX) / ((105000000 * 10)* (polling interval[2])) * 100 If utilization is less than 1, the value is 0.0.
Cumulative Compression Ratio	FCIP	N/A	.1.3.6.1.4.1.1588.4.1.1.4	Compression Ratio = current value/ 1000 The compression ratio is the current compression ratio value.
Current Compression Ratio	FCIP	N/A	N/A	(ifHCInOctets + ifHCOutOctets) / fcipExtendedLinkCompressedBytes
Receive EOF	TE		.1.3.6.1.2.1.16.1.1.1.5	Receive EOF = delta value[1] / (1000 * 1000)
Other[3]				Other counters = delta value[1]

1. The difference of the value retrieved between two consecutive polling cycles.
2. The duration between two polling cycle in seconds.
3. Additional performance counters are detailed in Table 86.

Table 87 lists the additional counters for which you can obtain performance statistics.

TABLE 87 Performance counters

Counter name	Type	Protocol	Source OID value
CRC Errors	FC	SNMP	.1.3.6.1.3.94.4.5.1.40
Signal Losses	FC	SNMP	.1.3.6.1.3.94.4.5.1.43
Sync Losses	FC	SNMP	.1.3.6.1.3.94.4.5.1.44
Link Failures	FC	SNMP	.1.3.6.1.3.94.4.5.1.39
Sequence Errors	FC	SNMP	.1.3.6.1.3.94.4.5.1.42
Invalid Transmissions	FC	SNMP	.1.3.6.1.3.94.4.5.1.41
Rx Link Resets	FC	SNMP	.1.3.6.1.3.94.4.5.1.33
Tx Link Resets	FC	SNMP	.1.3.6.1.3.94.4.5.1.34
C3 Discard	FC	SNMP	.1.3.6.1.3.94.4.5.1.28
C3 Discard Rx Timeout	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.27.1.25
C3 Discard Unreachable	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.27.1.26
C3 Discard Tx Timeout	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.27.1.27
C3 Discard Others	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.27.1.28
Encode Error Out	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.27.1.29
Temperature	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.28.1.1.1
Voltage	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.28.1.1.2
Current	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.28.1.1.3
Rx Power	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.28.1.1.4
Tx Power	FC	SNMP	.1.3.6.1.4.1.1588.2.1.1.1.28.1.1.5
Invalid Oredered Set	FC	SNMP	.1.3.6.1.3.94.4.5.1.45
BB Credit Zero	FC	SNMP	1.3.6.1.3.94.4.5.1.8
Truncated Frames	FC	SNMP	1.3.6.1.3.94.4.5.1.47
FEC Corrected Blocks	FC	SNMP	1.3.6.1.4.1.1588.2.1.1.1.27.1.31
FEC Uncorrected Blocks	FC	SNMP	1.3.6.1.4.1.1588.2.1.1.1.27.1.32
Latency	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.5
Dropped Packets	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.3
Link Retransmits	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.2
Timeout Retransmits	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.9
Fast Retransmits	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.10
Duplicate Ack Received	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.11
Window Size RTT	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.12
TCP Out of Order Segments	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.13
SlowStart Status	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.14
CRC Errors	EE Monitors	HTTP	PortCRC (variable from the return html file)

FIGURE 397

NOTE
Policies set for switches enabled for Monitoring and Alerting Policy Suite (MAPS) also display in this dialog box.

IP performance monitoring and traffic analysis

Use information in the following sections to monitor IP performance and analyze IP traffic.

IP configuration requirements

To be able to use **SNMP Monitor** for performance monitoring, make sure the following requirements are met:

- Ensure that SNMP is enabled on the devices you want to monitor and that SNMP community strings have been defined for **set** and **get** operations.
- Make sure discovery has been run and the devices appear on the Network Object Manager tree. If a device is not on the tree, add the device using Network Object Manager.
- Define what data you want to collect.
- If you need to monitor devices within specific device groups, you must create the device groups.
- You must have the **SNMP Monitor** privilege in your user account or role.

Management application comes with default MIB files, such as standard MIB and Brocade proprietary MIB files.

IP real-time performance monitoring

Real-time performance monitoring allows you to view a snapshot of current performance data. You can enable real-time performance monitoring without configuring historical data collectors. The data is not stored in the database. Performance monitoring allows you to define a data collector by mapping a Management Information Base (MIB) object to a unit name (refer to "MIB data collectors" on page 1013).

Real-time performance measures are built-in expressions. The following measures are available:

Device measures

- Power Allocation (NS)
- Power Allocation % (NS)
- CPU utilization
- Memory utilization
- Temperature

Port measures

- Optics
- Power Allocation (NS)
- Consumption (W)
- Power Consumption %
- Input and output utilization
- Throughput
- Input and output errors
- FC Port transmit and receive utilization (VDX only)
- FC Port transmit and receive in megabits per second (VDX only)

Monitoring real-time performance

If no products have been selected for real-time performance monitoring, you can select products and data collectors by taking the following steps.

1. Select **Monitor > Performance > Real Time Graphs/Tables**.

   The **Select Sources - Real Time Graphs/Tables** dialog box displays, as shown in .Figure 398 on page 983.

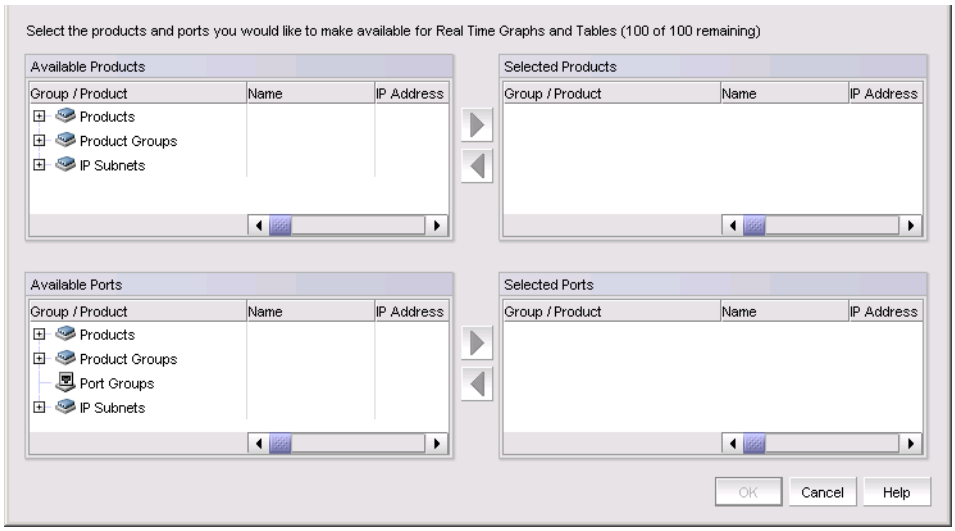


FIGURE 398 Select Sources - Real Time Graphs / Tables dialog box

2. Select the products you want in the **Available Products** list and click the right arrow button to move them to the **Selected Products** list.

NOTE
You cannot select more than 100 products and ports.

3. Select the ports you want in the **Available Ports** list and click the right arrow button to move them to the **Selected Ports** list.
4. Click **OK**.

   The **Real Time Graphs/Tables** dialog box displays.
5. Use the **Show** list to toggle the tree structure display between **Products** and **Collectibles**.

   When you select **Products**, the tree structure shows devices on the network that are being polled for collectible data.

   When you select **Collectibles**, the tree structure shows the MIB objects and expressions associated with products.
6. Add collectors to be monitored by completing the following steps.

NOTE
You cannot select more than 20 collectors at a time.

   a. Choose from the following options:
      - To view performance for all collectors defined for the product, click the product. To add collectors to a product, refer to "Adding measures to products" on page 986.
      - To view performance for all collectors defined for the port, click an individual port. To add collectors to a port, refer to "Adding measures to ports" on page 987.
      - To view a single collector, click an individual collector under a product or port.

   b. Click the right arrow button.
7. Remove collectors from the monitor by selecting the collector beneath the graph and clicking the left arrow button.
8. To configure the look and feel of the performance graph from the **Real Time Graphs/Tables** dialog box, refer to "Configuring the performance graph" on page 989.
9. Click the **Collection Status Summary** tab to view the following information.

   The **Collection Status Summary** tab provides a high-level overview of all defined collectors. The information is displayed in the following columns:
   - **Product** - Shows the product name and IP address. There may be multiple instances of the product name for each collectible assigned to the product.
   - **Port** - The port name when a port is selected.
   - **Collectible** - The MIB objects and expressions used by the data collector.
   - **Status** - The status field uses the following icons, as shown in Table 88 on page 985.

TABLE 88 Collection status icons

	Failed. No value was ever collected for this collectible.
	Warning: Data collection failed in the last polling cycle.
	Successful: Last collection successful.
	Scheduled but not currently active.

- **Last Value** - The last (most current) value collected.
- **Last Time Polled** - The time that the collector was last polled.

10. Click **Sources** to add products and ports to or remove products and ports from real-time performance monitoring. Refer to "Adding products and ports to real-time performance" on page 985 and "Removing products and ports from real-time performance" on page 985.
11. Click **Close** to close the dialog box.

Adding products and ports to real-time performance

To add products and ports to real-time performance monitoring, complete the following steps.

1. Click **Sources** from the **Real Time Graphs/Tables** dialog box.
2. Select the products you want in the **Available Products** list and click the right arrow button to move them to the **Selected Products** list.

NOTE
You cannot select more than 100 products and ports.

3. Select the ports you want in the **Available Ports** list and click the right arrow button to move them to the **Selected Ports** list.
4. Click **OK**.

   The **Real Time Graphs/Tables** dialog box displays.

Removing products and ports from real-time performance

To remove products and ports from real-time performance monitoring, complete the following steps.

1. Click **Sources** from the **Real Time Graphs/Tables** dialog box.
2. Select the products you want to remove in the **Selected Products** list and click the left arrow button to move them to the **Available Products** list.
3. Select the ports you want to remove in the **Selected Ports** list and click the left arrow button to move them to the **Available Ports** table.
4. Click **OK**.

5. The **Real Time Graphs/Tables** dialog box displays.

Adding measures to products

To add measures to products, complete the following steps.

1. Right-click a device and select **Performance > Real Time Graph/Table.**

   The **Real Time Graphs/Tables** dialog box displays.

2. Select **Products** from the **Show** list.

   The available products display in a list.

3. Select a product in the list and click **Measures**.

   The **Select measures - Real Time Graphs/Tables** dialog box displays.

4. Select **Device Measures** from the **Show** list.

5. To add a MIB measure to the product, complete the following steps.

   a. Click **MIBS** tab in the **Available Measures** area.

   b. Select the MIB measure you want to add to the product.

      Select multiple measures by holding down the **CTRL** key and clicking more than one measure.

      You can also search (refer to "Search" on page 299) for a MIB in the list.

   c. Click the right arrow button to move them to the **Selected Measures** list.

6. To add an expression to the product, complete the following steps.

   a. Click the **Expressions** tab in the **Available Measures** area.

   b. Select the expression you want to add to the product.

      Select multiple expressions by holding down the **CTRL** key and clicking more than one expression.

      To add an expression to the list, refer to "Adding, editing, or duplicating a user-defined expression" on page 1006.

   c. Click the right arrow button to move them to the **Selected Measures** list.

7. If you want to launch the **Expressions** dialog box, click the **Expressions** button.

8. Click **OK**.

   The **Real Time Graphs/Tables** dialog box displays.

Removing measures from products

To remove measures from products, complete the following steps.

1. Right-click a device and select **Performance > Real Time Graph/Table.**

   The **Real Time Graphs/Tables** dialog box displays.

2. Select **Products** from the **Show** list.

   The available products display in a list.

3. Select a product in the list and click **Measures**.

   The **Select measures - Real Time Graphs/Tables** dialog box displays.

4. Select **Device Measures** from the **Show** list.
5. To remove an MIB or expression from the product, complete the following steps.
   a. Select the MIB or expression you want to remove from the product in the **Selected Measures** list.

      Select multiple MIBs and expressions by holding down the **CTRL** key and clicking more than one MIB or expression.

   b. Click the left arrow button to remove them from the **Selected Measures** list.
6. Click **OK**.

   The **Real Time Graphs/Tables** dialog box displays.

Adding measures to ports

To add measures to ports, complete the following steps.

1. Right-click a device and select **Performance > Real Time Graph/Table.**

   The **Real Time Graphs/Tables** dialog box displays.

2. Select **Products** from the **Show** list.

   The available products display in a list.

3. Expand the list and select a port in the list and click **Select Measures**.

   The **Select measures - Real Time Graphs/Tables** dialog box displays.

4. Select **Port Measures** from the **Show** list.
5. To add a MIB measure to the port, complete the following steps.
   a. Click the **MIBS** tab in the **Available Measures** area.
   b. Select the MIB measure you want to add to the port.

      Select multiple measures by holding down the **CTRL** key and clicking more than one measure.

      You can also search (refer to "Search" on page 299) for a MIB in the list.

   c. Click the right arrow button to move them to the **Selected Measures** list.
6. To add an expression to the port, complete the following steps.
   a. Click the **Expressions** tab in the **Available Measures** area.
   b. Select the expression you want to add to the port.

      Select multiple expressions by holding down the **CTRL** key and clicking more than one expression.

      To add an expression to the list, refer to "Adding, editing, or duplicating a user-defined expression" on page 1006.

   c. Click the right arrow button to move them to the **Selected Measures** list.
7. If you want to launch the **Expressions** dialog box, click the **Expressions** button.

8. Click **OK**.

   The **Real Time Graphs/Tables** dialog box displays.

Removing measures from ports

To remove measures from ports, complete the following steps.

1. Right-click a device and select **Performance > Real Time Graph/Table.**

   The **Real Time Graphs/Tables** dialog box displays.

2. Select **Products** from the **Show** list.

   The available products display in a list.

3. Expand the list and select a port in the list and click **Measures**.

   The **Select measures - Real Time Graphs/Tables** dialog box displays.

4. Select **Port Measures** from the **Show** list.

5. To remove an MIB or expression from the port, complete the following steps.

   a. Select the MIB or expression you want to remove from the port in the **Selected Measures** list.

      Select multiple MIBs and expressions by holding down the **CTRL** key and clicking more than one MIB or expression.

   b. Click the left arrow button to remove them from the **Selected Measures** list.

6. Click **OK**.

   The **Real Time Graphs/Tables** dialog box displays.

Adding collectibles to monitoring

NOTE
You cannot select more than 20 collectors at a time.

To add collectibles to performance monitoring, complete the following steps.

1. Add all collectibles defined for a device by completing the following steps.

   a. Select **Show > Products** to show devices on the network that are being polled for collectible data.

   b. Select the product you want to include in performance in the tree. Press CTRL and click to select multiple products.

   c. Click the right arrow button.

      The graph and table are populated with the collectible performance values. All collectibles defined for the selected product display beneath the graph.

2. Add all collectibles defined for a port by completing the following steps.

a. Select **Show > Products** to show devices on the network that are being polled for collectible data.

b. Select the port you want to include in performance in the tree. Press CTRL and click to select multiple ports.

c. Click the right arrow button.

The graph and table are populated with the collectible performance values. All collectibles defined for the selected port display beneath the graph.

3. Add an individual collectibles by completing the following steps.

a. Select **Show > Collectibles** to show the MIB objects and expressions.

b. Select the collectible to include in performance in the tree. Press CTRL and click to select multiple collectibles.

c. Click the right arrow button.

The graph and table are populated with the collectible performance values. The selected collectibles displays beneath the graph.

Removing collectibles from monitoring

To remove collectibles from performance monitoring, complete the following steps.

1. Select the collectible you want to delete remove the graph. Press CTRL and click to select multiple collectible.
2. Click the left arrow button.

Configuring the performance graph

To configure the look and feel of the performance graph from the **Historical** or **Real Time Graphs/Tables** dialog boxes, complete the steps under "Configuring the performance graph display" and "Configuring graph options" on page 991.

Configuring the performance graph display

Use the procedure to configure the graph display for the **Real Time Graphs/Tables** dialog box and **Historical Graphs/Tables** dialog box as well as time series monitors on the **Dashboard** tab or **Performance Dashboard**.

1. Right-click the graph and select one of the following options.

- Select the **Show Controls** check box to show or hide additional display options on the graph (refer to step 3 through step 9 for more information).
- Select the **Show Legend** check box to show or hide the measurements beneath the graph.
- Select **Clear Graph** to clear the graph.
- Select **Deleted Selected Measures** to delete the selected measures from performance.
- Select **Zoom In** to zoom in on the graph.
- Select **Zoom Out** to zoom out on the graph.
- Select **Fit in window** to fit the graph in the window.

- Select **Go to Latest** to go to the latest data point on the graph.
- Select the **Use Logarithmic Axis** check box to present data on a logarithmic or non-logarithmic axis.
- Select the **Show Values** check box to annotate data point values in the graph.
- Select the **Enable Auto Scrolling** check box to automatically jump to display the new data when new data is collected while the graph is in view.
- Select the **Enable Transition Effect** check box to automatically adjusts the range on the vertical axis so that all the data are contained within the view area when you drag the chart into a different time range on the SNMP monitoring graph.
- Select **Plot Min/Max** to plot minimum and maximum values along with the average data point This option is not available if minimum interval granularity (5 minutes for SAN historical graph) is selected. The width of the color band displayed on the graph indicates the variation during the time period.
- Select **Show Events** to display advanced monitoring service (AMS) violation events received during the chart time range and master log events logged on the same product as the measure being plotted.
- Select **Chart Styles** to display data as a line chart, area chart, or bar chart.
- Select **Options** to launch the **Graph Options** dialog box. Refer to "Configuring graph options" on page 991 for more information.
- Select **Export** to export to a spreadsheet (.csv) or an image (.png).
- Select **Print** to print the graph.

2. (**Historical Graphs/Tables** and **Real Time Graphs/Tables** dialog boxes only) Select **Graph Style** on the **Real Time Graphs/Tables** dialog toolbar to display an **Options** dialog box. The following options are available for **Performance Graph Styles**:

   - **Color Scheme** - Change the graph background to white or black.
   - **Show Data Points** - Displays data points on the graph. Figure 399 on page 990 is an example of a graph when **Show data points** is selected.

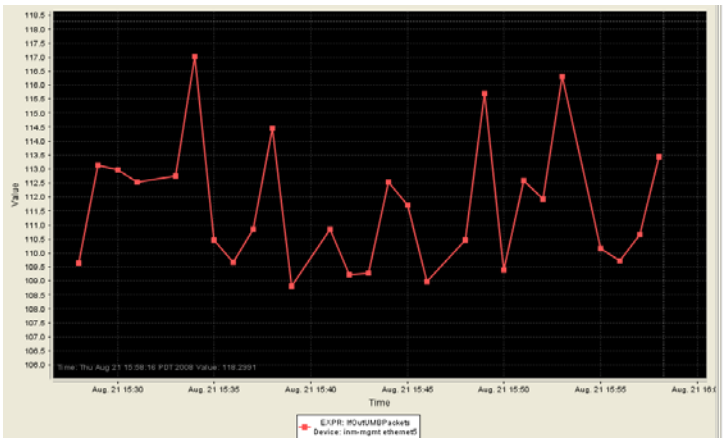


FIGURE 399 Show data points graph

NOTE
Although these settings will apply to all performance graphics in the management application. the change will not reflect instantly on the **Performance Dashboard** monitor that displays the graph. Rather it will be updated the next time those monitors are launched.

3. Click **Options** to launch the **Graph Options** dialog box. Refer to "Configuring graph options" on page 991 for instructions on using this dialog box.
4. Select the **Graph** or **Table** option to display data in graphical or tabular format.
5. Select a time range relative to the present for the display of historical data from the **For** list.

   The options are incremental from the last 30 minutes to the last 24 hours.
6. (Historical graphs and monitors only) Select the **Plot Min/Max** check box to plot minimum and maximum values along with the average data point.

   The range between the minimum and maximum values will be represented in a color band surrounding the data points. The width of the color band indicates the variation during the time period. Note that this option is not available if you select **Minimum Interval** granularity.
7. (Historical graphs and monitors only) Select one of the following options from the **Granularity** list to set the granularity of the data point to display on the graph:
   - 5 minutes
   - 30 minutes
   - 2 hours
   - 1 day

NOTE
The graph will not update dynamically if the granularity is 30 minutes, 2 hours, or 1 day. To update, move from one granularity setting to another. The graph will update dynamically when **Minimum interval** is selected.

8. Select the **Events** check box to display advanced monitoring service (AMS) violation events received during the chart time range.
9. (**Real Time Graphs/Tables** and **Historical Graphs/Tables** dialog boxes only) Click **Save as Widget** to create a performance monitor published widget on the active dashboard. For instructions, refer to "Configuring a monitor from a performance graph" on page 278.

Configuring graph options

Use the following steps to configure graph options for Real Time Performance Graph display as well as time series monitors on the **Dashboard** tab or **Performance Dashboard**.

1. Click **Options** on the graph.

   The **Graph Options** dialog box displays, as shown in Figure 400 on page 992.

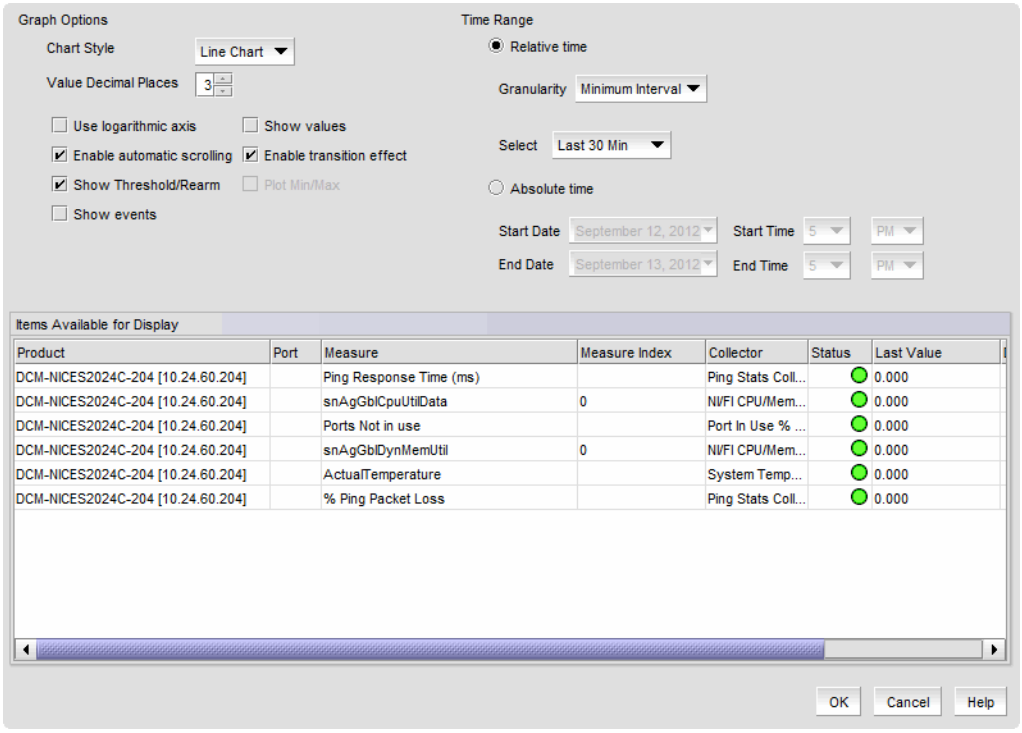


FIGURE 400 Graph Options dialog box (Historical Graphs/Tables dialog box)

NOTE
Figure 400 illustrates the **Graph Options** dialog box available from the **Historical Graphs/Tables** dialog box. The **Graph Options** dialog box available from the **Real Time Graphs/Tables** dialog box is similar, but has fewer control options.

2. Select the type of chart style from the **Chart Style** list.

   Available chart styles include **Line Chart**, **Area Chart**, or **Bar Chart**.

3. Select the graph accuracy to up to three decimal places in the **Value Decimal Places** list.
4. Select from the following check boxes to define how polled data displays:

   - **Use logarithmic axis** check box — Data can be presented on a logarithmic or non-logarithmic axis. Each unit in a non-logarithmic axis presents the data in equal segments. However, logarithmic axis units are not equal and can increase exponentially by 10. Therefore, use a logarithmic axis if you have a large amount of data to view.
   - **Show values** check box — Annotates data point values in the graph.
   - **Enable automatic scrolling** check box — If new data is collected while the chart is in view, the chart will automatically jump to display the new data.
   - **Enable transition effect** check box — The SNMP monitoring chart automatically adjusts the range on the vertical axis so that all the data are contained within the view area when you drag the chart into a different time range. Enabling this option provides an animated smooth transition between the adjustments while the monitoring chart is being dragged or any action that may cause the range of vertical axis to change.
   - **Show Threshold/Rearm** — Displays threshold and rearm events on the chart.

- (Historical graphs and monitors only) **Plot Min/Max** - Plots minimum and maximum values along with the average data. The range between the minimum and maximum values will be represented by the width of a color band surrounding the data points as shown in the following illustration. Note that this option is not available if you select **Minimum Interval** granularity. It also does not apply and is not available for Real Time Performance graphs.

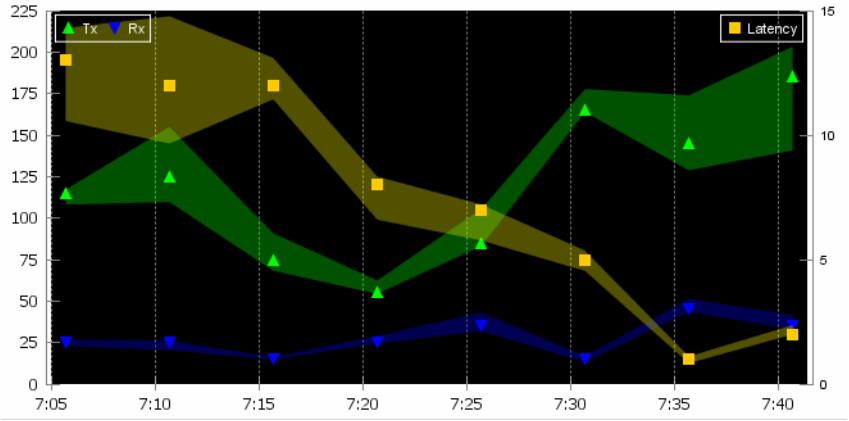


FIGURE 401 Data points graph

- **Show Events** - Select to display advanced monitoring service (AMS) violation events received during the chart time range and master log events logged on the same product as the measure being plotted. Each event will be represented by the same severity icon that is shown in the master log (refer to icons a bottom of following graph). Hovering the cursor over the icon displays details of the violation, such as violation time, switch/port information, violated rule name, and violated rule condition. Monitoring and Alerting Policy Suite (MAPS) violations are plotted for a product or port level measure (whichever is selected) during the plotted time range. The show events graph is shown in Figure 402 on page 993

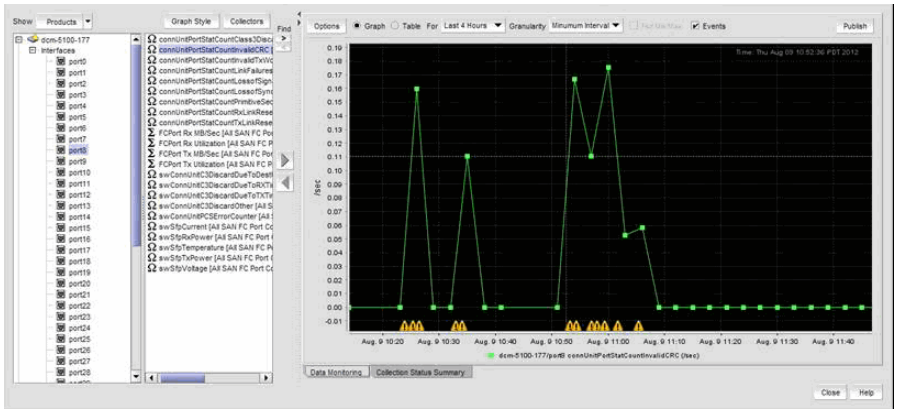


FIGURE 402 Show events graph

5. In the **Time Range** area, select one of the following options:
   - Select **Relative time** to set a time range relative to the present for the display of historical data.

a. (Historical graphs and monitors only) Select the granularity of the data points to display on the graph from the **Granularity** list. Options are 5 minutes, 30 minutes, 2 hours, or 1 day.

NOTE
The graph will not update dynamically if the granularity is 30 Minutes, 2 Hours, or 1 day. To update, click **Apply**. The graph will update dynamically when Minimum interval is selected.

b. Select the duration of time for data display on the graph from **Select** list.
Real time options are incremental from the last 30 minutes to the last 6 hours.
Historical options are incremental from the last 30 minutes to the last 24 hours.

- (Historical graphs and monitors only) Select **Absolute time** to get a snapshot of data from a specific time range and complete the following steps.

a. Select the start date from the **Start Date** list.

b. Select the start time (1 through 12) from the first **Start Time** list.

c. Select **AM** or **PM** from the second **Start Time** list.

d. Select the end date from the **End Date** list.

e. Select the end time (1 through 12) from the first **End Time** list.

f. Select **AM** or **PM** from the second **End Time** list.

6. Include items in the graph by selecting the **Display** check box for each item in the **Items Available for Display** list.
7. Set the scale factor for each item by entering a value (integer between -2147483648 and 2147483647) in the **Scaling Factor** column for each item in the **Items Available for Display** table.
8. Click **OK** on the **Graph Options** dialog box.

Exporting a graph

To export a graph, complete the following steps.

1. Right-click the graph and select **Export**.

   The **Choose Export File Format** dialog box displays.
2. Select one of the following options.
   - **Spreadsheet (.csv)**
   - **Image (.png)**

   The **Save** dialog box displays.
3. Browse to the location where you want to save the export file.
4. Enter a name for the export file.
5. Click **Save**.

Printing a graph

To print a graph, complete the following steps.

1. Right-click the graph and select **Print**.

   The **Page Setup** dialog box displays.

2. Edit the paper, orientation, and margins, as needed.
3. Click **Printer** to select a printer.
4. Click **OK**.

IP historical performance monitoring

Historical performance monitoring allows you create data collectors by choosing MIB object and by choosing or creating mathematical expressions. You can also configure a historical data graph or table to display data. The following options and features are available for obtaining historical performance data:

- Define a data collector by mapping a MIB (Management Information Base) object to a unit name (refer to "MIB data collectors" on page 1013).
- Specify and adjust threshold values and polling intervals, and set time schedules for data collection. Historical data is recorded in a database for retrieval in the form of graphs and tables.
- Store records for each port.
- Create a custom graph or table display for data by defining options such as the following:
  - Selecting a product for displaying data.
  - Selecting measures to collect.
  - Modifying collectors.
  - Plotting minimum and maximum values.
  - Displaying data points or polling intervals.
  - Displaying events.
  - Selecting a graph or table format.
  - Enabling granularity of data to display:
    - 5 minutes granularity for last 8 days
    - 30 minutes granularity for last 14 days
    - 2 hour granularity for last 30 days
    - 1 day granularity for last 730 days
  - Displaying advanced monitoring service (AMS) violation events.
  - Providing a period for plotting the graph or table.

Related topics

"Editing system collectors"

"Displaying historical data collectors"

"Enabling a historical data collector"

"Adding or editing a historical data collector"

""

Editing system collectors

Subject to the following restrictions, you can edit system collectors using the **Data Collector** wizard (refer to "Adding or editing a historical data collector" on page 998).

You can modify the following attributes:

- Enable/disable settings - **Collector Basics** page
- Target selection - **Select Source** page
- Threshold and Rearm settings - **Threshold and Rearm** page

You cannot modify the following attributes:

- Name - **Collector Basics** page
- Device or port level - **Collector Basics** page
- Polling interval - **Collector Basics** page
- Schedule setting - **Collector Basics** page
- MIB selection - **MIB Object** page
- Expression selection - **Expression** page
- MIB index - **MIB Index** page

NOTE
The MIB Index page for system collectors will not show because you cannot configure the MIB index for system collectors.

Displaying historical data collectors

Select **Monitor > Performance > Historical Data Collectors** to display configured historical data collectors.

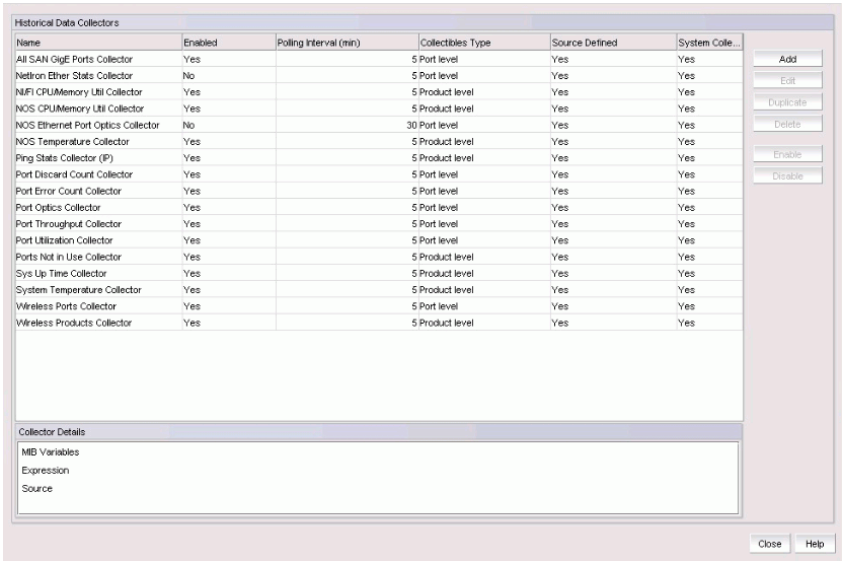


FIGURE 403 **Historical Data Collectors dialog box**

All configured data collectors are listed, showing the following information:

- **Name** - The name of the data collector.
- **Enabled** - Whether or not the data collector is enabled (Yes) or disabled (No).

NOTE
The Netiron Ether Stats Collector and NOS Ethernet Port Optics Collector will be disabled by default.

- **Polling Interval** - The time interval, in minutes, between attempts to contact the information source and gather data.

NOTE
The Polling Interval for NOS ethernet port optics collector is 30 minutes.

- **Collectibles Type** - At what level the data will be collected and the types of MIB objects used:
  - **Product Level** - SNMP data is collected at the product (device) level.
  - **Port Level** - SNMP data is collected at the port level.
- **Source Defined** - Whether or not the information source (product or port) is defined (Yes) or not configured (No).
- **System Collectors** - Whether or not this is a system data collector. Refer to the following sections for more information:
  - "Editing system collectors" on page 996
  - "Duplicating system data collectors" on page 1006

When you select a listed data collector, The following information is displayed in the **Collector Details** field:

- **MIB Variables** - The MIB variables used (if any).
- **Expression** - The expression used (if any).
- **Source** - The defined products used as information sources by this collector.

Enabling a historical data collector

Use the following steps to enable a data collector to collect historical data or disable a data collector from collecting data.

1. Select an historical data collector on the **Historical Data Collectors** dialog box.

- If the collector is disabled, the **Enable** button is active.
- If the collector is enabled, the **Disable** button is active.

2. Click **Enable** to enable the collector.
3. Click **Disable** to disable the collector.

Adding or editing a historical data collector

Use the following procedure to add or edit a historical data collector using the **Data Collector** wizard.

NOTE
There are specific options that you can edit for system collectors. Refer to "Editing system collectors" on page 996 for details.

1. Select **Monitor** > **Performance** > **Historical data collectors.**

   The **Historical Data Collectors** dialog box displays.

2. Perform either of the following steps:

   - Select a collector and click the **Edit** button.

     The **Data Collector** wizard **Collector Basics** dialog box displays where you can edit values for the existing collector.

   - Click the **Add** button

     The **Data Collector** wizard **Collector Basics** dialog box displays where you can add values for a new collector.

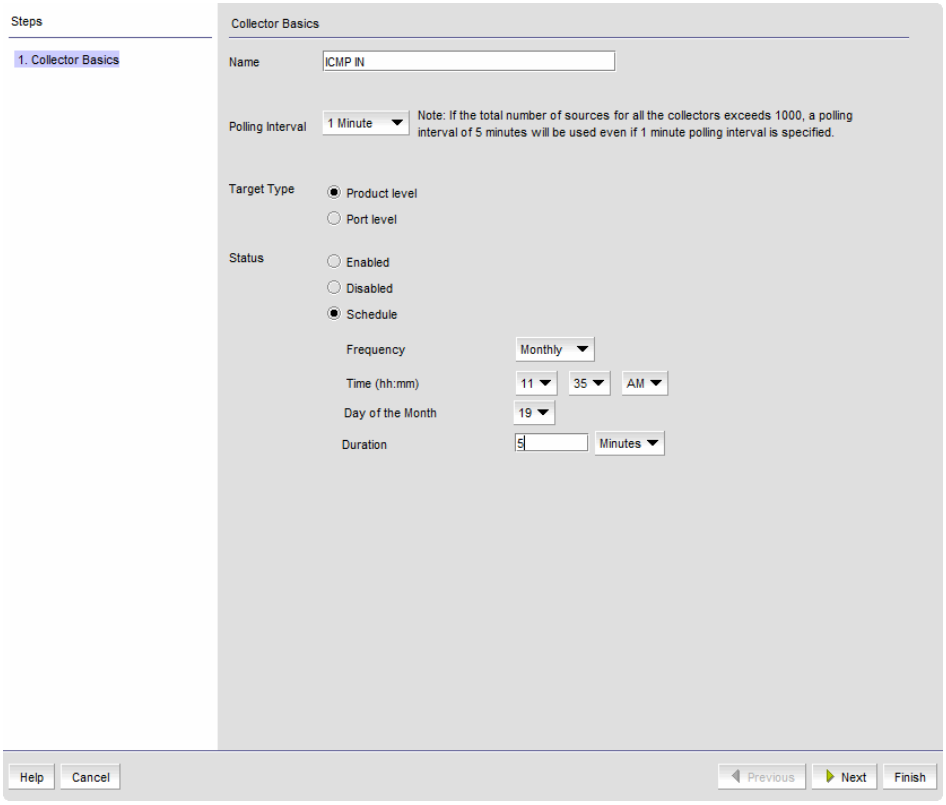


FIGURE 404 Data Collector wizard Collector Basics dialog box

3. Enter a descriptive name for the data collector in the **Name** field.
4. Use the **Polling Interval** list to set the polling interval.

   The choices are 1 minute, 5 minutes, 10 minutes, 15 minutes, and 30 minutes.
5. Select the **Target Type**.
   - If you select **Product level**, SNMP data is collected at the product (device) level.
   - If you select **Port level**, SNMP data is collected at the port level.
6. Select the **Status** of the collector.
   - If you select **Enabled**, the data collector starts collecting data immediately.
   - If you select **Disabled**, the data collector stops collecting data.
   - If you select **Schedule**, you may set up a time schedule for running the data collector.

   The following options become active when you select **Schedule**:

   - **Frequency** - This list allows you to run the data collector on a **Yearly**, **Monthly**, **Weekly**, **Daily**, **Hourly**, or **One Time** basis. Appropriate options are displayed allowing you to set a start time and duration for data collection.
     - If you select **Yearly**, or **One Time**, the **Time (hh:mm)** and **Date** selectors display.
     - If you select **Monthly**, the **Time (hh:mm)** and **Day of the Month** selectors display.
     - If you select **Weekly**, the **Time (hh:mm)** and **Day of the Week** selectors display.
     - If you select **Daily**, the **Time (hh:mm)** selector displays.

- **Duration** - Enter a value in the **Duration** field, and then select the unit of measure. The options are **Minutes**, **Hours**, and **Days**.

7. Click **Next** on the **Collector Basics** dialog box.

   The **MIB Objects** dialog box displays.

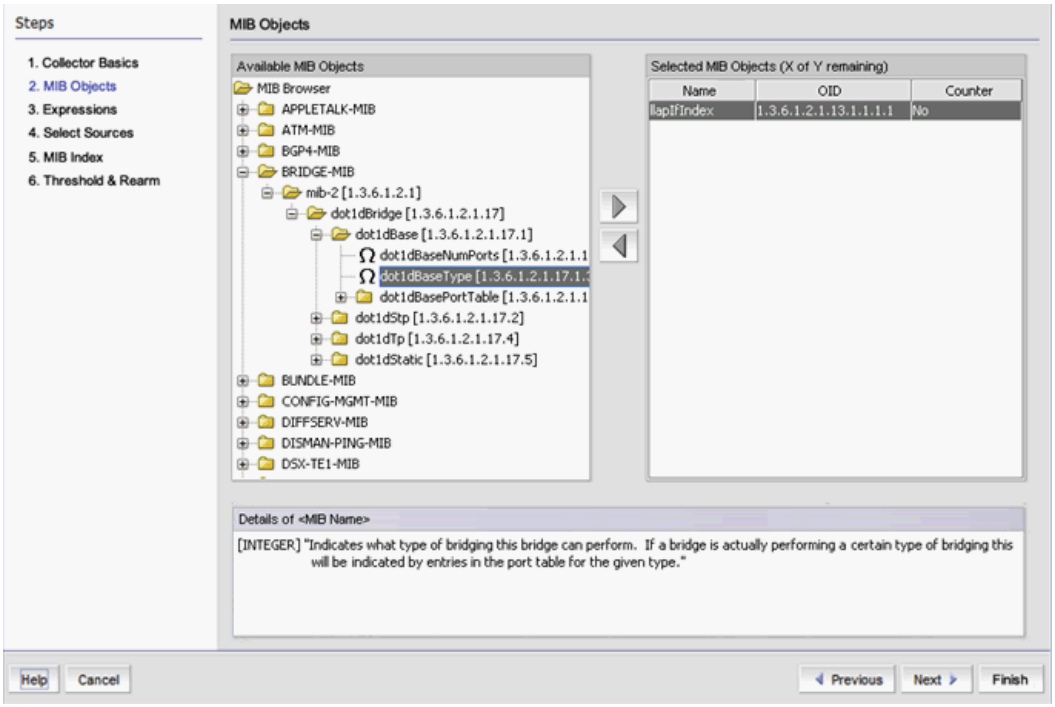


FIGURE 405 Data Collector wizard MIB Objects dialog box

The **Available MIB Objects** tree includes all integer-based objects that are available by default and any that have been imported. Third-party device MIB objects are not available by default. You must manually add the third-party device MIB objects (refer to "Adding third-party device MIB objects manually" on page 1005).

NOTE
Performance does not support string-based MIB objects.

8. Expand a MIB folder to display the MIB objects.
9. Select a MIB object.

   A description of the MIB object displays under **Details of <MIB name>**.

10. To include the MIB object in your data collector, click the right arrow button to move the object to the **Selected MIB Objects** list. You can select multiple MIB objects, however, you cannot move a folder. Note the limit on the number of objects that can be selected and the number of choices remaining.
11. Click **Next** on the **MIB Objects** dialog box.

    The **Expressions** dialog box displays.

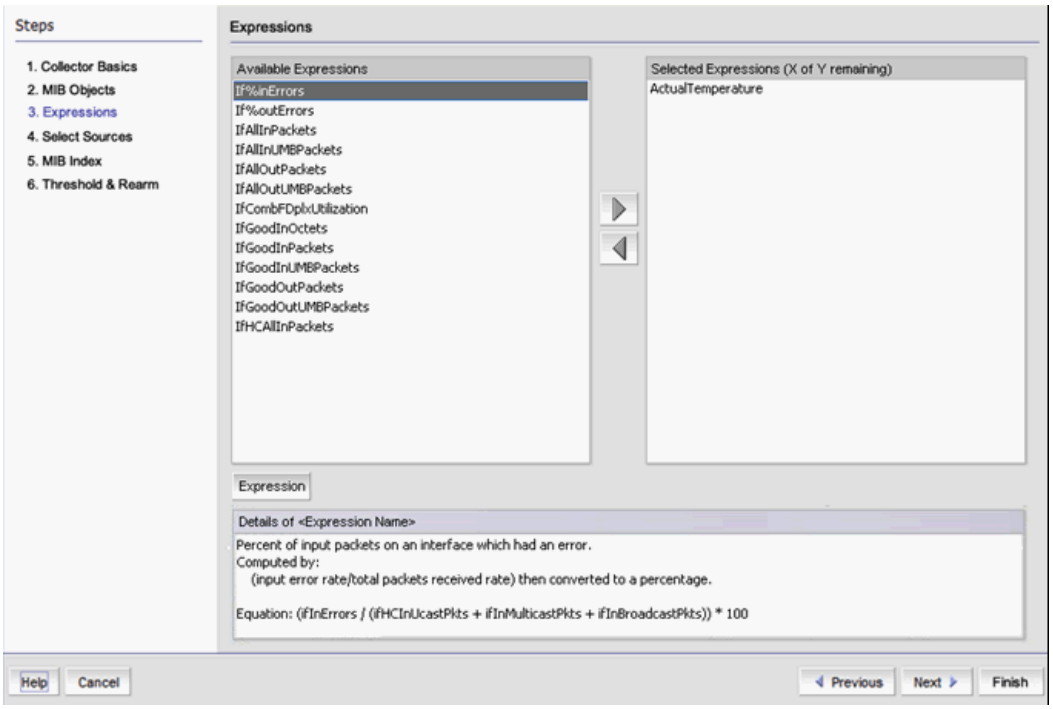


FIGURE 406 Data Collector wizard Expressions dialog box

The **Available Expressions** list shows all expressions that are available by default and any that have been defined by the user.

12. Select an expression from the **Available Expressions** list.

    A description of the expression displays under **Details of <Expression Name>**.

13. To include the expression in your data collector, click the right arrow button to move the expression to the **Selected Expressions** list. Note the limit on the number of expressions that can be selected and the number of choices remaining.

NOTE
You can click the **Expression** button to add a user-defined expression at this time. Refer to "Adding, editing, or duplicating a user-defined expression"for instructions.

14. Click **Next** on the **Expressions** dialog box.

    The **Select Sources** dialog box displays.

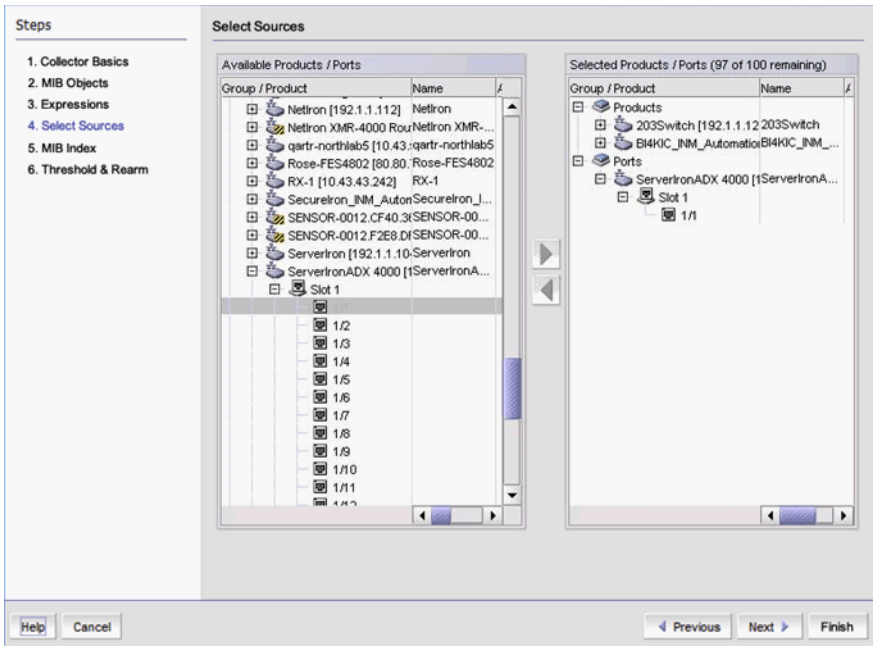


FIGURE 407 Data Collector wizard Select Sources dialog box

The **Available Products/Ports** tree structure includes all products and ports that can be monitored. You can expand folders to display all available products and ports.

If you have selected **Port Level** on the **Collector Basics** dialog box, trunk objects will be included as available targets in the form of LAG, vLAG, or TRILL objects. Only ifindex-based MIBs or expressions are supported.

15. Select a folder, individual products, and ports that you want to monitor (the sources of data for your data collector) and click the right arrow to move the folder, product, or port to the **Selected Products/Ports** list.

    When you select a product and move it to **Selected Products/Ports**, the folder is moved into a **Products** folder tree structure. When you select a port and move it to **Selected Products/Ports**, the port is moved into a **Ports** folder tree structure.

    You can also select a product group or port group. When you select a group and move it, all member products or ports are moved to the **Selected Products/Ports** list.

16. Click **Next** on the **Select Sources** dialog box.

    The **MIB Index** dialog box displays.

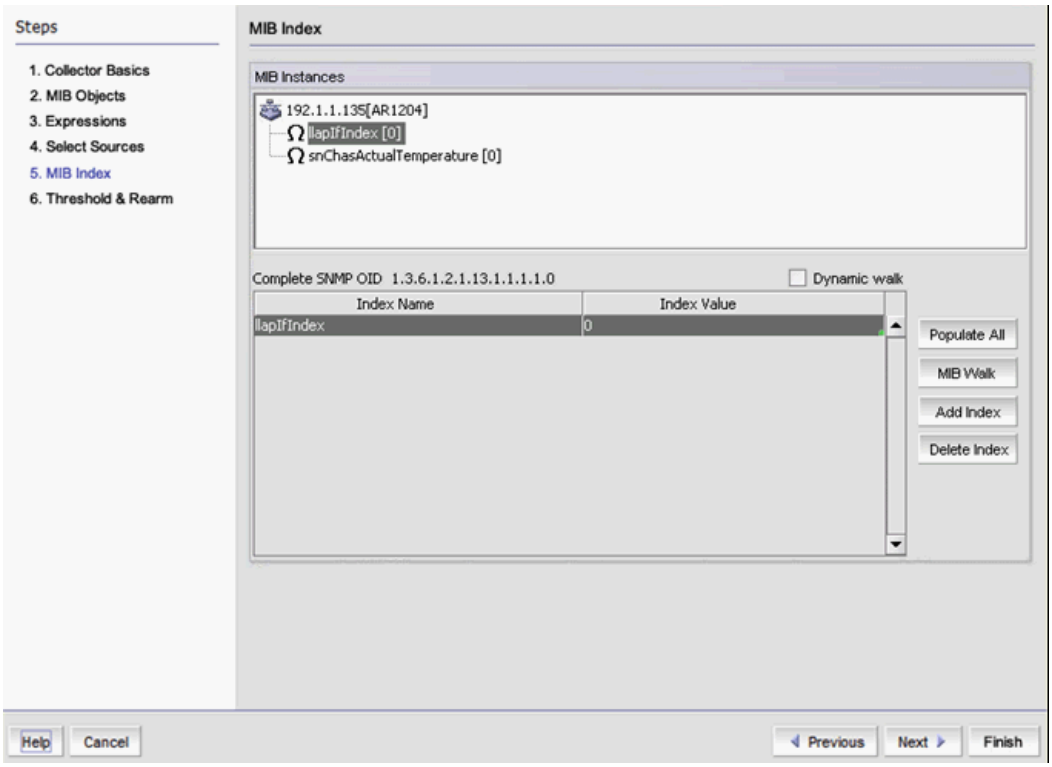


FIGURE 408 Data Collector wizard MIB Index dialog box

You can define index values for each MIB object that requires an index.

17. From the **MIB Instances** list, select the required MIB variable.

    The **Complete SNMP OID**, the **Index Name**, and the **Index Value** display beneath the **MIB Instances** list.

18. You have several options for entering index information:

    - Select the **Dynamic walk** check box to dynamically select index values for a particular index. When enabled, instances are selected based on a MIB walk.
    - Click the **Populate All** button to populate the index with all objects. You can then use the **Delete Index** button to delete any objects you do not need.

      If you selected a product collector, the index is populated with indexes of all instances of the selected MIB variable.

      If you selected a port collector, the index is populated with the ifIndex value of the port with which the MIB variable is associated.
    - Click the **MIB Walk** button to start a MIB walk facility. Refer to "Configuring a MIB walk instance" on page 1005.
    - Click the **Add Index** button to add an index.
    - Click the **Delete Index** button to delete an index.

19. Click **Next** on the **MIB Index** dialog box.

    The **Threshold & Rearm** dialog box displays.

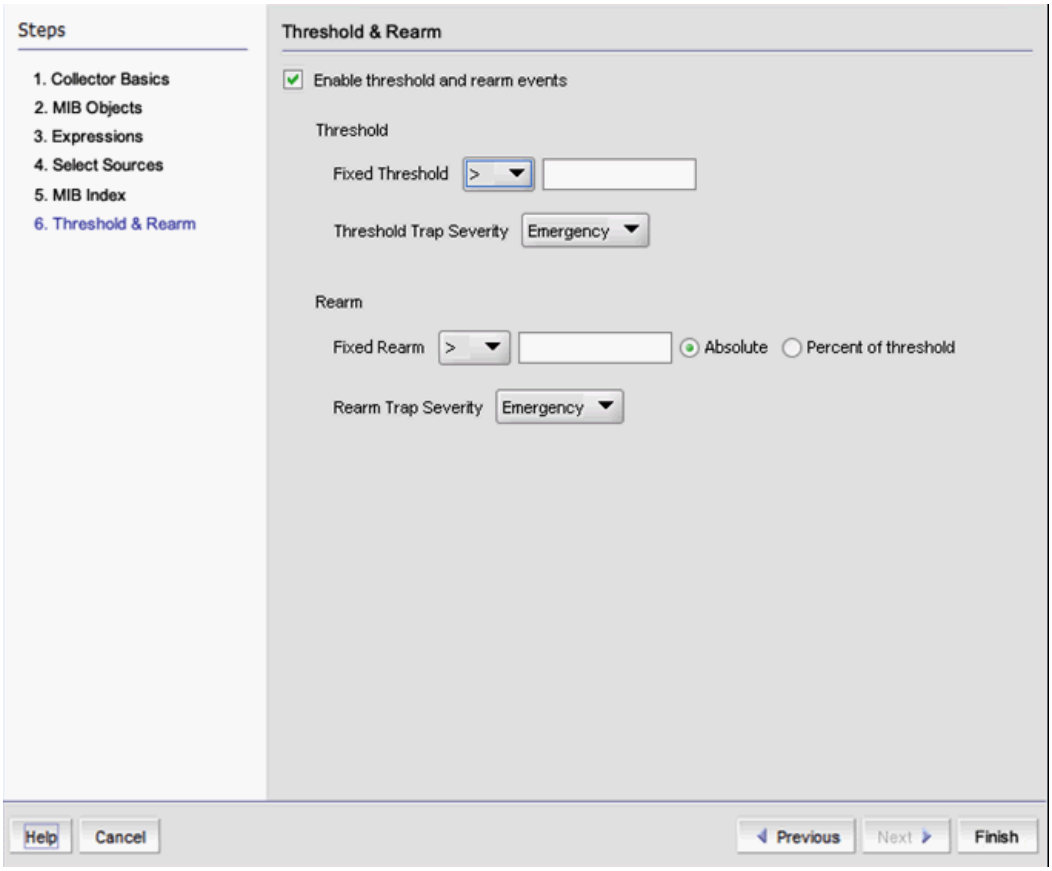


FIGURE 409 Data Collector wizard Threshold & Rearm dialog box

This **Threshold & Rearm** dialog box allows you to establish a a threshold value that triggers a trap message when the threshold is met, and to establish conditions for repeating threshold check and trap messages.

20. Select the **Enable threshold and rearm events** check box to enable the **Threshold** and **Rearm** selectors.
21. Select the **Fixed Threshold** value and assign a **Threshold Trap Severity** level.
22. Select the **Fixed Rearm** value and assign a **Rearm Trap Severity** level. If the **Fixed Rearm** value is the exact value used to trigger rearming (repeating the threshold check and trap message), select **Absolute**. If the **Fixed Rearm** value is expressed as a percentage of the threshold value, select **Percent of threshold**.
23. Click **Finish** to accept your entries.

Adding third-party device MIB objects manually

To add a third-party device MIB object manually, complete the following steps.

1. Copy the third-party device MIB objects to the *Install_Home*\conf\mibs\ip directory.
2. Go to *Install_Home*\conf\mibs and open the mibs_to_compile.txt file in a text editor.
3. Add the MIB file names to the mibs_to_compile.txt file.
4. Save and close the mibs_to_compile.txt file.
5. Launch the **MIB Objects** dialog box to view the third-party device MIB objects. Refer to "Adding or editing a historical data collector" on page 998.

Configuring a MIB walk instance

To configure a MIB walk instance, complete the following steps.

1. Launch the **MIB Index** dialog box. Refer to "Adding or editing a historical data collector" on page 998.
2. Select an MIB object from the **MIB Instance** list and click **MIB Walk**.

   The **MIB Walk** dialog box displays all existing instances of the selected MIB on the selected product.

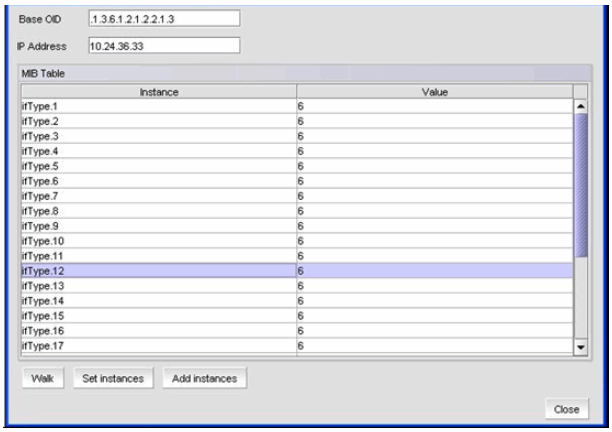


FIGURE 410 MIB Walk dialog box

3. Select an instance from the list and click **Add Instances** to add the selected index to the list.
4. Select an instance from the list and click **Set Instances** to override the existing index with the selected index.
5. Click **Close** to close the **MIB Walk** dialog box.

Duplicating a historical data collector

You can create a new data collector by duplicating an existing data collector, changing the name, and editing any values in the duplicate that you want to change.

1. Select **Monitor > Performance > Historical Data Collectors**.
2. Select the data collector you want to duplicate.
3. Click **Duplicate**.

   The Data Collector wizard is launched. The wizard is pre-populated with the data for the selected data collector. The **Name** field shows the name of the collector followed by the word copy. Go to any step to edit any of the values.
4. Click **Finish** on any of the wizard dialog boxes when you are done.

Duplicating system data collectors

Although you can duplicate a system collector, only the following target types will carry over to the duplicate collector:

- Individual products
- Individual ports
- User-defined port groups
- User-defined product groups
- System product groups

The following internal product group or port groups will carry over to the duplicated collector:

- FastIron/NetIron products
- Network OS products
- IP physical ports

Deleting a historical data collector

You can delete one or more data collectors from the **Historical Data Collectors** dialog box.

1. Select **Monitor > Performance > Historical Data Collectors**.
2. Select the data collector or data collectors you want to delete.
3. Click **Delete**.

   You are prompted to confirm the delete operation.
4. Click **Yes** to confirm.

NOTE
You cannot delete system data collectors.

Adding, editing, or duplicating a user-defined expression

You may want to create an expression to collect information in a specific way. For example, you may want the total count of all received and transmitted packets on an interface, requiring a value derived from two MIB objects; the MIB object for the incoming packet count and the MIB object for the outgoing packet count. Take the following steps to add a user-defined expression.

1. Select **Monitor > Performance > Expressions.**

   The **Expressions** dialog box displays.

2. Perform either of the following steps:
   - Click **Add**.

     The **Add Expressions** dialog box displays.

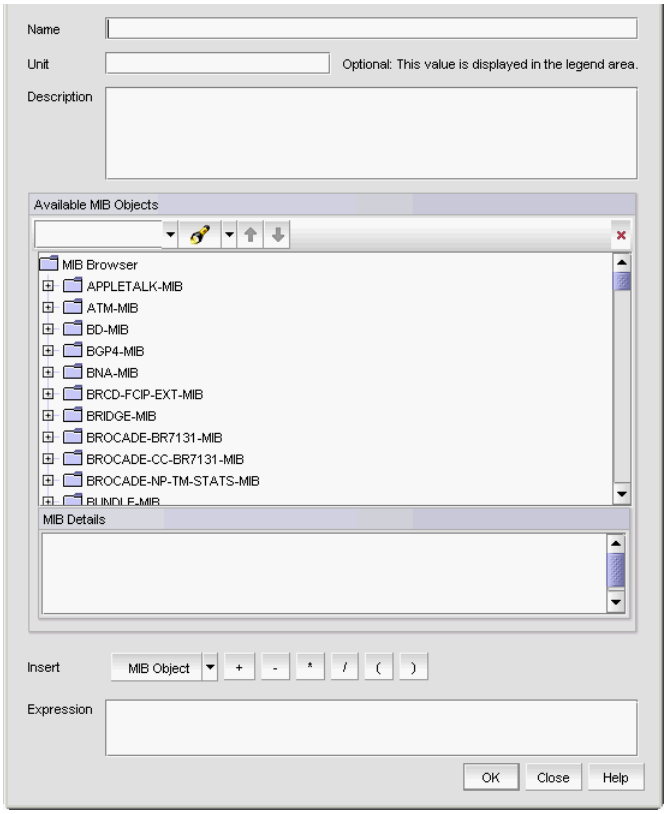


FIGURE 411 Add Expressions dialog box

- Select the expression you want to edit or duplicate from the **Expressions** list and click **Edit** or **Duplicate**.

  The **Edit Expression** or **Duplicate Expression** dialog box displays with the details for the selected expression. If you are duplicating an expression, the Management application appends *_copy* to the name of the expression.

3. Enter a name for the expression in the **Name** field.
4. (Optional) Enter text that you want to display in the legend area of the graph in the **Unit** field.
5. Enter a brief description in the **Description** field.
6. Select a MIB object from the **Available MIB Objects** tree structure.

   A description of the MIB object displays in the **MIB Details** field.
7. Build your expression in the **Expression** field using the operators above the field.
   - **MIB Object.Abs** — The raw value of the MIB variable that is polled from the product will be used in the SNMP expression calculation.

- **MIB Object.Delta** — Assuming the MIB value polled in the current polling period is M(T1) and the value polled in the previous polling period is M(T0), the MIB value to be used in the expression is calculated using M(T1)- M(T0).
- **MIB Object.Rate** — Assuming the MIB value polled in the current polling period is M(T1) and the value polled in the previous polling period is M(T0), the MIB value to be used in the expression is calculated using (M(T1)- M(T0))/ (T1 – T0) (T0 and T1 are measured in seconds).

The following example is the formula used to create the If%Errors expression, which calculates the error percentage for input packets on an interface.

(iFInErrors / (ifHCInUcastPkts + ifInMulitcastPkts + ifInBroadcastPkts)) * 100

8. Click **OK** to accept your changes.

Deleting an expression

Complete the following steps to delete an expression.

1. Select **Monitor > Performance > Expressions.**

   The **Expressions** dialog box displays.

2. Select the expression you want to delete from the **Expressions** list.
3. Click **Delete**.

   A confirmation dialog box displays.

4. Click **OK** to delete the expression.

Viewing Historical Graphs/Tables

1. Right-click a row in a performance monitor on the dashboard and select **Show Graph/Table**.

   OR

   Select **Monitor > Performance > Historical Graphs/Tables**.

   The **Historical Graphs/Tables** dialog box displays.

2. Select the **Data Monitoring** tab.

   The main features are a tree structure and a graph area. You can collapse the tree structure to expand the graph area.

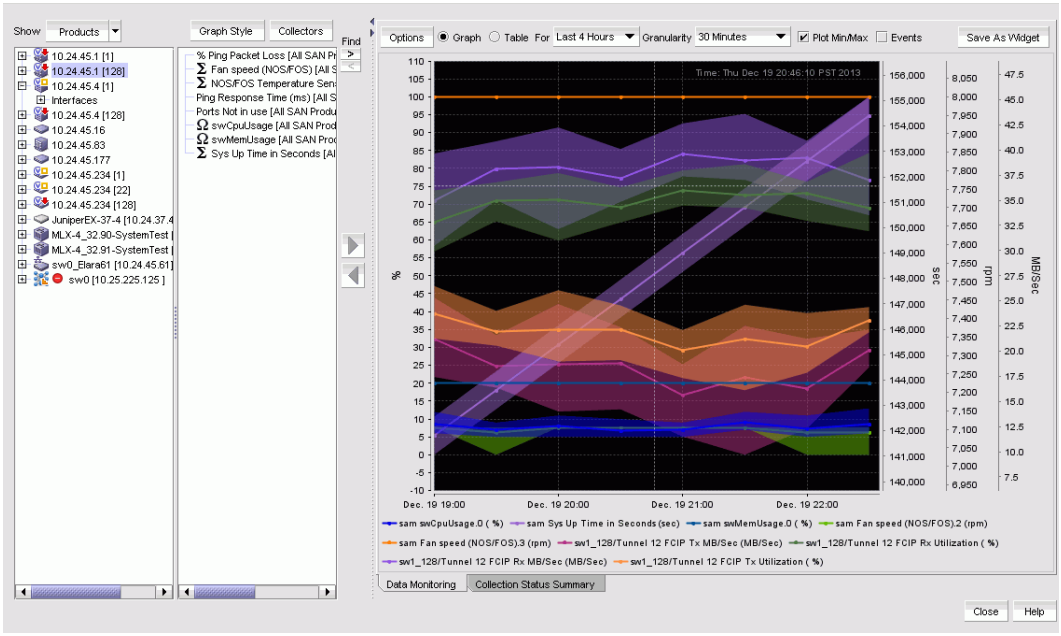


FIGURE 412 Historical Graphs/Tables Data Monitoring tab

3. Use the **Show** selector to toggle the tree structure display in the left panel between **Products** and **Collectibles**.

   - Select **Products** and the left panel displays the tree structure of devices and device interfaces on the network being polled for collectible data. The right panel displays measures currently being collected for the selected product or port in the left panel.

     In addition, measures collected for attached wireless access point (AP) devices and controllers display. Refer to Figure 415 on page 1010 for an example.

     Measures also displays for IP products that appear in the device tree. Refer to Figure 414 for NetIron devices.

FIGURE 413

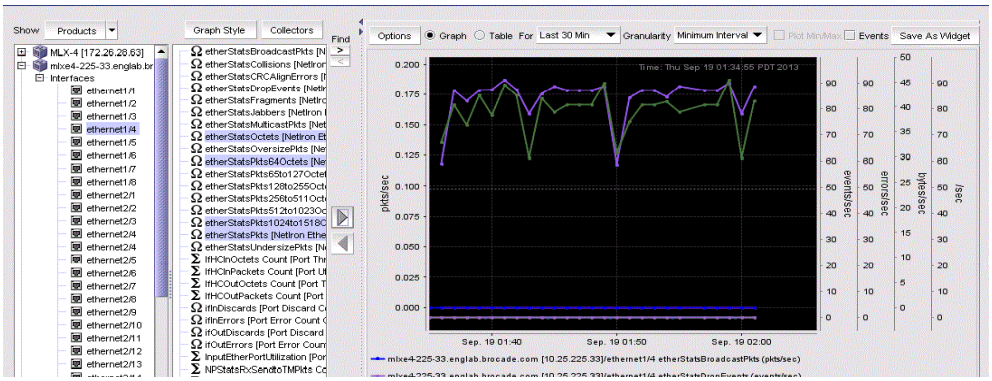


FIGURE 414 NetIron Historical Graph display

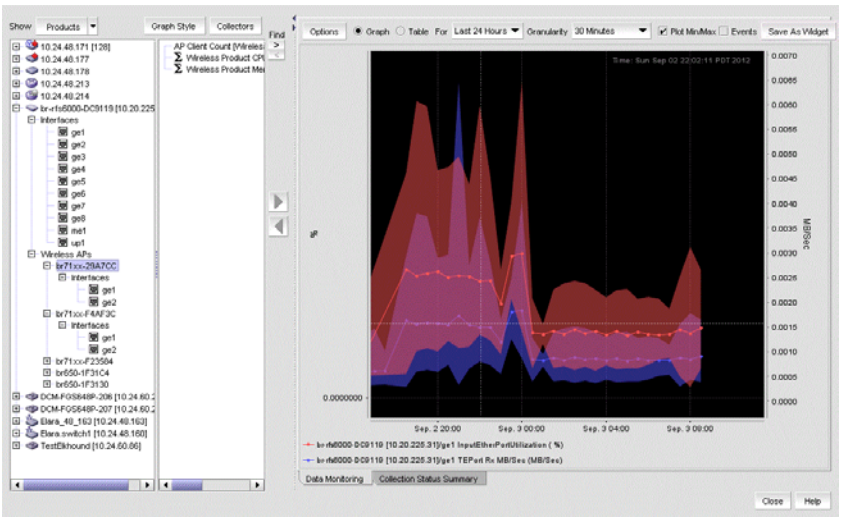


FIGURE 415 Wireless access point devices and controllers display

- Select **Collectibles** and the left panel displays measures (MIB objects and expressions) currently being collected. Select a measure, and the targets (products or ports) from which the measure was collected display in the right panel. If SAN historical data collection is enabled, corresponding SAN products and ports display.

  Measures also display for SAN products, ports, and FCIP tunnels that appear in the device tree. In addition, measures collected for attached wireless access point (AP) devices and controllers display. You can select these collectibles to create applicable historical graphs and tables.

4. Select **Collectors** to open the **Historical Data Collectors** dialog box. Use this dialog box to display, enable or disable, add or delete, and duplicate historical data collectors. Refer to the following sections for instructions:

- "Displaying historical data collectors" on page 996
- "Enabling a historical data collector" on page 998
- "Adding or editing a historical data collector" on page 998

5. Optional: To configure the look and feel of the performance graph from the **Historical Graphs/Tables** dialog box, refer to "Configuring the performance graph" on page 989.

6. Optional:Once data collection begins, the data is presented on the chart (if **Graph** is selected) or table (if **Table** is selected).

   If a graph is displayed, the legend under the graph shows what data each color represents. Also, you see the following text:

   - *MIB*: Shows the name of the MIB object that is being used to collect the data and the device that is being polled. If the target is a port, then the interface ID is also displayed.
   - *EXP*: Shows the name of the expression being used to collect the data and the device that is being polled. If the target is a port, then the interface ID is also displayed.

   Each collectible is represented by a different color and the color for a collectible can change as new data is collected.

   If a table is displayed, the first column displays the time of the collection. The remaining columns display the value of each collectible at the specified time. There is one column for every collectible you select to display.

7. Optional: To add the performance monitor published widget to the active dashboard, click **Save As Widget**.

   The **Performance Dashboard Monitor Title** dialog box displays.

   Select **Add the Widget to active dashboard (Product status and Traffic)** check box to enable the published widget. By default, the check box is enabled.

   Click **OK.**

8. Select the **Collection Status Summary** tab.

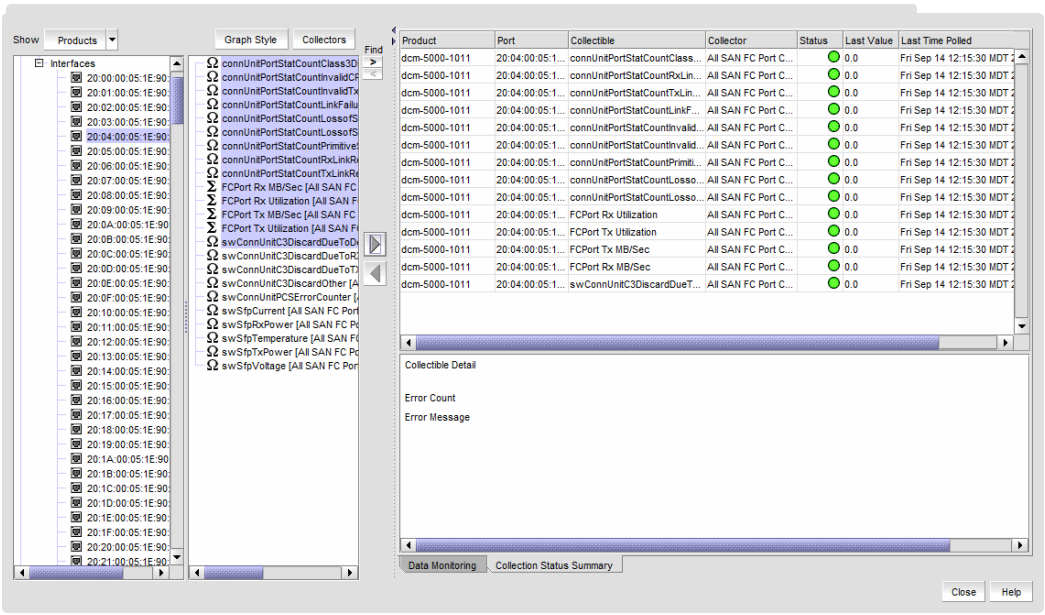


FIGURE 416 Historical Graphs/Tables Collection Status Summary tab

The **Collection Status Summary** tab provides a high-level overview of all defined collectors. The information is displayed in the following columns:

- **Product** - Shows the product name. There maybe multiple instances of the product name for each collectible assigned to the product.

- **Port** - The port name when a port is selected.
- **Collectible** - The MIB objects and expressions used by the data collector. When you select a collectible row, collectible information displays in the bottom portion of the panel, such as errors, error count, and messages.
- **Collector** - The data collector name.
- **Status** - The status field uses the following icons:.


Failed. No value was ever collected for this collectible.


Warning: Data collection failed in the last polling cycle.


Successful: Last collection successful.


Scheduled but not currently active.

- **Last Value** - The last (most current) value collected.
- **Last Time Polled** - The time that the collector was last polled.

When you use the **Show** selector to select **Products**, devices and ports display in a tree structure in the left-most column. If you select a device or port, the right collectibles column lists all the collectors that have been defined for the device or port.

If you use the **Show** selector to select **Collectible**, the left-most column shows all the collectibles (MIB objects or SNMP expressions) currently being collected. Select a collectible to display a tree structure in the right column of all products and ports from which the expression or MIB object are to be collected.

When a specific collectible is selected, collectible detail, error count, and error messages display in an area below the table.

Mouse functions for graphs

The following mouse functions can be used for graphs:

- Zoom: Use the mouse wheel to zoom in or zoom out of a graph.
- Graph panning: Hold down the left mouse button and move the mouse left and right to pan through the graph.
- Selective zooming: Select an area that you want to zoom by holding down the right mouse button at one edge of the area, then drag the mouse to the left or right to the other edge of the area. The area you selected changes color. Release the right mouse button to zoom the selected area.
- Highlighting: Place the mouse over a data point. Information about that data point appears in a tooltip-like format.
- Drag and drop from trees: If you want to monitor additional devices on the same graph, select the device from the device tree, then drag and drop it into the graph. You can monitor up to twenty entries in one graph. If you drag and drop a device node, all MIB variables and expressions collected from that device are included.

MIB data collectors

The Management application enables you to define a data collector by mapping a MIB object to a unit name in the mib_unit.properties file. This property file is located in the Install_Home/conf/mibs directory. The default mib_unit.properties file contains commonly used MIB unit definitions.

Once mapped, the unit name displays on the line chart of the performance graphs when you select that MIB object as a data collector.

You can map a unit name from either a MIB name or MIB object identifier (OID).

Example

```
#MIB OID mapping
1.3.6.1.2.1.31.1.1.1.6 = Octects
#MIB name mapping
ifHCInOctets=Octects
```

Mapping a MIB object to a unit name

To map a MIB name or OID to a unit name, complete the following steps.

1. Open the `mib_unit.properties` file in a text editor.

   The mib_unit.properties file is located in the Install_Home/conf/mibs directory.

2. To map a MIB OID, use the following format:

   ```
   1.3.6.1.2.1.31.1.1.1.6 = Octects
   ```

3. To map a MIB name, use the following format:

   ```
   ifHCInOctets=Octects
   ```

4. Save and close the file.

   You can then annotate the performance graphs using the unit name by assigning the MIB object as a data collector. For counter values, the unit name is appended with “/sec” to indicate the rate information for that counter value.

   If you define a data collector with a MIB object that does not have an associated unit name, the unit name displays as an empty string on the performance graph.

IP Custom performance reports

You can create customized reports and run or schedule them in the same manner as a standard report.

You can modify, copy, or delete customized reports. Select the report from the **Report Definitions** tab, then click the **Edit, Duplicate**, or **Delete** button.

Related topics

"IP performance monitoring and traffic analysis"

"IP real-time performance monitoring"

"IP historical performance monitoring"

"IP Custom performance reports"

"IP Custom performance reports"

"IP sFlow configuration"

"IP Traffic analyzer monitoring and sFlow reports"

"IP traffic accounting"

Creating a custom report

Complete the following steps to create a report.

1. Select **Monitor > Performance > Custom Reports**.

   The **Performance Custom Reports** dialog box displays, as shown in Figure 417 on page 1014.

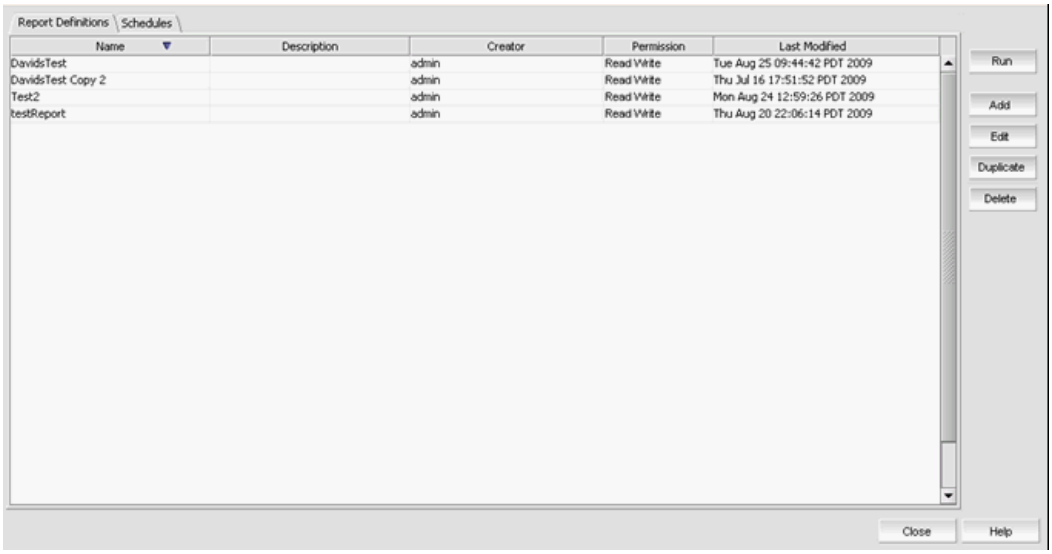


FIGURE 417 Performance Custom Reports dialog box

2. Perform one of the following steps:

   - Click **Add** to add a new report.

- Select an existing report from the **Performance Custom Reports** dialog box and click **Edit** to edit the report.
- Select an existing report from the **Performance Custom Reports** dialog box and click **Duplicate** to duplicate the report.
- Select an existing report from the **Performance Custom Reports** dialog box and click **Delete** to delete the report.

If you select **Add**, **Edit**, or **Duplicate**, the **Add/Edit/Duplicate Report Definition** dialog box displays, as shown in Figure 418 on page 1015. If you are editing or duplicating an existing report, fields are already populated. Simply make changes as required.

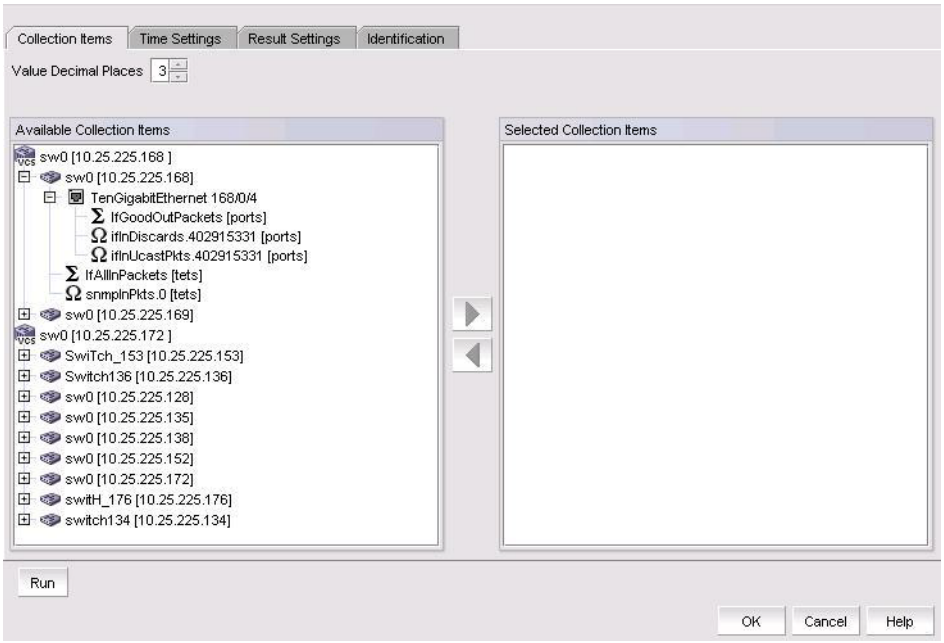


FIGURE 418 Add/Edit /Duplicate Report Definition dialog box - Collection Items tab

By default, the **Collection Items** tab is selected. On this tab, the collectibles in all data collector configurations are listed by device in the **Available Collection Items** list.

3. Select the collectible you want to include in the report and click the right arrow button to move it to the **Selected Collection Items** list. To move a collectible back to the **Available Collection Items** list, select it and click the left arrow button.
4. Select the decimal places for displaying values. From 1 to 3 places are available.

5. To schedule the report to run at a specific time, click the **Time Settings** tab.

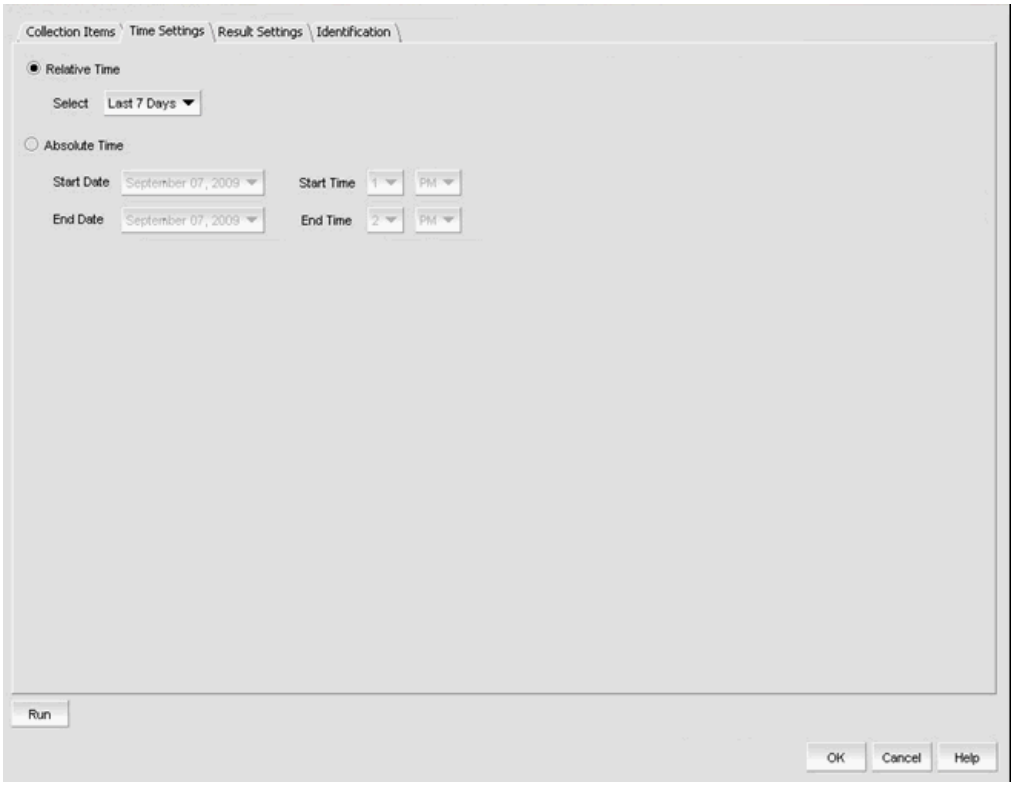


FIGURE 419 Add/Edit Report Definition dialog box - Time Settings tab

You can choose from the following settings:

- **Relative Time** - Enables you to select a time range relative to the present for the display of historical data. The choices are incremental from the last 30 minutes to the last 24 hours.
- **Absolute Time** - Enables you to get a snapshot of data from a specific time range, as specified by the **Start Date**, **Start Time**, **End Date**, and **End Time** parameters.

Data collected for the report comes from data sampled at different granularities depending on your time setting as shown in Table 89.

TABLE 89 Granularity of data collected for time settings

Time Settings	Sampling Granularity
Less than or equal to 12 hours	Real-time or “raw”
Less than or equal to 1 week	30 minutes
Less than or equal to 30 days	2 hours
Up to 2 years	1 day

6. To arrange the order of the columns in the generated report, click the **Result Settings** tab.

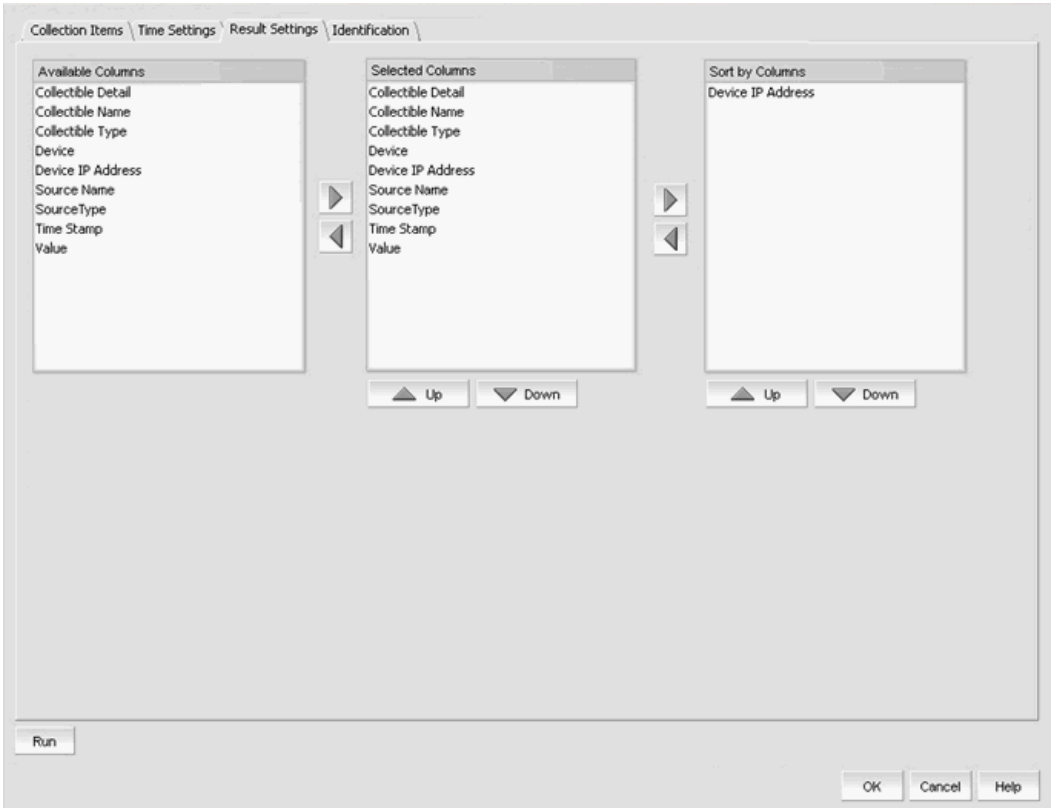


FIGURE 420 Add/Edit Report Definition dialog box - Result Settings tab

- Data types that will be collected are listed in the **Available Columns** list. Select the data type you want to include in the report and click the right arrow button to move it to the **Selected Columns** box.
- Select a data type to be used to sort the report. Select that data type from the **Selected Columns** list and click the right arrow button to move it to the **Sort by Columns** list. Click the left arrow button to move a data type back to the **Selected Columns** list. You can select more than one column. If more than one column is selected, the report will be sorted according to the sequence of the data types in the **Sort by Columns** list.
- Use the up and down arrows to move attributes up and down in the columns.

7. Click the **Identification** tab.

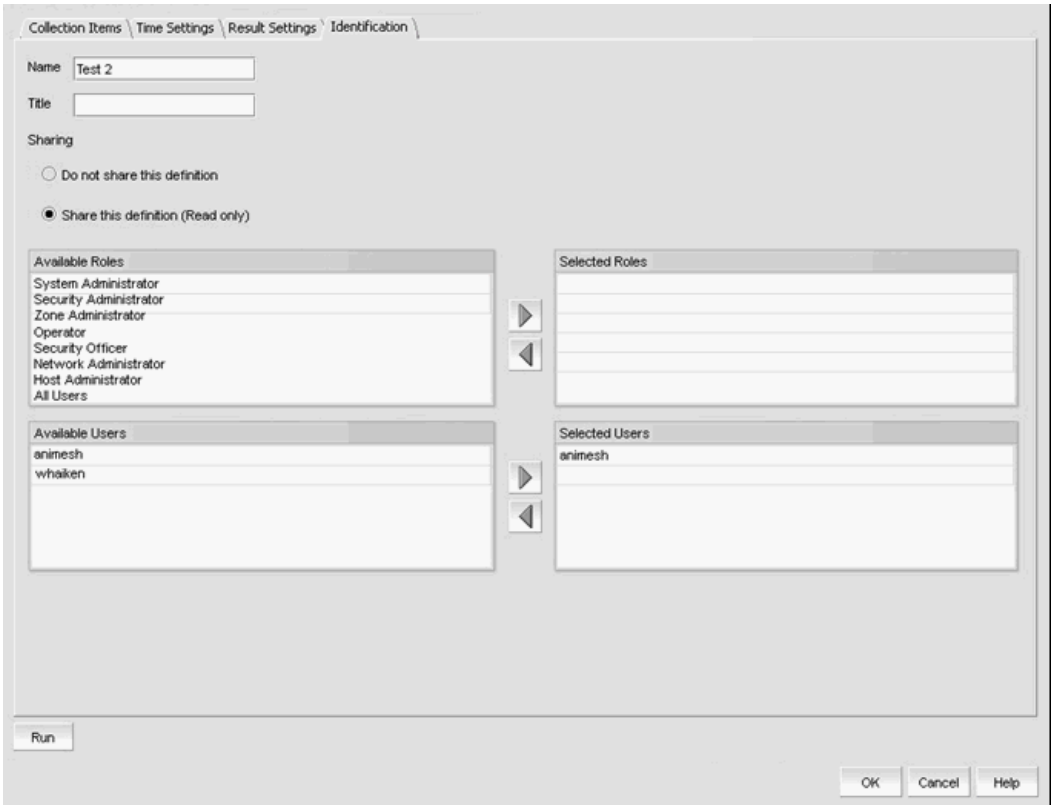


FIGURE 421 Add/Edit Report Definition dialog box - Identification tab

8. Enter a name for the report in the **Name** field. You can use up to 64 alphanumeric characters.

   This name appears under the **Name** column on the **SNMP Monitor** reports tree. This name must be unique for each **SNMP Monitor** report.

9. Enter a title for the report, which will be used as the title of a generated report, in the **Title** field. You can use up to 128 alphanumeric characters.

10. Select one of the following options:

    - Select the **Do not share this definition** option if you do not want to share this definition with other Management application users. Go to step 12.

      If this option is selected, Management application users will not see this definition on the **Report Definitions** table when they log in.

    - Select the **Share this definition (read only)** option if you want other Management application users to have read-only permission for this definition. Continue with step 10.

11. Select the roles that will have view and run access to this definition in the **Available Roles** list and click the right arrow button to move those roles into the **Selected Roles** list.

    If you selected the **Share this definition (read only)** option, a list of Management application roles appears in this list. All Management application users who have the selected roles will be able to view, copy, and run the definition.

12. Select the user accounts that will be able to view and run this definition in the Available Users list and click the right arrow button to move those user accounts into the **Selected Roles** box. Click the left arrow button to move the user accounts back to the **Available Users** list.

    You can share this definition with specific Management application users. If you selected the **Share this definition (read only)** option, a list of Management application user accounts appears in this list.

13. Choose one of the following options:

    - To save your entries, click **OK**.
    - To run the report immediately, click **Run**.

      The Management application generates the HTML report first, then generates a CSV file. The HTML report launches in a browser immediately after the report is complete. Click **Abort** to stop the report generation.

Interpreting the SNMP Monitor report

An **SNMP Monitor** report displays the information such as the following:

- Report title - Title of the report as defined in the **SNMP Monitor** report definition.
- Day, date and time - Time range when data was collected.
- Graph - Graph of the collection activity.
- Legend - Legend to help interpret the data on the graph. Each collectible is indicated by a different color.
- Details table - Details for each collectible included in the report.
- Records Per Page - The number of records displayed on each page of the report is controlled at the bottom of the reports page. You can select the number of records from the drop-down list.

Exporting an SNMP Monitor report

To export an SNMP Monitor report to a .csv file, press the **Export** button on the report and save the displayed report to a .csv file.

IP sFlow configuration

The Management application supports the creation of sFlow reports to capture traffic data.

Configuring sFlow

You can use the sFlow configuration wizard to configure an sFlow data collector and a destination for the sFlow data collector.

1. Select **Monitor > Traffic Analysis > Configure sFlow**.

   The **Interface Payload - sFlow Configuration** dialog box displays.

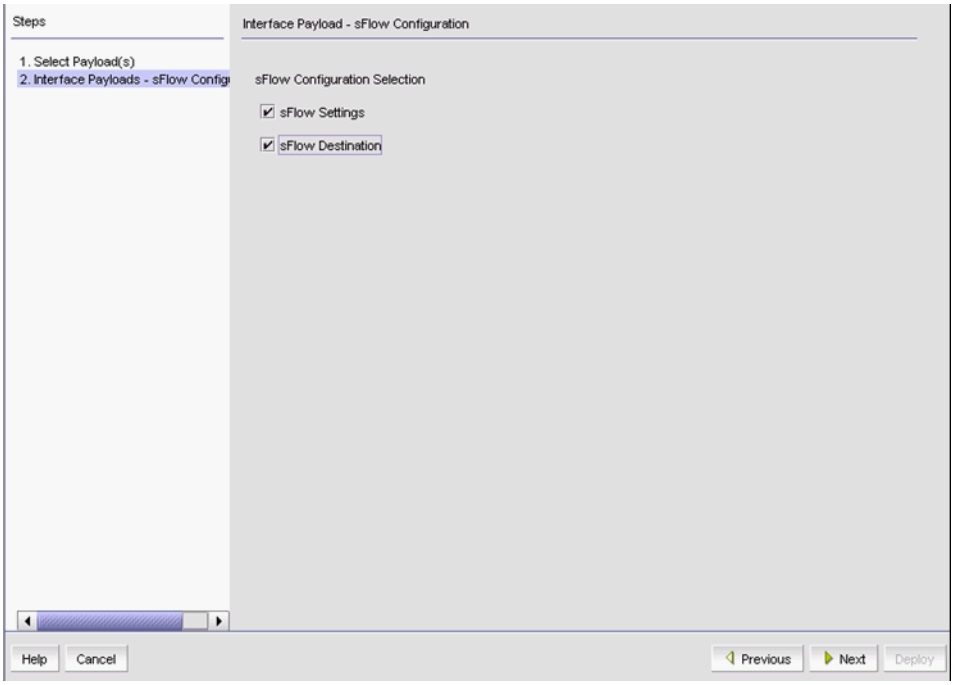


FIGURE 422 Interface Payload - sFlow Configuration dialog box

Under **SFlow Configuration Selection**, there are two check boxes:

- **sFlow Settings** - Allows you to enable or disable sFlow, and allows you to configure traffic sampling rates.
- **sFlow Destination** - Allows you to add or delete sFlow collector entries in the device.

Select both if you are adding an sFlow data collector. If you are enabling or disabling sFlow of modifying traffic sampling rates, you may select only **sFlow Settings**.

2. Click **Next**.

   The **Interface Payload - sFlow Settings** dialog box displays.

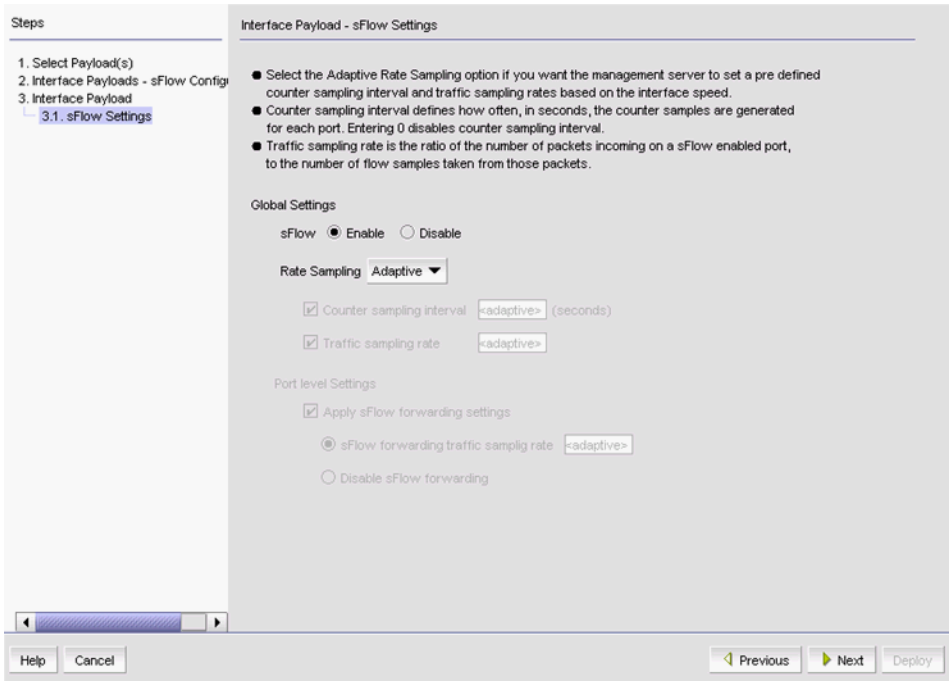


FIGURE 423 Interface Payload - sFlow Settings dialog box

3. Under Global Settings, select **Enable** to have the sFlow report enabled when it is deployed. Select **Disable** to deploy the sFlow report as initially disabled.
4. Use the **Rate Sampling** selector to choose either **Adaptive** or **Custom** sampling.

   If you choose **Adaptive**, the management server selects the sampling interval and traffic sampling rate. The sampling rate is the ratio between the total number of incoming packets and the number of flow samples taken at the product level. When **Adaptive** is chosen, the sampling rate is based on interface speeds as shown in Table 90 on page 1021.

TABLE 90 Interface Payload

Interface Speed	Sampling rate
10 Mbps	256
100 Mbps	512
1 Gbps	1024
10 Gbps	2048
100 Gbps	8192

If you choose **Custom**, you may set your own sampling interval and traffic sampling rate.

- Global Settings
  - **Counter sampling interval** - defines the interval in seconds between samples. For Ironware devices, the range is 0 to 86400. For Network OS devices, the range is 1 to 65535.
  - **Traffic sampling rate** - the ratio between the total number of incoming packets and the number of flow samples taken at the product level. The ratio is expressed as n to 1; for example, if you specify a sampling rate of 100, the ratio is 100:1. The lower the ratio, the higher the demand on CPU resources to process the samples. For Ironware devices, the range is 1 through 1048576. For Network OS devices, the range is 2 to 16777215.
- Port Level Settings
  - **Apply sFlow forwarding settings** - This check box is used to enable traffic sampling at the port level using the rate value specified in the **sFlow forwarding sampling rate** field.
  - **sFlow forwarding sampling rate** - the ratio between the total number of incoming packets and the number of flow samples taken at the port level. The ratio is expressed as n to 1; for example, if you specify a sampling rate of 100, the ratio is 100:1. The lower the ratio, the higher the demand on CPU resources to process the samples.
  - **Disable sFlow forwarding** - disables port level sampling.

5. Click **Next**.

   The **Product Payload - Select Action** dialog box displays.

   There are four possible actions to take:

   - Select **Add** to add entries to the target products.
   - Select **Delete** to remove matching entries to the target products.
   - Select **Replace All** to replace all existing entries to the target products.
   - Select **Clear All** to clear all existing entries from the target products.

   The **Product Payload - SFlow Destination** dialog box displays.

6. Click **Next**.

   The **Product Payload - sFlow Destination** dialog box displays.

7. Click **Add** to add collector details and complete the following steps.

   a. Use the **IP Address** selector to select an IP address from the existing list of IP addresses of management server NICs, or enter a new IP address in the field. IPv4 and IPv6 addresses are allowed. IPv6 addresses are not supported for Network OS previous to v4.0 and Fabric OS previous to v7.2.

   b. Enter the port number in the **UDP Port** field for the UDP port used to forward sFlow samples to the collector.

   NOTE
   VCS devices use the default port 6343. If you change the VCS device default port number, all sflow configuration are deployed to the device except the port number. The 6343 port number cannot be changed.

   c. Click **OK**.

A new row appears under **Collector Details** for the collector you just added.

NOTE
A limit of four collectors is enforced in the **Collector Details** table. If you add more than four collectors, an error message displays. An error message also displays if you try to add a collector with the same IP address and UDP port combination as an existing collector.

NOTE
For VCS devices running Network OS v4.0 and above, you can deploy up to five collectors. If you add more than five collectors, an error message displays. For versions prior to v4.0, you can deploy only one collector.

8. Click **Next**.

   The **Deployment Targets** dialog box displays.

9. Select the product or port to which you want to deploy this collector and click the right arrow to move under the **Selected Targets** column.

10. **Click Next**.

    The **Deployment Properties** dialog box displays.

11. Select one of the following options to set the **Persistence Properties**:

    - **Do not Save to Flash or Reload** — Use this option if you want to update the running configuration. The payload configuration is not saved to the device flash memory, nor is the device rebooted when the payload configuration is deployed.
    - **Save to Flash** — Use this option if you want to make the payload configuration permanent in the device flash memory and saved to the running configuration. This is equivalent to entering a write memory command. The payload configuration is applied to the device when the device reboots.
    - **Save to Flash and Reload** — Use this option if you want to save the payload configuration to the device flash memory and reboot the device. This is equivalent to entering the write memory and reload commands. The availability of this option depends on your user privileges.

12. Select one of the following check box to set the **Pre-Post Snapshot Properties**:

    - To run and save a report before this configuration is deployed to the product, select the **Pre-deployment** check box and select a CLI template from the list.
    - To run and save a report after this configuration is deployed to the product, select the **Post-deployment** check box, select a CLI template from the list, and select the post deployment delay.

13. Select one of the following options to determine if you want to save the payload configuration.

    - To schedule a one-time deployment, select **One time deployment, do not save configuration**.
    - To save the configuration for future deployment, select **Save configuration** and enter a configuration name and description.

14. Click **Next**.

    The **Summary Page** dialog box displays.

15. Review the configuration summary and click **Deploy**.

Creating custom sFlow reports

You may create custom sFlow reports if you want to capture traffic analysis information that is not available in the standard reports.

1. Select **Monitor > Traffic Analysis > Custom Reports**.

   The **Traffic Analyzer Custom Reports** dialog box displays.

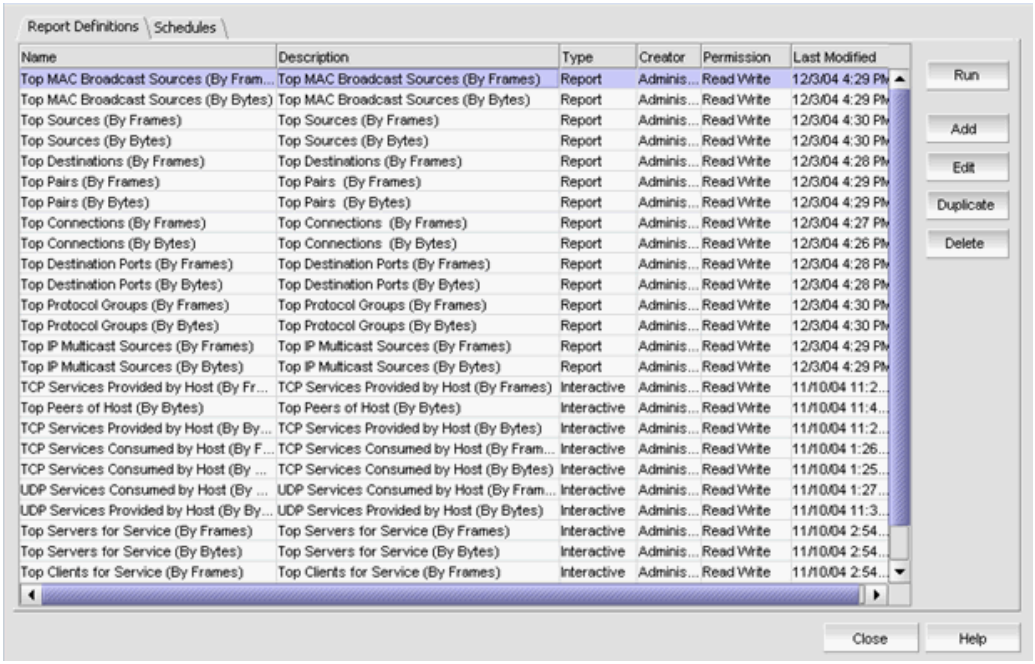


FIGURE 424 Traffic Analyzer Custom Reports dialog box, Definition tab

2. Select the **Report Definitions** tab.
3. Click the **Add** button.

   The **Add Report Definitions** dialog box displays.

4. Select the **Product & Port** tab.

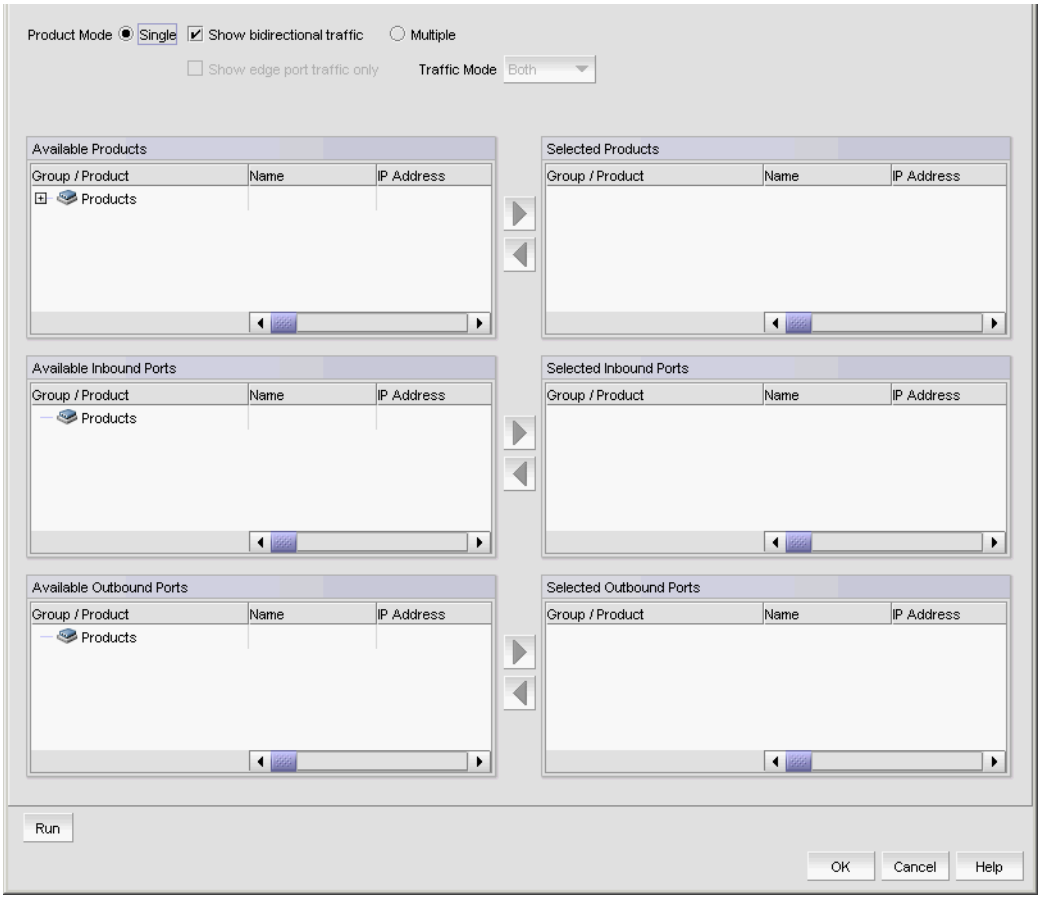


FIGURE 425 Add Report Definitions dialog box, Product & Port tab

The **Product & Port** tab contains tables of available products and ports that may be selected for sFlow data collection.

5. Determine if you want a report on only one product or port or on two or more products or ports, and select either **Single** or **Multiple** as appropriate.

   Options are displayed differently depending on your choice of **Single** or **Multiple**. If you chose **Single**, complete the following steps.

   - To monitor both inbound and outbound traffic, select **Show bidirectional flow**.
   - To monitor edge port traffic, select **Show edge port traffic**. Only available when you move a VCS fabric to the **Selected Products** list
   - Select products and ports from **Available Products**, **Available Inbound Ports**, and **Available Outbound Ports** and move them to **Selected Products**, **Selected Inbound Ports**, and **Selected Outbound Ports** using the right arrow.

For VCS fabrics, if you select **Single** mode, the following report definition behavior may occur:

- Displays all ports from all members of the selected VCS fabric in the available ports tables on the **Product & Port** tab.
- Automatically includes fabric changes (adding or deleting members) when you run the report.
- Generates an application event and displays a warning message for the following issues when you edit or run a report:
  - If the selected fabric is deleted for any reason (such as, seed switch changed to standalone VDX or merging with another fabric).
  - If the selected fabric port is deleted for any reason (such as, member leaving the fabric).
  - If the selected standalone VDX is added to a fabric for any reason (VDX device forming a node fabric or joining a fabric).

If you chose **Multiple**, complete the following steps:

- Use the **Traffic Mode** selector to choose **Inbound**, **Outbound**, or **Both** as the traffic direction.
- Select products and ports from **Available Products/Ports**, and move them to **Selected Products/Ports**, using the right arrow.

For VCS fabrics, if you select **Multiple** mode, the selected device remains in the report definition regardless of any changes to the fabric or mode.

6. Select the **VM** tab.

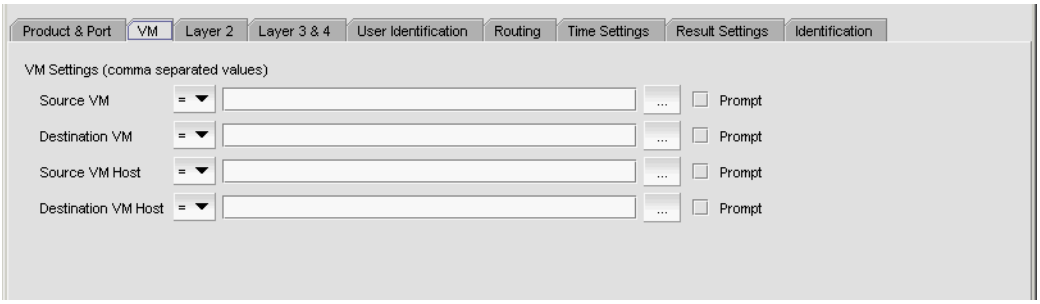


FIGURE 426 Add Report Definition dialog box, VM tab

7. Examine each listed item and decide the following:
   - Do you want to enter values in the field, or be prompted to enter the value when running the report? If you want to be prompted, select the **Prompt** check box. Go to step 9.
   - If you choose to list values in the field, would you rather include or exclude the listed values? The selector next to the field may be used to include (**=**) or exclude (**!=**) the values. Go to step 9.
   - Are the values relevant to the design of your report? If not, leave the fields blank. Continue with step 8.

8. If you do not chose the **Prompt** check box, complete the following for each field.
   - **Source VM** — Enter the name, IP address, or MAC address of the source VMs in comma separated value (CSV) format or click the ellipsis button to the right of the field to select the VMs from the **Select VMs** dialog box.
   - **Destination VM** — Enter the name, IP address, or MAC address of the destination VMs in comma separated value (CSV) format or click the ellipsis button to the right of the field to select the VMs from the **Select VMs** dialog box.
   - **Source VM Host** — Enter the name or IP address of the source VM hosts in comma separated value (CSV) format or click the ellipsis button to the right of the field to select the VM hosts from the **Select VM Hosts** dialog box.
   - **Destination VM Host** — Enter the name or IP address of the destination VM hosts in comma separated value (CSV) format or click the ellipsis button to the right of the field to select the VM hosts from the **Select VM Hosts** dialog box.
9. Select the **Layer 2** tab.

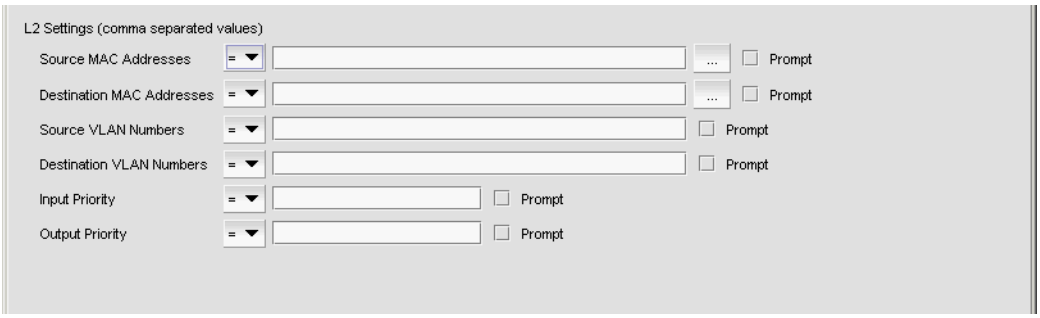


FIGURE 427 Add Report Definitions dialog box, Layer 2 tab

10. Examine each listed item and decide the following:
    - Do you want to enter values in the field, or be prompted to enter the value when running the report? If you want to be prompted, select the **Prompt** check box.
    - If you choose to list values in the field, would you rather include or exclude the listed values? The selector next to the field may be used to include (**=**) or exclude (**!=**) the values.
    - Are the values relevant to the design of your report? If not, leave the fields blank.
11. If you do not chose the **Prompt** check box, complete the following for each field.
    - **Source MAC Address** — Enter the source MAC addresses in comma separated value (CSV) format or click the ellipsis button to the right of the field to select the MAC addresses from the **Source MAC Address Selector** dialog box.
    - **Destination MAC Addresses** — Enter the destination MAC addresses in comma separated value (CSV) format or click the ellipsis button to the right of the field to select the MAC addresses from the **Destination MAC Address Selector** dialog box.
    - **Source VLAN Numbers** — Enter the source VLAN numbers in comma separated value (CSV) format.
    - **Destination VLAN Numbers** — Enter the destination VLAN numbers in comma separated value (CSV) format.
    - **Input Priority** (QoS priorities for inbound traffic) — Enter the input priority (0 - 7).
    - **Output Priority** (QoS priorities for outbound traffic) — Enter the output priority (0 - 7).

12. Select the **Layer 3 & 4** tab.

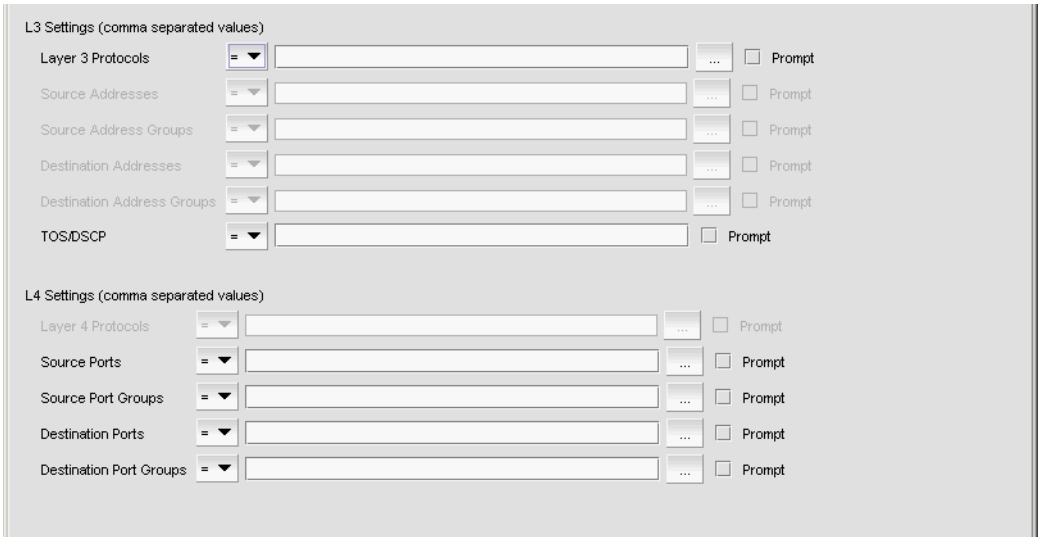


FIGURE 428 Add Report Definitions dialog box, Layer 3 & 4 tab

13. Examine each listed item and decide the following:
    - Do you want to enter values in the field, or be prompted to enter the value when running the report? If you want to be prompted, select the **Prompt** check box.
    - If you choose to list values in the field, would you rather include or exclude the listed values? The selector next to the field may be used to include (**=**) or exclude (**!=**) the values.
    - Are the values relevant to the design of your report? If not, leave the fields blank.

14. If you do not chose the **Prompt** check box, you may enter any of the following in comma separated value (CSV) format in the fields provided:
    - **Layer 3 Protocols** — Enter the L3 protocols in comma separated value (CSV) format or click the ellipsis button to the right of the field to select the protocols from the **Layer 3 Protocols** dialog box.
    - **Source Addresses** — Enter the addresses in comma separated value (CSV) format or click the ellipsis button to the right of the field to select the addresses from the **L3 Source Addresses** dialog box.
    - **Source Address Groups** — Enter the addresses in comma separated value (CSV) format or click the ellipsis button to the right of the field to select the addresses from the **L3 Source Address Groups** dialog box.
    - **Destination Addresses** — Enter the addresses in comma separated value (CSV) format or click the ellipsis button to the right of the field to select the addresses from the **L3 Source Addresses** dialog box.
    - **Destination Address Groups** — Enter the addresses in comma separated value (CSV) format or click the ellipsis button to the right of the field to select the addresses from the **L3 Source Address Groups** dialog box.
    - **TOS/DSCP values** — Enter one or more TOS or DSCP value (0-255).
    - **Layer 4 Protocols** — The layer 4 protocols you can use as a filter depends on which layer 3 protocols you selected. Enter the L4 protocols in comma separated value (CSV) format or click the ellipsis button to the right of the field to select the protocols from the **Layer 4 Protocols** dialog box.
    - **Source Ports** — Enter the ports in comma separated value (CSV) format or click the ellipsis button to the right of the field to select the ports from the **L4 Source Port** dialog box.
    - **Source Port Groups** — Enter the port groups in comma separated value (CSV) format or click the ellipsis button to the right of the field to select the port groups from the **L4 Source Port Groups** dialog box.
    - **Destination Ports** — Enter the ports in comma separated value (CSV) format or click the ellipsis button to the right of the field to select the ports from the **L4 Source Port** dialog box.
    - **Destination Port Groups** — Enter the port groups in comma separated value (CSV) format or click the ellipsis button to the right of the field to select the port groups from the **L4 Source Port Groups** dialog box.
15. Select the **User Identification** tab.

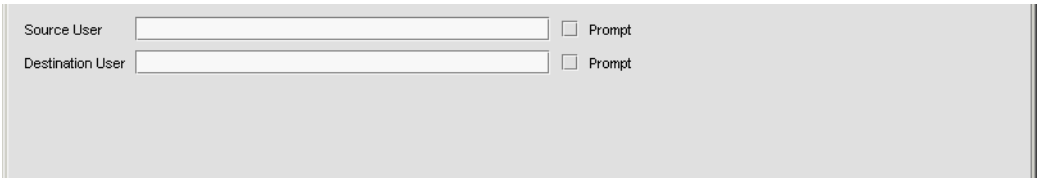


FIGURE 429 Add Report Definitions dialog box, User Identification tab

16. Decide if you want to enter the user names in the fields provided, or if you want to be prompted for the user names.
    - If you want to be prompted, select the **Prompt** check box. This disables the field.
    - If you do not want to be prompted, enter the name of the user that is sending the traffic in the **Source User** field, and enter the name of the user that is receiving the traffic in the **Destination User** field.
17. Select the **Routing** tab.

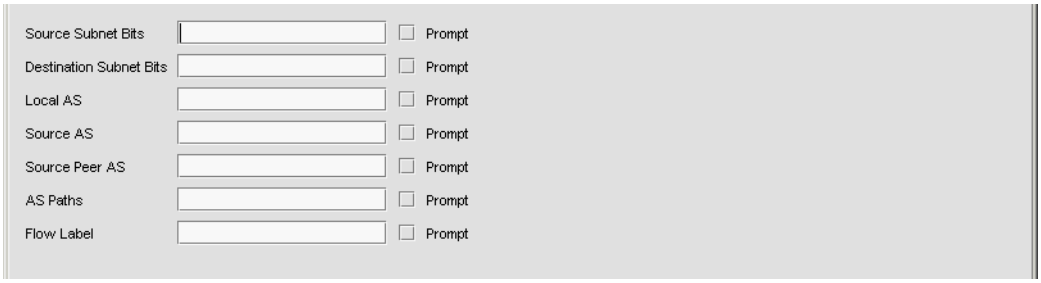


FIGURE 430 Add Report Definitions dialog box, Routing tab

18. Examine each listed item and decide the following:

    Do you want to enter values in the field, or be prompted to enter the value when running the report? If you want to be prompted, select the **Prompt** check box.

    If you do not chose the **Prompt** check box, you may enter any of the following in the fields provided:
    - **Source Subnet Bits** - Enter the source subnet of the route.
    - **Destination Subnet Bits** - Enter the destination subnet of the route.
    - **Local AS** - Enter the local AS number.
    - **Source AS** - Enter the destination AS number.
    - **Source Peer AS** -Enter a source peer AS number.
    - **AS Paths** - Enter an AS path number.
    - **Flow Label** - Enter a flow label.
19. Select the **Time Settings** tab.

FIGURE 431 Add Report Definitions dialog box, Time Settings tab

20. Select **Relative time** if the you want to retrieve information relative to a time range, or **Absolute time** if you want to run the report at a specific date and hour.
    - If you select **Relative** time, use the **Range** selector to
    - If you select **Absolute** time, use the **Start Date** and **Start Time** selectors to set the time that data collection begins, and the **End Date** and **End Time** selectors to set the time when data collection ends.
21. Select the **Result Settings** tab.

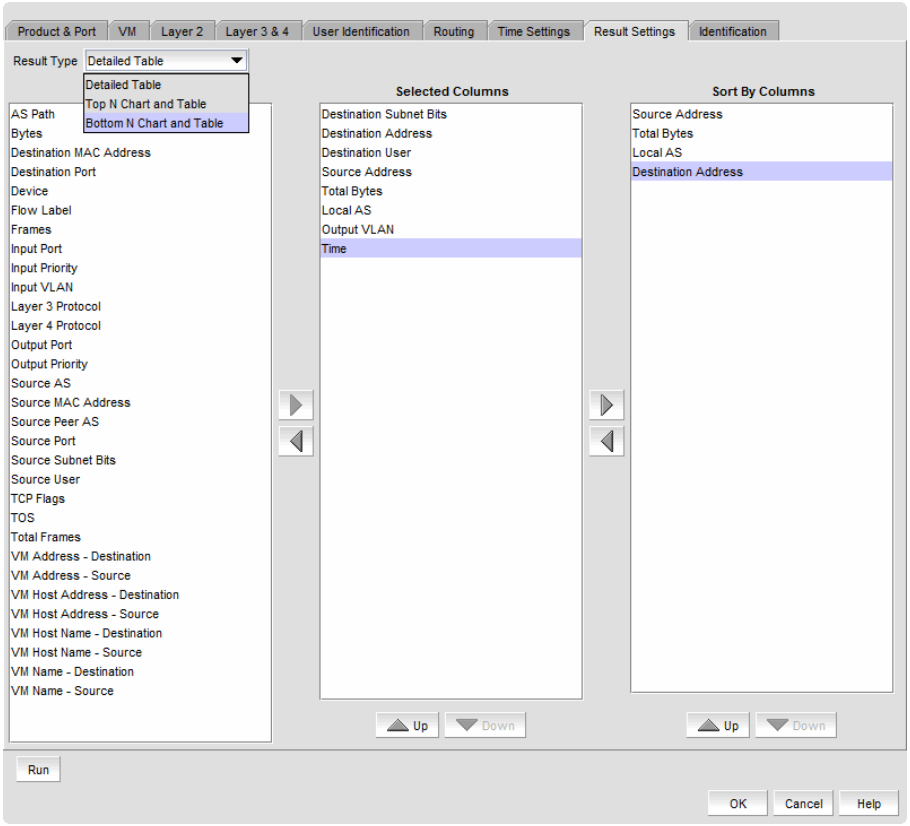


FIGURE 432 Add Report Definitions dialog box, Result Settings tab

22. Select one of the following options for displaying report data from **Result Type** list:
    - **Detailed Table** - Displays data in table format.
    - **Top N Chart and Table** - Displays a pie chart of the top N talkers for your selected sorting options above tabular data.
    - **Bottom N Chart and Table** - Displays a pie chart of the bottom N talkers above the tabular data.

    For the **Bottom N Chart and Table** and **Top N Chart and Table** selections, Total Bytes is automatically selected under Selected Columns if Total Bytes or Total Frames is not already selected. The Time column cannot be selected and the **Sort By Columns** box is not displayed in the dialog box (refer to Figure 433 on page 1032).

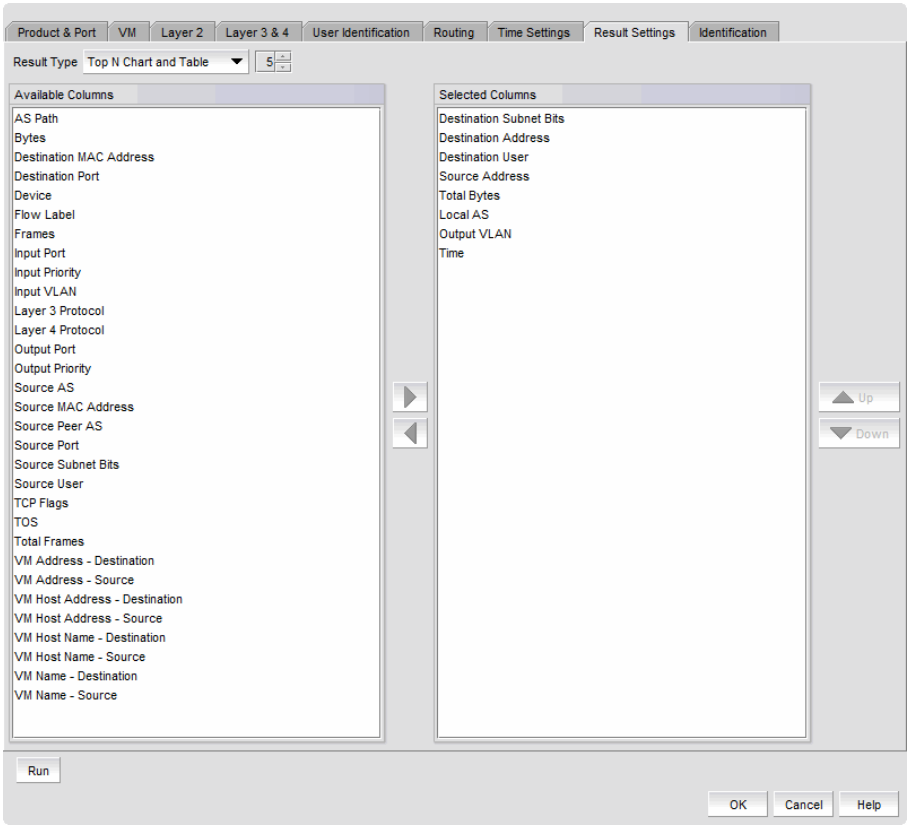


FIGURE 433 Add Report Definitions dialog box, Result Settings tab

23. If you selected **Bottom N Chart and Table** or **Top N Chart and Table**, select the top or bottom number (N) of talkers that you want in the report by clicking the arrows on the selector to the right of the **Result Type** list. Select a minimum of 5, with increments of 5 to a maximum of 25.

    Figure 435 on page 1034 shows an example report for the top five talkers shown in total bytes for source and destination MAC addresses.

24. Under **Available Columns**, select the attributes you want to display, and click the right arrow to move them to **Selected Columns**. Among those you move should be the attribute you want to use to sort the columns. For example, you may want to display Destination Address, Destination MAC Address, and Destination Port and sort them by Device.

25. Under **Selected Columns**, select the attribute you want to use to sort the columns and use the right arrow to move that attribute to **Sort by Columns** (only available if you select **Detailed Table** for the **Result Type**.

    You can use the up and down arrows to arrange the order in which columns will display in your report.

26. Select the **Identification** tab. **Add Report Definitions** dialog box displays, as shown in Figure 434 on page 1033.

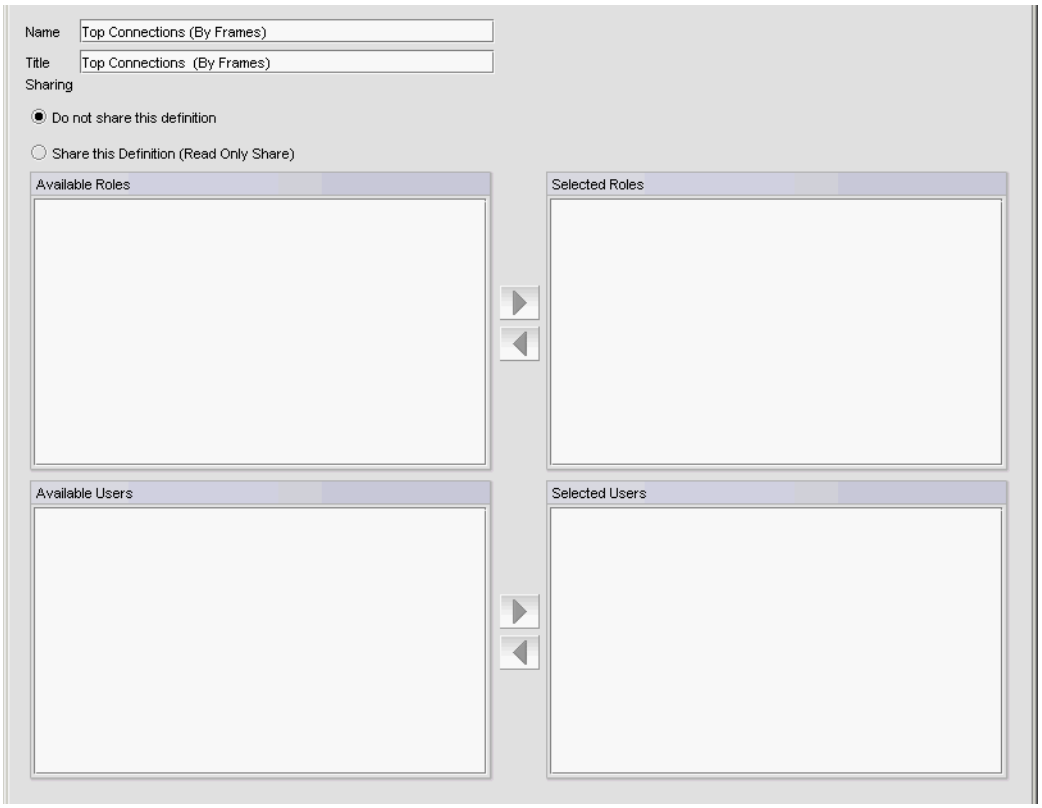
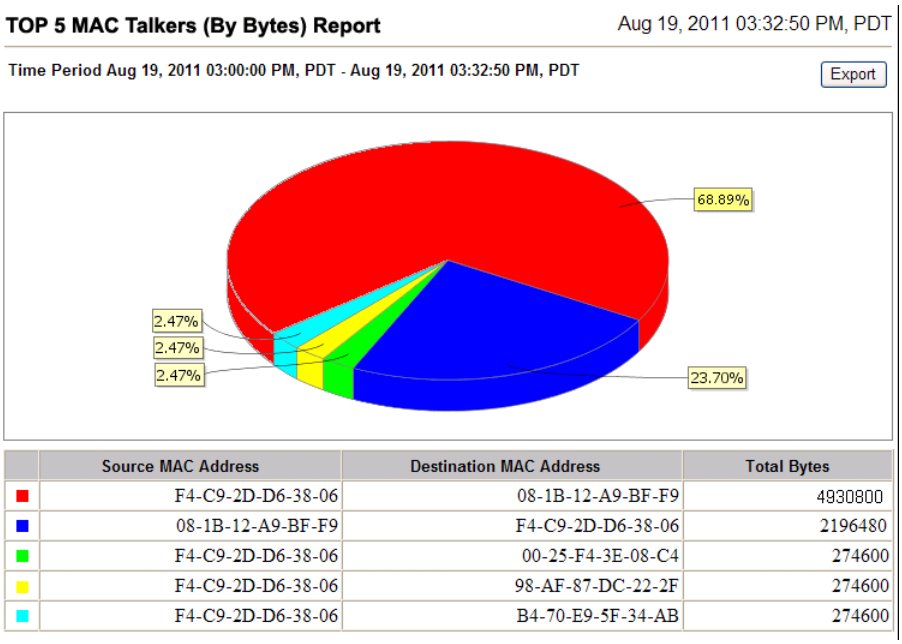


FIGURE 434 Add Report Definitions dialog box, Identification tab

27. Enter a name for the report in the **Name** field. The name must be unique among all sFlow reports, and can be a maximum of 64 alphanumeric characters.
28. Enter the report title in the **Title** field. The Title field supports a maximum of 128 alphanumeric characters.
29. Select **Do not share the definition** if you do not want other users to see the report definition when they log in.
30. Select **Share this definition** if you want other users to have read only access to the report definition.
31. If you select **Share this definition**, a list of user roles displays under **Available Roles**. Select user roles that you want to empower to view and run the report definition, and use the right arrow button to move the roles to **Selected Roles**.
32. If you select **Share this definition**, a list of users displays under **Available Users**. Select users that you want to empower to view and run the report definition, and use the right arrow button to move the users to **Selected Users**.

    Click **OK** to save the definition or click **Run** to run the report.

    The Figure 435 on page 1034 shows an example report for the top five talkers shown in total bytes for source and destination MAC addresses.



	Source MAC Address	Destination MAC Address	Total Bytes
■	F4-C9-2D-D6-38-06	08-1B-12-A9-BF-F9	4930800
■	08-1B-12-A9-BF-F9	F4-C9-2D-D6-38-06	2196480
■	F4-C9-2D-D6-38-06	00-25-F4-3E-08-C4	274600
■	F4-C9-2D-D6-38-06	98-AF-87-DC-22-2F	274600
■	F4-C9-2D-D6-38-06	B4-70-E9-5F-34-AB	274600

FIGURE 435 Example report for top 5 MAC Talkers

Scheduling custom sFlow reports

You can schedule a custom sFlow report from the **Schedules** tab of the **Custom Reports** dialog box.

1. Select **Monitor > Traffic Analysis > Custom Reports**.
2. Select the **Schedules** tab. Custom sFlow Reports dialog box displays, as shown in Figure 436 on page 1035.

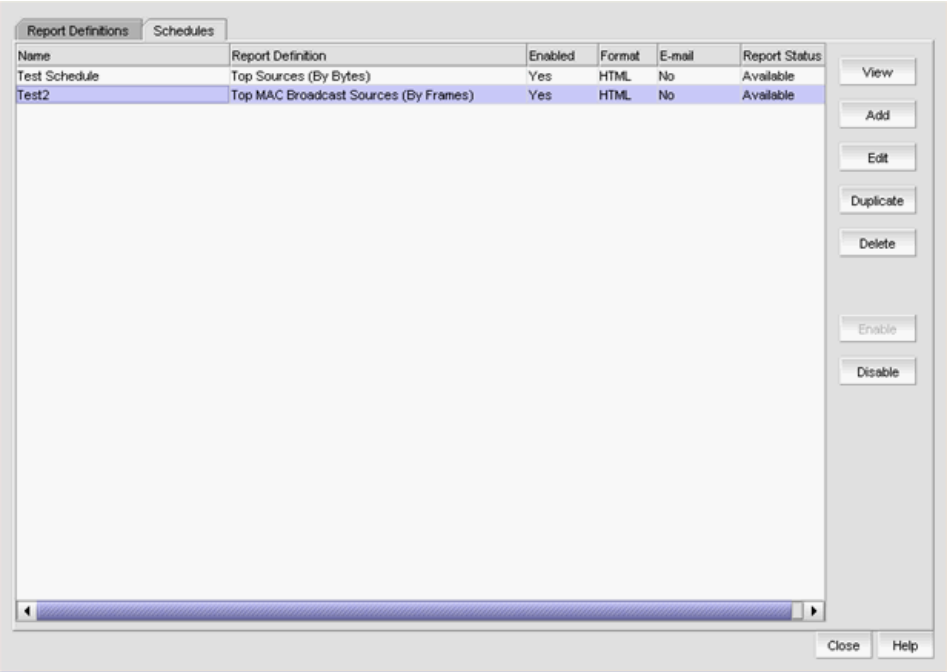


FIGURE 436 Custom sFlow Reports dialog box, Schedules tab

3. Click **Add**.

   The **Add Schedule** dialog box displays, as shown in Figure 437 on page 1036.

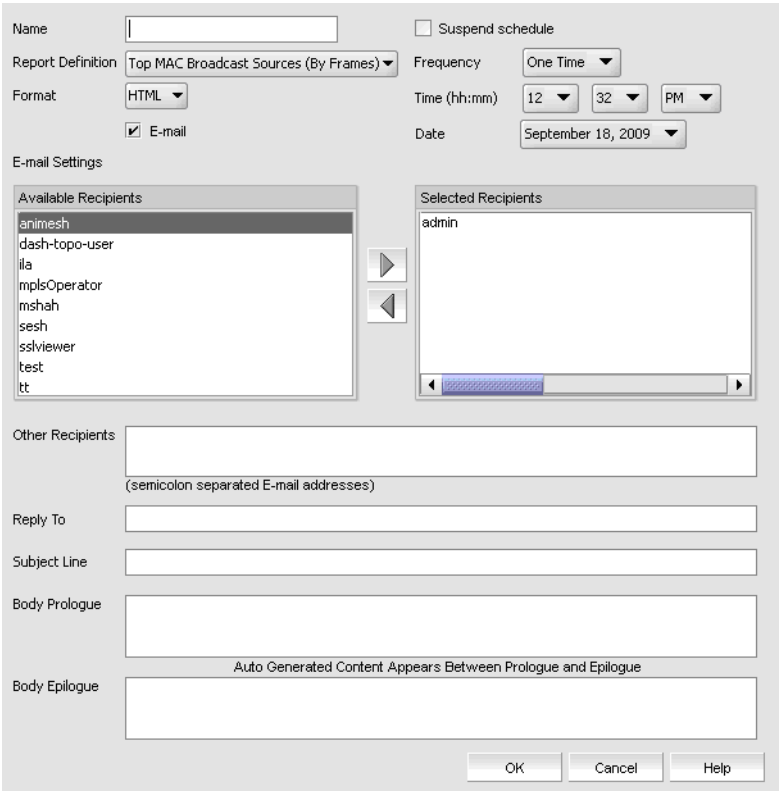


FIGURE 437 Add Schedule dialog box

4. Enter a name for the schedule in the **Name** field.
5. Use the **Report Definition** selector to select the report definition you want to schedule.

NOTE
Report definitions that included a prompt are not listed.

6. Use the **Format** selector to choose either **HTML** or **CSV** format.
7. Use the **Frequency** selector to choose to run the data collector on a **Yearly**, **Monthly**, **Weekly**, **Daily**, **Hourly**, or **One Time** basis. Appropriate options are displayed allowing you set a start time and duration for data collection.
   - If you select **Yearly**, or **One Time**, the **Time(hh:mm)** and **Date** selectors display.
   - If you select **Monthly**, the **Time(hh:mm)** and **Day of the Month** selectors display.
   - If you select **Weekly**, the **Time(hh:mm)** and **Day of the Week** selectors display.
   - If you select **Daily**, the **Time(hh:mm)** selector displays.
8. If you want to send the report to an e-mail recipient, check the **E-mail** check box.
9. If you checked the **E-mail** check box, select recipients under **Available Recipients** and use the right arrow to move them to **Selected Recipients**. Use the **Other Recipients** field to add recipients that are not listed under **Available Recipients**.
10. Enter an e-mail address for replies in the **Reply To** field. This is mandatory.
11. Enter text for the subject line in the **Subject Line** field.

12. You may include text that you want to add before the auto-generated report content in the **Body Prologue** field.
13. You may include text that you want to add after the auto-generated report content in the **Body Epilogue** field.
14. Click **OK**.

Suspending a custom sFlow report schedule

To suspend the schedule of a custom sFlow report, complete the following steps.

1. Select **Monitor > Traffic Analysis > Custom Reports**.
2. Select the **Schedules** tab.
3. Select the schedule you want to suspend and click **Edit**.

   The **Edit Schedule** dialog box displays.
4. Select the **Suspend schedule** check box.
5. Click **OK**.

IP Traffic analyzer monitoring and sFlow reports

Traffic analyzer monitoring includes reports that can be used to display sFlow traffic information. The sFlow standard, as described in RFC 3176, is a method for capturing traffic data in switched or routed networks. An sFlow agent samples traffic on the hardware. The sFlow datagrams are stored and may be analyzed and organized into reports.

- **Layer 2 reports:** MAC addresses, VMs, and VLANs
- **Layer 3 or Layer 4 traffic reports:** All Layer 3 protocols, IP, IPv4, and IPv6

  IPv4 and IPv6 reports provide the following additional reports:
  - Top users of all Layer 4 protocols
  - Top TCP Talkers
  - Top ICMP Talkers
  - Top UDP Talkers
  - Top talkers for all services.
  - Top talkers for all Layer 4 protocol services excluding TCP, UDP, and ICMP
- **TCP reports:** Invalid TCP flags and valid TCP flags
- **Miscellaneous:** BGP path reports

Device-level configuration requirements

To be able to collect sFlow network traffic data, make sure sFlow is supported and enabled on the product or port you want to monitor. The number of sFlow destinations you can have depends on the device and the software release it is running. Refer to the configuration guide for your device for details on how to enable and configure sFlow monitoring on the device.

802.1X configuration requirements

802.1X user information can be displayed on sFlow reports. To ensure that this information is displayed, do the following:

- Make sure the device and software release it is running supports 802.1X.
- 802.1X must be enabled on the device ports.
- Clients must be running software platforms that support 802.1X (for example, Windows XP operating system).
- RADIUS authentication servers must have the 802.1X feature enabled and properly configured.

Displaying sFlow monitoring reports

NOTE
You cannot display sFlow monitoring reports for DCB or ADX devices.

To display sFlow monitoring reports, complete the following steps.

1. Select **Monitor > Traffic Analysis > Monitor sFlow**.

   The **Monitor sFlow** dialog box displays, as shown in Figure 438 on page 1038.

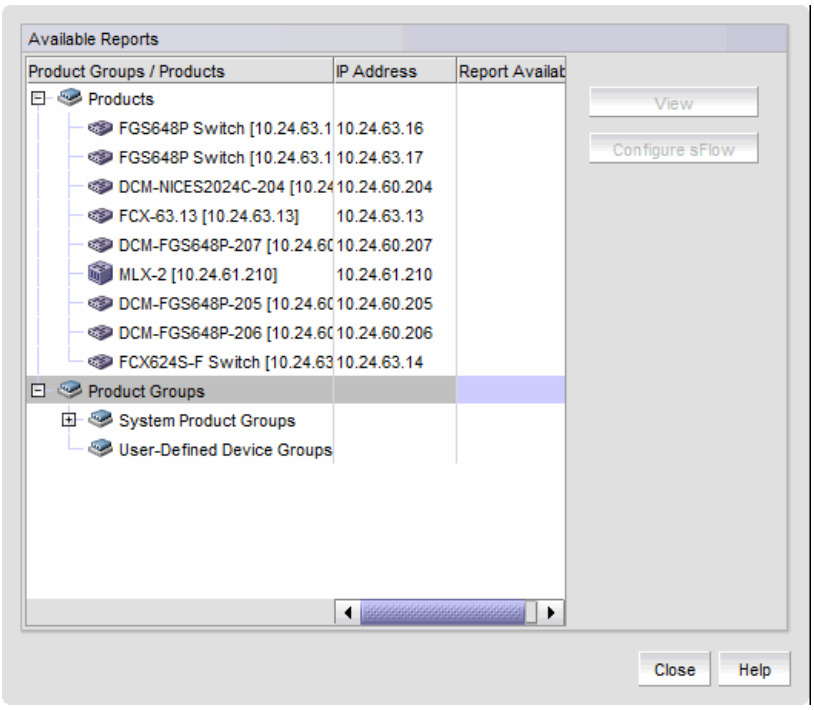


FIGURE 438 Monitor sFlow dialog box

2. Select a report that has a bar graph icon under **Report Available**.

   For VCS fabrics, the report only displays traffic sampled from the edge ports of the fabric.

3. Click **View** to display the report.

4. To launch the sFlow Configuration wizard and configure an sFlow data collector, select **Configure sFlow**.

Selecting a report

Use the report header to configure the report display. This section explains the available fields and selection options.

Report list

Select the type of traffic that you want to view from the list.

- For Layer 2 reports, select MAC, VM, or VLAN.
- For L3/L4 reports, select IPv4, IPv6, IPX, AppleTalk (AT), VM, or Others.
- For TCP reports, select Invalid TCP Flags or Valid TCP Flags.
- For Misc. reports, select BGP Paths.

When you select IPv4 or IPv6 from the **Report** list, another list appears. From this additional list, select the Layer 4 protocol to be included in the report. You can select All, TCP, UDP, ICMP, or Other, which includes all protocols excluding TCP, UDP, and ICMP.

Direction list

This is only available for VM Reports. Select one of the following from the list:

- Source
- Destination
- Both

Graph list

If the **Graph** box is enabled, select the format of the graph to be used to display the report. You can choose, Bar, Line, or Pie.

End Date/Time list

Select the date and time when the report is to end from the lists.

Span list

Span is the amount of data you want to include in the report. Select 1, 2, 4, 6, or 12 hours or 1 day (24 hours) from the list.

How End Date/Time and Span works:

Assume you have seven days of sFlow data from June 1 through 7. You want to view the first four hours of data during June 2. From the End Date/Time lists, select 6/2 for day and 4 am for time. In the Span list, select 4h. The resulting report shows four hours of data for June 2, beginning at 12 am and ending at 4 am.

Also, if you select 1, 2, 4, or 6 hours for span, top talkers are shown as stacked bar graphs; each bar represents two minutes of data. For example, each bar below represents 2 minutes of data. Each bar is divided into the top talkers for that 2-minute period.

Measure list

Select how data is to be sorted: Bytes or Frames. Frames is the default.

Refresh list

If you select 12 hours or 1 day for span, each bar represents one hour of aggregated data and a bar represents each top talker. For example, each set of 6 bars represents an hour of data; one bar represents a top talker.

Select the refresh rate for the graph from the list. The default refresh rate is configured in the configuration.properties file.

NOTE
The sFlow Monitoring report automatically refreshes the displayed information as specified in the Refresh Rate box. Once any of the Monitoring Actions arrow is clicked, this auto-refresh action fails. This is true even if you click Cancel in the confirmation dialog. You must initiate a refresh by changing the values in any of the header selections for the auto-refresh to start working again.

2D or 3D button

Click this button to toggle between a two-dimensional and three-dimensional graph.

Graph check box

Select this check box if you want data to be presented in a graph format.

Table check box

Select this check box if you want data to be presented in a table.

If Table (box) is enabled, a table shows details for the top resource users, beginning with the heaviest user. If you are viewing a report for a device group, the top users in the group are presented. If you are viewing a report for a device, the top resource users for the device are listed. Traffic for the remaining users on the network appear at the end of the table, along with the traffic total.

If the table is displayed, you can also do the following to manage a port that appears on the report:

- Disable a port.
- Enable a port.
- Apply rate limiting policies to a port.
- Apply ACL policies to a port.

Show DNS Name

Select this check box if you want domain name server (DNS) names of IP addresses to be displayed on the report.

Include Remaining Talkers

The sFlow monitoring reports display the top five talkers and remaining talkers. To exclude any remaining talkers in the chart area, select this check box.

Report Title and Device Group Name or Device Name and Device IP Address

This field shows the name of the report, followed by one of the following:

- Device group name (Group level): If you selected a report for a device group.
- Device name and IP address: If you selected a report for a device

Date and time

This field shows the date and time the report was requested.

Changing the number of records gathered for sFlow accounting

To change the number of records gathered for sFlow accounting, complete the following steps.

1. Go to the *Install_Home*/conf/ directory.
2. Open the ipconfig.properties file in a text editor.
3. Change the **SFlowAccounting.MaxRowsToFetchPerDevice** parameter to the number of records you want gathered for sFlow accounting.
4. Save and close the ipconfig.properties file.

Interpreting an sFlow traffic report

All sFlow traffic reports contain the following sections:

- Navigation arrows.
- Data presented in a graph, if enabled.
- Color legend.
- Data presented in a table, if enabled.
- Total traffic appears in frames and megabytes.

The report header displays the criteria selected for the report.

If the **Graph** check box is selected, a graph appears below the report header. Data for the most current time on the report is displayed when a report is requested. The navigation arrows in the report header allow you to display the next or previous panel of the report. Refer to the "Selecting a report" on page 1039 for information on what the graph represents.

There are differences in the graphs for periods up to six hours and for the 12 and 24 hour graphs:

- For periods up to 6 hours, the graph shows stacked bars. Each bar represents a flow aggregated for a 2-minute period. Each stack represents all the flows in the system aggregated for a 2-minute period.

- The 12 and 24 hour graphs show bars (not stacked bars). Each bar represents a flow aggregated for a 1-hour period. There are six bars to a set, starting with red and ending with gray. Each set represents all the flows in the system aggregated for a 1-hour period, beginning with the time shown on the x-axis. You see this time halfway between the set of six bars.

The first five colors used on the graph represent the top five resource users. The last color (gray by default) represents all the remaining users in the device group. The color legend defines the individual source and destination of the traffic.

If Table is enabled, a table appears under the graph and presents details about the top users. The number of pairs displayed depends on the value of the MaxPairsToShow parameter on the **Options** dialog box (refer to "Configuring sFlow monitoring preferences" on page 164). Combined usage by all remaining users and a total for all users appear at the end of the table. The number of top resource users shown and the number of rows displayed on a report depends on how sFlow parameters in the **Options** dialog box are defined.

Refer to the following sections to interpret the table:

- "Viewing top MAC talkers" on page 1042
- "Viewing top VLAN talkers" on page 1043
- "Viewing all Layer 3 and Layer 4 traffic" on page 1044
- "Viewing all IPv4 Layer 3 or Layer 4 Top Talkers" on page 1044
- "Viewing IPv4 – top TCP talkers" on page 1045
- "Viewing IPv4 – top UDP talkers" on page 1047
- "Viewing IPv4 – top ICMP talkers" on page 1048
- "Viewing IPv6 Top Talkers" on page 1049, discusses the following reports:
  - Top IPV6 Talkers using all Layer 4 services
  - Top TCP Talkers
  - Top UDP Talkers
  - Top ICMP Talkers
  - Top IPV6 Talkers of all Layer 4 service, excluding TCP, UDP, and ICMP
- "Viewing other Layer 3 or Layer 4 Top Talkers" on page 1050
- "Enabling and viewing TCP reports" on page 1051
- "Viewing BGP paths report" on page 1053

The sFlow report that you request may not display all the data collected. The reports may be truncated if there are more rows than the limit specified in the **Options** dialog box file. To view the entire report, you must export it to a tab-separated file.

Viewing top MAC talkers

The **Top MAC Talkers** report shows the top pairs of source and destination MAC addresses being used on the network. Follow the steps below to display the report.

1. Select **Monitor > Traffic Analysis > Monitor sFlow**.
2. On the **Monitor sFlow** dialog box, choose one of the following options:
   - To view a report for a product group, click the report icon for the product group you want.

- To view a report for a product, click the name of the product group to which the product belongs, and on the Product list page, click the icon for the product.

3. Click **View** to display the report.
4. In the **Category** list, select **L3/L4 Reports**.
5. In the **Reports** list, select **MAC**.

The following information is provided:

- MAC - The source and destination MAC addresses of the traffic and the VM host (Top VM Talkers reports). If Source and Destination VM Host column values are not related to VM, no values will display.
- Port - The ID of ports on which the traffic is being received and being sent. For VCS fabrics, the send and receive ports are from different devices.
- VLAN - The ID of the source and destination VLANs in the traffic.
- Ethernet QOS - The 802.1p priority tag configured on the incoming and outgoing traffic.
- User (802.1X) - The name of the user who originated the traffic and the user who received the traffic. This name is the ID the client used to gain access to the network.
- Frames - The size of the traffic in frames.
- MBytes - The size of the traffic in megabytes for the time duration shown on the report.

A subtotal is displayed under each top user by source and destination MAC addresses. If the report is for a product group, the name and IP address of the product that the traffic accessed appear in parentheses next to the MAC addresses. If the report is for an individual product, only the MAC addresses are displayed.

A subtotal for the remaining network users and a total of all network traffic appears at the bottom of the report.

Viewing top VLAN talkers

The **Top VLAN Talkers** report shows the top pairs of source and destination VLAN IDs being used by the top users. Complete the following steps to display the report.

1. Select **Monitor > Traffic Analysis > Monitor sFlow.**
2. On the **Monitor sFlow** dialog box, choose one of the following options:
   - To view a report for a device group, click the report icon for the device group you want.
   - To view a report for a device, click the name of the device group to which the device belongs, and on the Device list page, click the report icon for the device.
3. In the **Category** list, select **L2 Reports**.
4. In the **Reports** list, select **VLAN**.

The report presents the following information:

- VLAN - The ID of the source and destination VLANs used by the users.
- Ethernet QOS - The 802.1p priority tag configured on the incoming and outgoing traffic.
- Port - The ID of the port on which the traffic is being received and being sent.
- For VCS fabrics, the send and receive ports are from different devices.

- MAC - The source and destination MAC addresses of the traffic and the VM host (Top VM Talkers reports). If Source and Destination VM Host column values are not related to VM, no values will display.
- User (802.1X) - The name of the user who originated the traffic and the user who received the traffic. This name is the ID the client used to gain access to the network.
- Frames - The size of the traffic in frames.
- MBytes - The size of the traffic in megabytes for the time duration shown on the report.

A subtotal is displayed for each of the top users. At the end of the report, a subtotal for the remaining network users and a total for the entire network are displayed.

Viewing all Layer 3 and Layer 4 traffic

The Layer3/4 All report displays the top users of all Layer 3 and Layer 4 traffic. Complete the following steps to display the report.

1. Select **Monitor > Traffic Analysis > Monitor sFlow**.
2. On the **Monitor sFlow** dialog box, choose one of the following options:
   - To view a report for a device group, click the report icon for the device group you want.
   - To view a report for a device, click the name of the device group to which the device belongs, and on the Device list page, click the report icon for the device.
3. In the **Category** list, select **L3/L4 Reports**.
4. In the **Report** list, select **All**.

The report you see is similar to the one shown in Other Layer 3/Layer4 Talkers. (Refer to "Viewing other Layer 3 or Layer 4 Top Talkers" on page 1050.)

Viewing all IPv4 Layer 3 or Layer 4 Top Talkers

The **IPV4 Top Layer 3/4 Top Talkers** report shows the top users of all Layer 3 and Layer 4 services on IPv4 traffic. Complete the following steps to display the report.

1. Select **Monitor > Traffic Analysis > Monitor sFlow**.
2. On the **Monitor sFlow** dialog box, choose one of the following options:
   - To view a report for a device group, click the report icon for the device group you want.
   - To view a report for a device, click the name of the device group to which the device belongs, and on the Device list page, click the report icon for the device.
3. In the **Category** list, select **L3/L4 Reports**.
4. In the **Report** list, select **IPv4**.
5. In the next list, select **All**.

The report provides the following information:

- L3 columns
  - Source - The source IP addresses of the IPv4 traffic and VM hosts (Top VM Talkers reports). If enabled, host names of the IP address are shown in parentheses.
  - Destination - The destination IP addresses of the IPv4 traffic and VM hosts (Top VM Talkers reports). If enabled, host names of the IP address are shown in parentheses.
  - TOS/DSCP - The TOS bit value or the Differentiated Services Code Points (DSCP) value in the packets.
- Port - For VCS fabrics, the send and receive ports are from different devices.
  - In - The ID of the port on which the traffic is being received.
  - Out - The ID of the port on which the traffic is being sent.
- L4 Protocol columns
  - Name - Name of the Layer 4 protocol used in the packet.
  - Src Port - ID of the port on which the packet originated. The value shown in this column can be one of the following values:
    - ID of the well-known port.
    - The term “various,” if the value is greater than 1023 (threshold for well-known ports) and if the port number on the other side of the connection is an ephemeral port.
  - Dest Port - ID of the port on which the packet was received. The value shown in this column can be one of the following values:
    - ID of the well-known port.
    - The term “various,” if the value is greater than 1023 (threshold for well-known ports) and if the port number on the other side of the connection is an ephemeral port.
- User (802.1X)
  - Source - Name of the user who originated the traffic. This name is the ID the client used to gain access to the network.
  - Destination - Name of the user who received the traffic. This name is the ID the client used to gain access to the network.
- Frames - Size of the traffic in frames.
- Mbytes - Size of the traffic in megabytes for the time duration shown on the report.

Viewing IPv4 – top TCP talkers

The **Top IPV4–TCP Talkers** report shows the top users of IPv4 TCP services. Complete the following steps to display the report.

1. Select **Monitor > Traffic Analysis > Monitor sFlow**.
2. On the **Monitor sFlow** dialog box, choose one of the following options:
   - To view a report for a device group, click the report icon for the device group you want.
   - To view a report for a device, click the name of the device group to which the device belongs, and on the Device list page, click the report icon for the device.
3. In the **Category** list, select **L3/L4 Reports**.
4. In the **Reports** list, select **IPV4**.
5. In the next list, select **TCP**.

The report shows the following information:

- IPV4
  - Source - The source IP addresses of the IPv4 traffic. If enabled, host names of the IP address are shown in parentheses.
  - Destination - The destination IP addresses of the IPv4 traffic. If enabled, host names of the IP address are shown in parentheses.
  - TOS/DSCP - The TOS bit value or the Differentiated Services Code Points (DSCP) value in the packets.
- Port - For VCS fabrics, the send and receive ports are from different devices.
  - In - The ID of the port on which the traffic is being received.
  - Out - The ID of the port on which the traffic is being sent.
- TCP
  - Src Port - ID of the port on which the TCP packet originated. The value shown in this column can be one of the following values:
    - ID of the well-known port.
    - The term “various”, if the value is greater than 1023 (threshold for well-known ports) and if the port number on the other side of the connection is an ephemeral port.
  - Dest Port - ID of the port on which the TCP packet was received. The value shown in this column can be one of the following values:
    - ID of the well-known port.
    - The term “various”, if the value is greater than 1023 (threshold for well-known ports) and if the port number on the other side of the connection is an ephemeral port.
- User (802.1X)
  - Name of the user who originated the traffic. This name is the ID the client used to gain access to the network.
  - Name of the user who received the traffic. This name is the ID the client used to gain access to the network.
- Frames - Size of the traffic in frames.
- Mbytes - Size of the traffic in megabytes for the time duration shown on the report.

A subtotal is displayed for each of the top users. This subtotal is displayed by source and destination IP addresses. If the report is for a device group, the name and IP address of the device that the traffic accessed appear in parentheses. If the report is for an individual device, only the source and destination IP addresses appear.

At the end of the report, a subtotal for the remaining network users and a total for the entire network are displayed.

Viewing IPv4 – top UDP talkers

The **Top IPV4–UDP Talkers** report shows the top users of IPv4 UDP services. Complete the following steps to display the report.

1. Select **Monitor > Traffic Analysis > Monitor sFlow**.
2. On the **Monitor sFlow** dialog box, choose one of the following options:
   - To view a report for a device group, click the report icon for the device group you want.
   - To view a report for a device, click the name of the device group to which the device belongs, and on the Device list page, click the report icon for the device.
3. In the **Category** list, select **L3/L4 Reports**.
4. In the **Reports** list, select **IPV4**.
5. In the next list, select **UDP**.

The report shows the following information:

- IPV4
  - Source - The source IP addresses of the IPv4 traffic. If enabled, host names of the IP address are shown in parentheses.
  - Destination - The destination IP addresses of the IPv4 traffic. If enabled, host names of the IP address are shown in parentheses.
  - TOS/DSCP - The TOS bit value or the Differentiated Services Code Points (DSCP) value in the packets.
- Port - For VCS fabrics, the send and receive ports are from different devices.
  - In - The ID of the port on which the traffic is being received.
  - Out - The ID of the port on which the traffic is being sent.
- UDP
  - Src Port - ID of the port on which the UDP packet originated. The value shown in this column can be one of the following values:
    - ID of the well-known port.
    - The term “various,” if the value is greater than 1023 (threshold for well-known ports) and if the port number on the other side of the connection is an ephemeral port.
  - Dest Port - ID of the port on which the UDP packet was received. The value shown in this column can be one of the following values:
    - ID of the well-known port.
    - The term “various,” if the value is greater than 1023 (threshold for well-known ports) and if the port number on the other side of the connection is an ephemeral port.
- User (802.1X)
  - Source - Name of the user who originated the traffic. This name is the ID the client used to gain access to the network.
  - Destination - Name of the user who received the traffic. This name is the ID the client used to gain access to the network.
- Frames - Size of the traffic in frames.
- Mbytes - Size of the traffic in megabytes for the time duration shown on the report.

A subtotal is displayed for each of the top users. This subtotal is displayed by source and destination IP addresses. If the report is for a device group, the name and IP address of the device that the traffic accessed appear in parentheses. If the report is for an individual device, only the source and destination IP addresses appear.

At the end of the report, a subtotal for the remaining network users and a total for the entire network are displayed.

Viewing IPv4 – top ICMP talkers

The **Top IPV4–ICMP Talkers** report shows the top users of IPv4 ICMP services. Complete the following steps to display the report.

1. Select **Monitor > Traffic Analysis > Monitor sFlow**.
2. On the **Monitor sFlow** dialog box, choose one of the following options:
   - To view a report for a device group, click the report icon for the device group you want.
   - To view a report for a device, click the name of the device group to which the device belongs, and on the Device list page, click the report icon for the device.
3. In the **Category** list, select **L3 or L4 Reports**.
4. In the **Reports** list, select **IPV4**.
5. In the next list, select **ICMP**.

The report shows the following information:

- IPV4
  - Source - The source IP addresses of the IPv4 traffic. If enabled, host names of the IP address are shown in parentheses.
  - Destination - The destination IP addresses of the IPv4 traffic. If enabled, host names of the IP address are shown in parentheses.
  - TOS/DSCP - The TOS bit value or the Differentiated Services Code Points (DSCP) value in the packets.
- Port - For VCS fabrics, the send and receive ports are from different devices.
  - In - The ID of the port on which the traffic is being received.
  - Out - The ID of the port on which the traffic is being sent.
- ICMP
  - Src Port - ID of the port on which the ICMP packet originated. The value shown in this column can be one of the following values:
    - ID of the well-known port.
    - The term “various,” if the value is greater than 1023 (threshold for well-known ports) and if the port number on the other side of the connection is an ephemeral port.
- User (802.1X)
  - Source - Name of the user who originated the traffic. This name is the ID the client used to gain access to the network.
  - Destination - Name of the user who received the traffic. This name is the ID the client used to gain access to the network.
- Frames - Size of the traffic in frames.

- Mbytes - Size of the traffic in megabytes for the time duration shown on the report.

A subtotal is displayed for each of the top users. This subtotal is displayed by source and destination IP addresses. If the report is for a device group, the name and IP address of the device that the traffic accessed appear in parentheses. If the report is for an individual device, only the source and destination IP addresses appear.

At the end of the report, a subtotal for the remaining network users and a total for the entire network are displayed.

Viewing IPv4 – Others

The **Top IPV4–Others** report shows the top users of IPv4 traffic excluding TCP, UDP, or ICMP services. Complete the following steps to display the report.

1. Select **Monitor > Traffic Analysis > Monitor sFlow**.
2. On the **Monitor sFlow** dialog box, choose one of the following options:
   - To view a report for a device group, click the report icon for the device group you want.
   - To view a report for a device, click the name of the device group to which the device belongs, and on the Device list page, click the report icon for the device.
3. In the **Category** list, select **L3/L4 Reports**.
4. In the **Reports** list, select **IPV4**.
5. In the next list, select **Others**.

A report, similar to other IPv4 reports is displayed; however, instead of the TCP, UDP, and ICMP columns, a column showing the Layer 4 protocol on the traffic appears on the report.

Viewing IPv6 Top Talkers

The **IPv6 Top Talkers** reports display the top users of Layer 3 and Layer 4 IPv6 traffic. Reports for top users of the following services are available:

- All Layer 3 and Layer 4 IPv6 services – Display this report by selecting **L3/L4 Reports > IPV6 > All**.
- IPv6 TCP users – Display this report by selecting **L3 or L4 Reports > IPV6 > TCP**.
- IPv6 UDP users – Display this report by selecting **L3 or L4 Reports > IPV6 > UDP**.
- IPv6 ICMP users – Display this report by selecting **L3 or L4 Reports > IPV6 > ICMP**.
- IPv6 users of other Layer 3 and Layer 4 services – Display this report by selecting **L3 or L4 Reports > IPV6 > Others**.

The IPv6 reports are similar to their IPv4 counterparts, except for the following:

- IPv4 reports show IP addresses in IPV4 format; but, IPv6 reports have IP addresses in IPv6 format.
- IPV4 reports show the TOS/DSCP values; but, IPv6 reports show Traffic Class values.

Viewing other Layer 3 or Layer 4 Top Talkers

The Others report under the Layer3/Layer 4 report category provides information on Layer 3 protocols excluding IPV4, IPV6, IPX, and AppleTalk services. Complete the following steps to display the report.

1. Select **Monitor > Traffic Analysis > Monitor sFlow**.
2. On the **Monitor sFlow** dialog box, choose one of the following options:
   - To view a report for a device group, click the report icon for the device group you want.
   - To view a report for a device, click the name of the device group to which the device belongs, and on the Device list page, click the report icon for the device.
3. In the **Category** list, select **L3/L4 Reports**.
4. In the **Reports** list, select **Other**.

The report shows the following information:

- L3
  - Source - The source IP addresses of the Layer 3 traffic and VM hosts (Top VM Talkers reports). If enabled, host names of the IP address are shown in parentheses.
  - Destination - The destination IP addresses of the Layer 3 traffic and VM hosts (Top VM Talkers reports). If enabled, host names of the IP address are shown in parentheses.
  - Protocol - The Layer 3 protocol on the traffic.
- Port - For VCS fabrics, the send and receive ports are from different devices.
  - In - The ID of the port on which the traffic is being received.
  - Out - The ID of the port on which the traffic is being sent.
- L4 Protocol
  - Name - Name of the Layer 4 protocol on the traffic.
  - Src port - ID of the port on which the traffic originated. The value shown in this column can be one of the following values:
    - ID of the well-known port.
    - The term “various,” if the value is greater than 1023 (threshold for well-known ports) and if the port number on the other side of the connection is an ephemeral port.
  - Dest Port - ID of the port on which the traffic was received. The value shown in this column can be one of the following values:
    - ID of the well-known port.
    - The term “various,” if the value is greater than 1023 (threshold for well-known ports) and if the port number on the other side of the connection is an ephemeral port.
- User (802.1X)
  - Source - Name of the user who originated the traffic. This name is the ID the client used to gain access to the network.
  - Destination - Name of the user who received the traffic. This name is the ID the client used to gain access to the network.
- Frames - Size of the traffic in frames.
- Mbytes - Size of the traffic in megabytes for the time duration shown on the report.

Enabling and viewing TCP reports

You can monitor TCP traffic to determine if there is any unusual activity on the network, such as TCP attacks. Identifying unusual activity will aid in understanding the nature of the traffic and the ports that are affected, so that you can take corrective actions. For example, you may decide to disable a port on which TCP attacks are being received.

This feature is disabled by default; however, enabling the feature increases the number of distinct flows that the Management application server must process and, therefore, increases the load on the server. Complete the following steps to enable TCP reports.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **IP Preferences** from the **Software Configurations** list in the **Category** pane.
3. Go to the **SFlowDataCollector** preferences section.
4. Select the **ProcessTCPFlagsData** check box to monitor TCP traffic.
5. Click **Apply** or **OK** to save your work.

Once TCP reports are enabled, the following reports can be displayed to determine any usual TCP traffic:

- **Valid TCP Flags:** TCP traffic containing packets that do not have any invalid bit combinations.
- **Invalid TCP Flags:** TCP traffic containing packets that have invalid bit combinations as defined in the configuration.properties file.

Defining invalid TCP packet combinations

TCP packets can be checked to see if they contain the following control bits:

- ACK: Acknowledgement field significant bit
- URG: Urgent pointer field significant bit
- PSH: Push function bit
- RST: Reset connection bit
- SYN: Synchronize sequence number bit
- FIN: No more data from sender

An occurrence of two of these bits together in a TCP packet could be regarded as invalid. You specify in the configuration.properties file which combinations are invalid combinations. By default, the following combinations are regarded as invalid:

- RST-SYN
- RST-FIN
- RST-PSH
- RST-URG
- FIN-SYN

Complete the following steps to change these combinations.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **IP Preferences** from the **Software Configurations** list in the **Category** pane.
3. Go to the **SFlowDataMonitoring** preferences section.
4. Click in the **TCPFlags_InvalidCombos** parameter field to edit the invalid bit combinations.
5. Click **Apply** or **OK** to save your work.

Displaying the invalid TCP Flags report

Complete the following steps to display the invalid TCP flags report.

1. On the Management application menu bar, click **Monitor > Traffic Analysis > Monitor sFlow**.
2. On the initial Monitoring page, choose one of the following options:
   - To view a report for a device group, click a report icon for the device group you want.
   - To view a report for a device, click the name of the device group to which the device belongs, then on the Device list page, click a report icon for the device.
3. In the **Report** list, select **TCP Reports**.
4. In the **Type** list, select **Invalid TCP Flags**.

You see a report similar to the Valid TCP Flags report, except only invalid TCP flags are included in the report.

Valid TCP flags report

The **Valid TCP Flags** report shows TCP traffic containing packets that do not have any invalid bit combinations. Complete the following steps to display the report.

1. Select **Monitor > Traffic Analysis > Monitor sFlow**.
2. On the initial Monitoring page, choose one of the following options:
   - To view a report for a device group, click a report icon for the device group you want.
   - To view a report for a device, click the name of the device group to which the device belongs, and on the Device list page, click a report icon for the device.
3. In the **Report** list, select **TCP Reports**.
4. In the **Type** list, select **Valid TCP Flags**.

The report shows the following information:

- TCP Flags - All TCP flags present in the packet are identified by the first letter of the flag. For example, if the packet contains the ACK flag, the letter A appears in this column. If the packet contains the PSH and ACK flags, AP appears in this column.
- Port - The ID of the ports on which the flag is being received and being sent.
- MAC - The source and destination MAC addresses of the traffic that generated the flag.
- Ethernet QOS - The 802.1p priority tag configured on the incoming and outgoing traffic.
- IP - The source and destination IP address of the traffic and the TOS or DSCP value assigned to it.
- TCP Port - The name or number of the TCP port of incoming and outgoing traffic.
- User (802.1X) - Name of the user who originated the traffic and the user who received the traffic. This name is the ID the client used to gain access to the network.

- Frames - Size of the traffic in frames.
- MBytes - Size of the traffic in megabytes for the time duration shown on the report.

Viewing BGP paths report

The **BGP Paths** report shows source and destination traffic based on BGP autonomous systems paths. Complete the following steps to display the report.

1. Select **Monitor > Traffic Analysis > Monitor sFlow**.
2. On the initial Monitoring page, choose one of the following options:
   - To view a report for a device group, click a report icon for the device group you want.
   - To view a report for a device, click the name of the device group to which the device belongs, then on the Device list page, click a report icon for the device.
3. In the **Report** list, select **Misc Reports**.
4. In the **Type** list, select **BGP Path**.

   The report shows the following information:

- Source AS - The AS path number that is the source of this BGP route. A 32-bit AS path number may be displayed.
- Destination AS Path - The AS path number that is the destination of this BGP route. A 32-bit AS path number may be displayed.
- Frames - Size of the traffic in frames.
- Mbytes - Size of the traffic in megabytes for the time duration shown on the report.

Viewing VCS fabric Top Talker reports

The VCS fabric Top Talker report only displays traffic captured on the edge ports. Complete the following steps to display the report.

1. Select **Monitor > Traffic Analysis > Monitor sFlow**.
2. On the **Monitor sFlow** dialog box, click the report icon for the fabric you want.
3. Click **View** to display the report.

   The VCS fabric level report provides an aggregated view of the entire fabric. The content of the report depends on your selections in the **sFlow Monitor Report** dialog box. You can view the following report types:

   - "Viewing top MAC talkers" on page 1042
   - "Viewing all Layer 3 and Layer 4 traffic" on page 1044
   - "Viewing all IPv4 Layer 3 or Layer 4 Top Talkers" on page 1044
   - "Viewing IPv4 – top TCP talkers" on page 1045
   - "Viewing IPv4 – top UDP talkers" on page 1047
   - "Viewing other Layer 3 or Layer 4 Top Talkers" on page 1050
   - "Viewing BGP paths report" on page 1053

Troubleshooting sFlow reports

If the sFlow Monitoring report launches with an error on RedHat Linux, use the following steps to resolve.

1. Stop the server.
2. Run the command unset DISPLAY on the terminal.
3. Restart the server.

NOTE
You can only restart the server using the Server Management Console (**Start > Programs > Management_Application_Name 11.X.X > Server Management Console**).

IP traffic accounting

Traffic analysis accounting reports the total number of frames and total number of bytes that have entered and exited a port. Accounting details are separated into incoming and outgoing traffic reports.

1. Select **Monitor > Traffic Analysis > Traffic Accounting**.

   The **Traffic Accounting** dialog box displays, as shown in Figure 439 on page 1054.

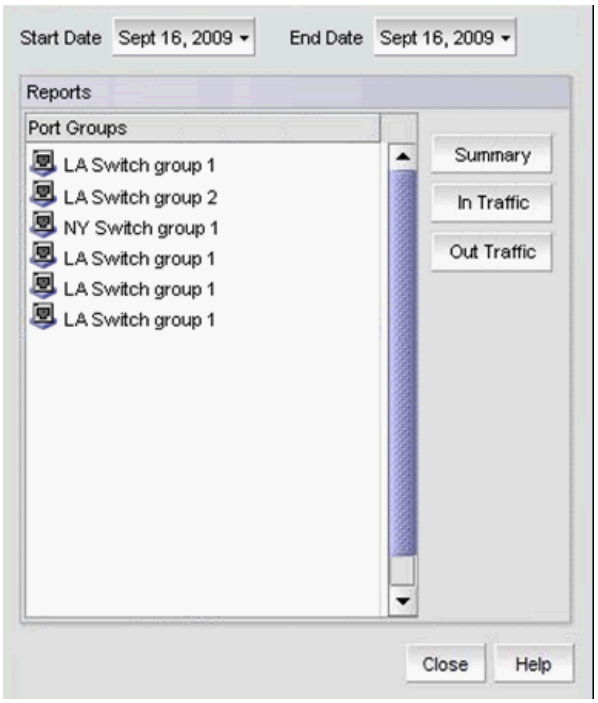


FIGURE 439 Traffic Accounting dialog box

2. Use the **Start Date** and **End Date** selectors to specify the time period for the accounting report.
3. Under **Port Groups**, select one of the listed groups.

4. You have three options for displaying traffic accounting information:
   - Click **Summary** to view the entire accounting summary report for the selected group.
   - Click **In Traffic** to view inbound traffic on the ports in the selected group.
   - Click **Out Traffic** to view outbound traffic on the ports in the selected group.

The number of records gathered for each device is limited to 10,000 by default. To change the number of records gathered, refer to "Changing the number of records displayed in a sFlow accounting report" on page 1055 and "Changing the number of records displayed in a sFlow accounting report" on page 1055.

Changing the number of records displayed in a sFlow accounting report

To change the number of records displayed in the report, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **IP Preferences** from the **Software Configurations** list in the **Category** pane
3. Scroll down to the **SFlow Accounting** section.
4. Enter the maximum number of rows to display in the log report in the **MaxRowsToShow** field.
5. Click **Apply** or **OK** to save your work.

Chapter

Frame Monitor

34

In this chapter

Frame Monitor

NOTE
Only available for Fabric OS products.

NOTE
Frame Monitoring is supported in Professional Plus and Enterprise Editions only. It is not supported in the Professional Edition.

Frame monitors count the number of frames transmitted through a port that match specific values in the first 64 bytes of the frame. Since the entire Fibre Channel frame header and many upper protocol (for example, SCSI) headers fall within the first 64 bytes of a frame, frame monitors can detect different types of traffic transmitted through a port. Each frame monitor keeps a timestamp of its last refresh. It also keeps a generation count, which is incremented each time the monitor is cleared.

Frame monitors generate alerts whenever the frame count for a certain frame type crosses the threshold configured for that frame type. You can configure high thresholds for every frame type, specify actions to be taken when the threshold is exceeded, and configure how often the data are sampled.

Virtual Fabrics considerations: You can assign frame monitors to ports in a logical switch. If a port is moved from one logical switch to another, however, all monitors that were assigned to the port are cleared in the new logical switch.

Trunking considerations: For trunked ports, the frame monitor is configured on the trunk master.

Frame types

The frame type can be a standard type (for example, a SCSI read command filter that counts the number of SCSI read commands that have been transmitted by the port) or a user-defined frame type customized for your particular use.

Pre-defined frame types

Pre-defined frame types include the following:

- ABTS (Abort Sequence Basic Link Service command)
- BA_ACC (Abort Accept)
- IP
- SCSI
- SCSI Read
- SCSI Write
- SCSI RW
- SCSI-2 Reserve
- SCSI-3 Reserve

Custom frame types

In addition to the standard frame types, you can create custom frame types to gather statistics that fit your needs. To define a custom frame type, you must specify a series of *offsets*, *bitmasks*, and *values*. For all transmitted frames, the switch performs these tasks:

- Locates the byte found in the frame at the specified *offset.*
- Applies the *bitmask* to the byte found in the frame.
- Compares the new value with the given *value*.
- Increments the filter counter if a match is found.

You can specify up to four values to compare against each offset. If more than one offset is required to properly define a filter, the bytes found at each offset must match one of the given values for the filter to increment its counter. If one or more of the given offsets does not match any of the given values, the counter does not increment. The value of the offset must be between 0 and 63, in decimal format. Byte 0 indicates the first byte of the Start of Frame (SOF), byte 4 is the first byte of the frame header, and byte 28 is the first byte of the payload. Thus only the SOF, frame header, and first 36 bytes of payload can be selected as part of a filter definition. Offset 0 is a special case, which can be used to monitor the first 4 bytes of the frame (SOF). When the offset is set to 0, the values 0–7 that are checked against that offset are predefined as shown in Table 91.

TABLE 91 Predefined values at offset 0

Value	SOF	Value	SOF
0	SOFf	4	SOFi2
1	SOFc1	5	SOFn2
2	SOFi1	6	SOFi3
3	SOFn1	7	SOFn3

Frame Monitoring requirements

To configure Frame Monitoring, the following requirements must be met:

- The switch must be running Fabric OS 7.0.0 or later.
- Frame Monitoring requires the Advanced Performance Monitoring license and the Fabric Watch license.

NOTE
The Advanced Performance Monitoring license is required to configure frame monitors. The monitoring functionality requires the Fabric Watch license.

The maximum number of frame monitors and offsets per port is platform-specific. Refer to the *Fabric OS Administrator's Guide* for more information.

Creating a custom frame monitor

Pre-defined frame monitors are already installed on switches that support Frame Monitoring. Use this procedure if you want to create a custom frame monitor.

1. Select **Monitor > Fabric Watch > Frame Monitor**.

   The Frame Monitor dialog box displays (Figure 440).

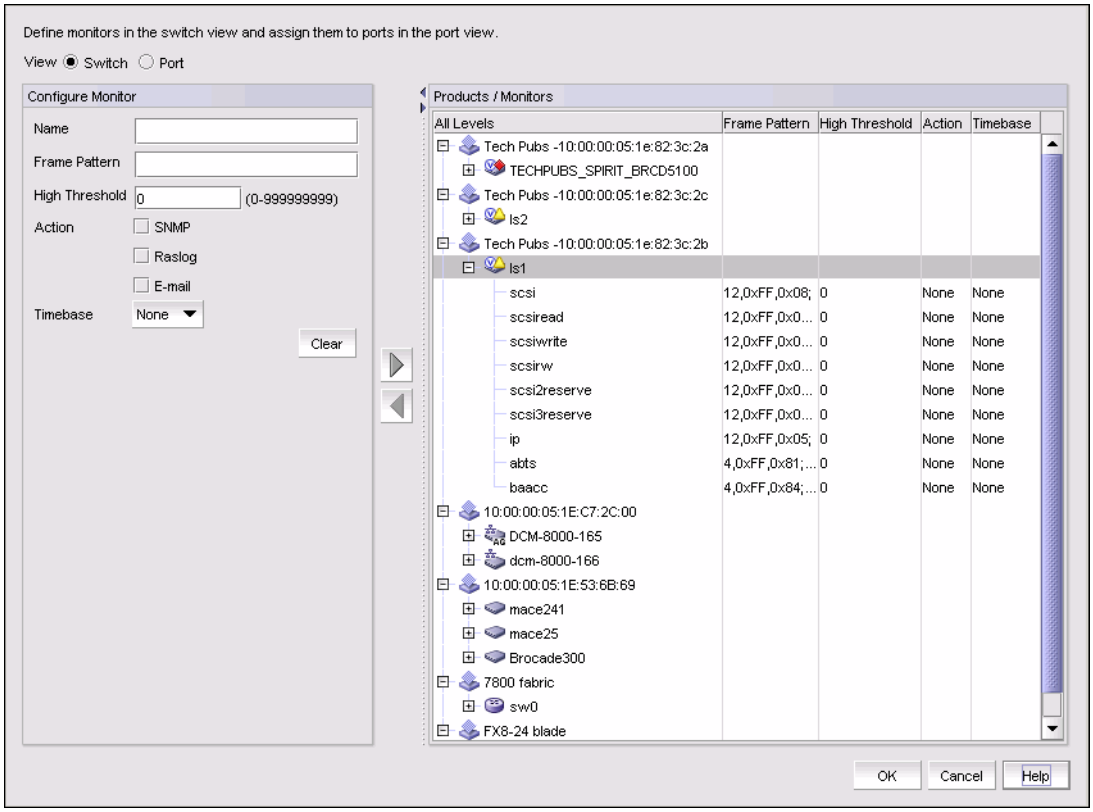


FIGURE 440 Frame Monitor dialog box

2. Select the **Switch** option.

   The Products / Monitors list displays the switches that support Frame Monitoring.

3. Enter the monitor data in the Configure Monitor area.
4. Select one or more switches in the Products / Monitors list, and click the right arrow button to assign the frame monitor to those switches.
5. Select the **Port** option.
6. Expand the switch in the Products / Ports list.

   The Monitors list displays all of the frame monitors defined for that switch.

7. Select one or more ports.

   You must select only ports belonging to the same switch.

8. Select one or more frame monitors in the Monitors list.
9. Click the right arrow button to move the frame monitor to the selected ports.

   The Monitor Details list displays the monitors that are assigned to a selected port. If no monitors are assigned, or if more than one port is selected, the Monitor Details list does not display.

10. Click **OK**.

    The Frame Monitor Configuration Status dialog box displays (Figure 441).

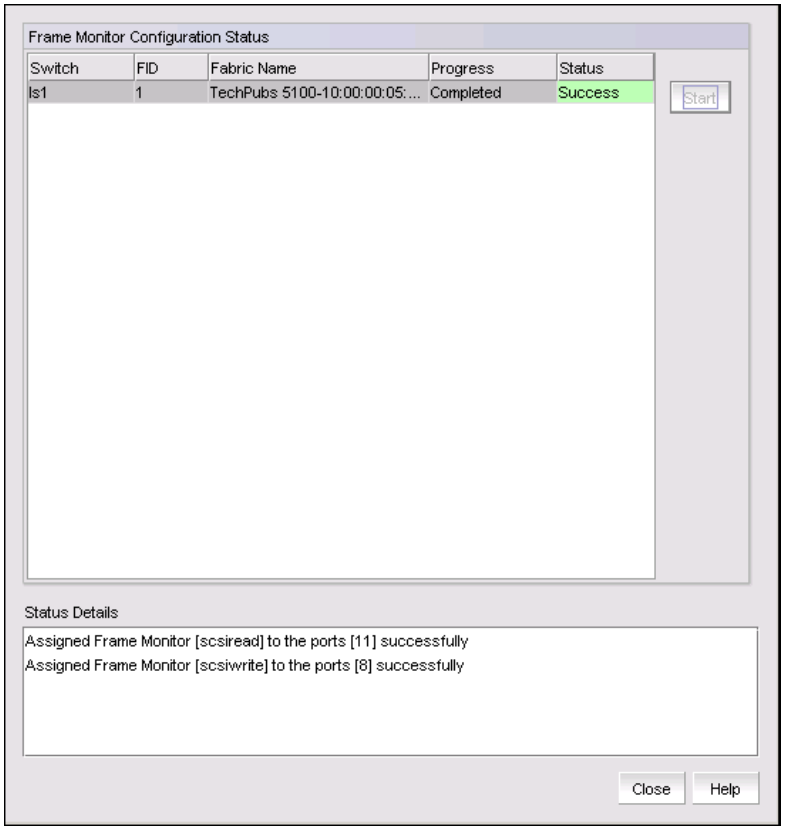


FIGURE 441 Frame Monitor Configuration Status dialog box

11. Click **Start**.

    The frame monitor configuration is applied to the switches.

12. Click **Close** after configuration is complete (indicated by “Completed” in the Progress column).

Editing a frame monitor

1. Select **Monitor > Fabric Watch > Frame Monitor**.

   The Frame Monitor dialog box displays.

2. Select the **Switch** option.
3. Expand the Products / Monitors list to display the frame monitors for each switch.
4. Select a frame monitor and click the left arrow button.

   The frame monitor is removed from the switch and the Configure Monitor area is populated with the values for that frame monitor.

5. Make changes to the monitor data in the Configure Monitor area.
6. Select one or more switches in the Products / Monitors list, and click the right arrow button to assign the frame monitor to those switches.

   If the frame monitor already exists on the switches, the frame monitor is modified. If the frame monitor does not exist on the switch, it is added.

7. Click **OK**.

   The Frame Monitor Configuration Status dialog box displays.

8. Click **Start**.

   The frame monitor configuration is applied to the switches and ports.

9. Click **Close** after configuration is complete (indicated by “Completed” in the Progress column).

Assigning a frame monitor to a port

1. Select **Monitor > Fabric Watch > Frame Monitor**.

   The Frame Monitor dialog box displays.

2. Select the **Port** option.
3. Expand the switch in the Products / Ports list.

   The Monitors list displays all of the frame monitors defined for that switch.

4. Select one or more ports.

   You must select only ports belonging to the same switch.

5. Select one or more frame monitors in the Monitors list.

6. Click the right arrow button to move the frame monitor to the selected ports.

   The Monitor Details list displays the monitors that are assigned to a selected port. If no monitors are assigned, or if more than one port is selected, the Monitor Details list does not display.

7. Click **OK**.

   The Frame Monitor Configuration Status dialog box displays.

8. Click **Start**.

   The frame monitor configuration is applied to the ports.

9. Click **Close** after configuration is complete (indicated by "Completed" in the Progress column).

Finding frame monitor assignments

Using the following procedure, you can select a frame monitor on a switch and see the ports to which it is assigned.

1. Select **Monitor > Fabric Watch > Frame Monitor**.

   The Frame Monitor dialog box displays.

2. Select the **Port** option.
3. Select a switch in the Products / Ports list.

   The Monitors list displays all of the frame monitors defined for that switch.

4. Select a frame monitor in the Monitors list.
5. Click the **Find** arrow.

   The ports to which the frame monitor is assigned are highlighted.

Removing a frame monitor from a port

1. Select **Monitor > Fabric Watch > Frame Monitor**.

   The Frame Monitor dialog box displays.

2. Select the **Port** option.
3. Expand the switch in the Products / Ports list.

   The Monitors list displays all of the frame monitors defined for that switch.

4. Select the port from which you want to remove the frame monitor.

   The Monitor Details list displays all of the frame monitors assigned to that port.

5. Select one or more frame monitors in the Monitor Details list.
6. Click **Remove**.
7. Click **OK**.

   The Frame Monitor Configuration Status dialog box displays.

8. Click **Start**.

   The frame monitor configuration is applied to the ports.

9. Click **Close** after configuration is complete (indicated by “Completed” in the Progress column).

Removing a frame monitor from a switch

When you remove a frame monitor from a switch, the frame monitor is automatically removed from all assigned ports in the switch.

You can remove only custom frame types; you cannot remove the pre-defined frame types.

1. Select **Monitor > Fabric Watch > Frame Monitor**.

   The Frame Monitor dialog box displays.

2. Select the **Switch** option.

   The Products / Monitors list displays the switches that support Frame Monitoring.

3. Expand the Products / Monitors list to display the frame monitors for each switch.
4. Select a frame monitor and click the left arrow button.

   The frame monitor is removed from the switch and the Configure Monitor area is populated with the values for that frame monitor.

5. Click **OK**.

   The Frame Monitor Configuration Status dialog box displays.

6. Click **Start**.

   The frame monitor configuration is applied to the switches and ports.

7. Click **Close** after configuration is complete (indicated by “Completed” in the Progress column).

Chapter

Power Center

35

In this chapter

Power center overview

NOTE
Power over Ethernet (PoE) is only supported on IronWare PoE-capable products.

PoE products enable you to safely pass electrical power, along with data, on Ethernet cabling. The power comes from a power supply within a PoE-capable networking device (such as an Ethernet switch). For more information about PoE, refer to the IronWare Ethernet switch Configuration Guide.

You can use Power Center to perform the following functions on PoE-capable products:

- Determine how much poweris consumed by devices (phones and so on) connected to the product.
- Create power thresholds.
- Monitor power thresholds.
- Power up ports.
- Power down ports.
- Determine PoE capacity.
- Determine PoE allocation.

Data monitoring

Power Center enables you to view PoE data for ports and products in both table and chart formats.

Viewing PoE data for products

To view PoE data for a product, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select **PoE Products** from the **View** list.

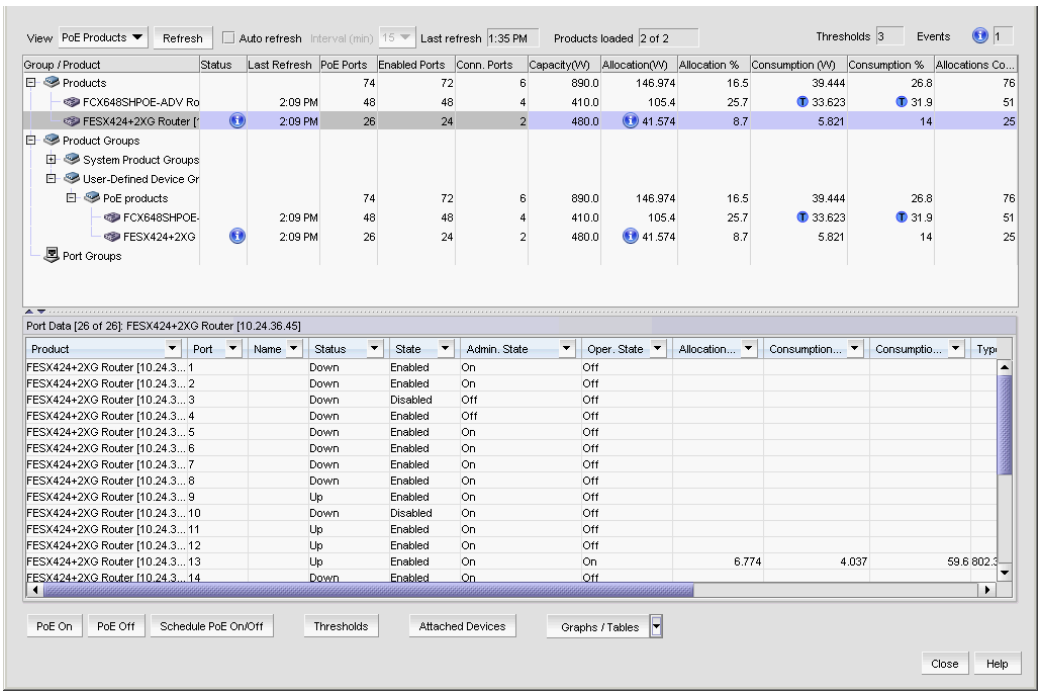


FIGURE 442 Power Center dialog box

3. Review the details in the PoE Products list:

   - **Group/Product** — Lists of the discovered PoE Products, Product Groups, and Ports.
   - **Status** — The threshold status icon for the product.
   - **Last Refresh** — The time of the last data refresh on the product.
   - **PoE Ports** — The number of PoE-capable ports on the product.
   - **Enabled Ports** — The number of PoE-enabled ports on the product.
   - **Conn. Ports** — The number of PoE ports connected to a powered device.
   - **Capacity (W)** — The total PoE capacity of the product in Watts.
   - **Allocation (W)** — The amount ofpower allocated bythe productto the connected devices in Watts. Only displays when the product running agent version 7.2.2 or later. If the product is running a agent version 7.2.1 or earlier, "-" displays.

- **Allocation %** — The percentage of allocated capacity. For example, if the Capacity (W) is 480 W and Allocation (W) is 120 W, then the Allocation percentage is 25. Only displays when the product running agent version 7.2.2 or later. If the product is running a agent version 7.2.1 or earlier, "-" displays.
- **Consumption (W)** — The power consumed by all powered devices connected to the product in Watts.
- **Consumption %** — The current power consumed as a percentage of allocated power.
- **Allocations Count** — The number of times power is allocated to the powered devices. Use this value to determine when a powered device requests multiple power allocations. Only displays when the product running agent version 7.2.2 or later. If the product is running a agent version 7.2.1 or earlier, "-" displays.

4. Click **Close** to close the **Power Center** dialog box.

Viewing PoE data for ports

To view PoE data for a port, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select **PoE Products** from the **View** list.
3. Select a product in the Product list.

   The port data for the selected product displays in the Port Data list.

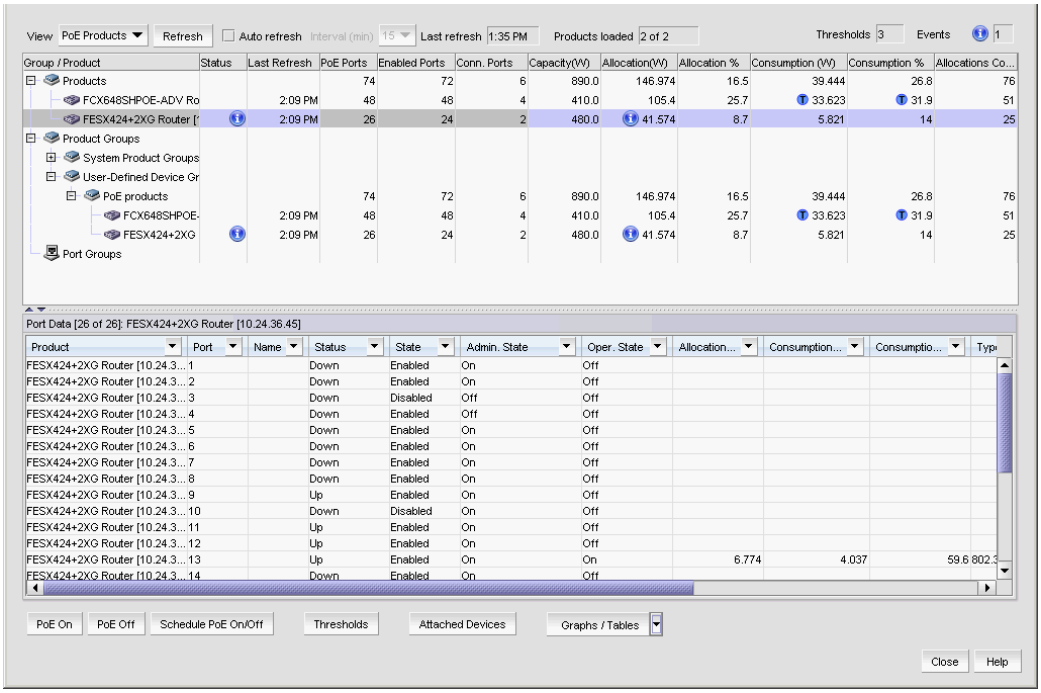


FIGURE 443 Port Data list on the Power Center dialog box

4. Review the details in the Port Data list:
    - **Product filter** — The name of the Product.
    - **Port filter** — The port identifier.
    - **Name filter** — The port name.
    - **Status filter** — The Ethernet status of the port. Values include: Up and Down.
    - **State filter** — The Ethernet state of the port. Values include: Enabled and Disabled.
    - **Admin State filter** — The PoE administrative state of the port. Values include: On (enabled) and Off (disabled).
    - **Oper. State filter** — The PoE operational state of a port. Values include: On (connected to a powered device) and Off (not connected to a powered device).

      NOTE
      The administrative state must be On for operational state to be On.

    - **Allocation (W) filter** — The amount of allocated power to the port in Watts.
    - **Consumption (W) filter** — The power consumed by the device connected to the port in Watts.
    - **Consumption % filter** — The power consumed as a percentage of allocated power.
    - **Type filter** — The type of the device connected to the port. Values include: 802.3af and 802.3at.
    - **Class filter** — The class of the device connected to the port. Values include: Class 0 through Class 4.
    - **Priority filter** — The priority of the device connected to the port. Values include: invalid, critical, high, low, medium, and other.
    - **Mfr. filter** — The manufacturer of the device connected to the port. This information is obtained using LLDP neighbor details command.
    - **Model filter** — The model of the device connected to the port. This information is obtained using LLDP neighbor details command.
    - **Software filter** — The software version on the attached device.
5. Click **Close** to close the **Power Center** dialog box.

Filtering port details

To filter port details, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.
2. Select **PoE Products** from the **View** list.
3. Select a product in the Product list.

   The port data for the selected product displays in the Port Data list.

4. Use the following filters to sort the Port Data list:
   - **Product filter**
   - **Port filter**
   - **Name filter**
   - **Status filter**
   - **State filter**
   - **Admin State filter**
   - **Oper. State filter**

     NOTE
     The administrative state must be On for operational state to be On.

   - **Allocation (W) filter**
   - **Consumption (W) filter**
   - **Consumption % filter**
   - **Type filter**
   - **Class filter**
   - **Priority filter**
   - **Mfr. filter.**
   - **Model filter**
   - **Software filter**
5. Click **Close** to close the **Power Center** dialog box.

Viewing attached device properties

To view properties for devices attached to a product or port, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.
2. Select **PoE Products** from the **View** list.
3. Select a product or port in the Product list and click **Attached Devices**.

   The **Attached Devices** tab of the **Properties** dialog box displays.

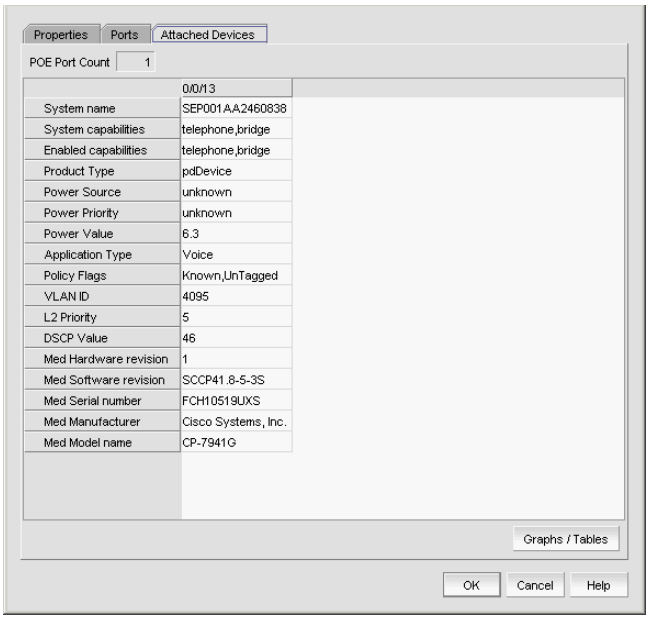


FIGURE 444 Attached Devices tab of the Properties dialog box

4. Review the details in the **Attached Devices** tab:

   - **POE Port Count** — The number of PoE ports, that have power devices which support LLDP, connected to the selected device.
   - **System name** — The system name of the connected device.
   - **System capabilities** — The system capabilities enabled on the remote system.
   - **Enabled capabilties** — The system capabilities enabled on the connected device.
   - **Device Type** — The type of Power-via-MDI (Power over Ethernet) on the remote device.
   - **Power Source** — The type of Power Source on the remote device.
   - **Power Priority** — The priority required by the powered device (PD) connected remotely to the port.
   - **Power Value** — The available power (in Watts) from the Power Sourcing Equipment (PSE) through the port on the remote device.
   - **Application Type** — The primary function of the application for the policy on the connected device.
   - **Policy Flags** — Indicates whether the network policy for the application type is known, as well as whether the application is using a tagged VLAN.
   - **VLAN ID** — The extension of the VLAN Identifier for the remote system connected to the port.
   - **L2 Priority** — The 802.1p priority associated with the remote system connected to the port.
   - **DSCP Value** — The Differentiated Service Code Point (DSCP), as defined in IETF RFC 2474 and RFC 2475, associated with the remote system connected to the port.
   - **Med Hardware revision** — The hardware revision on the connected device.
   - **Med Software revision** — The software revision on the connected device.

- **Med Serial number** — The serial number on the connected device.
- **Med Manufacturer** — The manufacturer name on the connected device.
- **Med Model name** — The model name on the connected device.

5. Click **OK** to close the **Properties** dialog box.
6. Click **Close** to close the **Power Center** dialog box.

Viewing PoE charts

To view a PoE chart, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select **Charts** from the **View** list.
3. Review the Chart data:

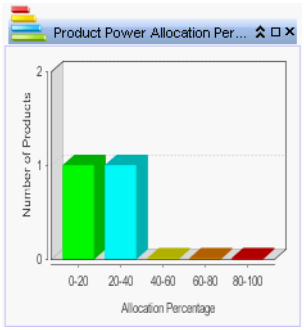


FIGURE 445 Product Power Allocation Percentage bar graph

Displays the power allocation percentages for all products in a bar graph using the following colors:

- 0 – 20 % = Green
- 20 – 40 % = Blue
- 40 – 60 % = Yellow
- 60 – 80 % = Orange
- 80 – 100 % = Red

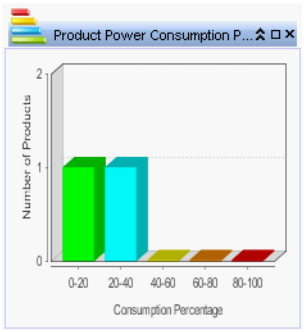


FIGURE 446 Product Power Consumption Percentage bar graph

Displays the power consumption percentages for all products in a bar graph using the following colors:

- 0 – 20 % = Green
- 20 – 40 % = Blue
- 40 – 60 % = Yellow
- 60 – 80 % = Orange
- 80 – 100 % = Red

Click a bar in the chart to display the products panel and highlight the corresponding products.

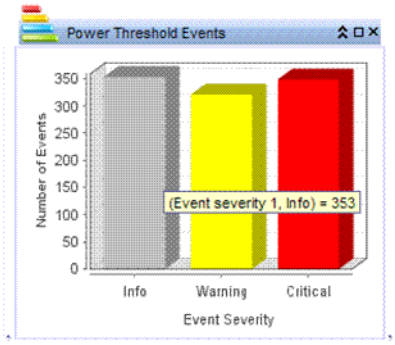


FIGURE 447 Power Threshold Events bar graph

Displays the number of threshold events triggered by severity in a bar graph using the following colors:

- Critical = Red
- Warning = Yellow
- Info = Grey

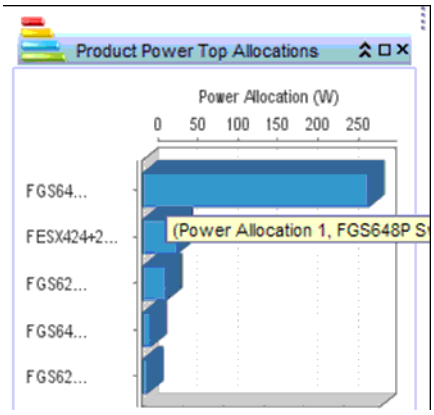


FIGURE 448 Product Power Top Allocations stacked bar graph

Displays the top five products with the highest power allocation values in Watts in a stacked bar graph.

Click a bar in the chart to display the products panel and highlight the corresponding product.

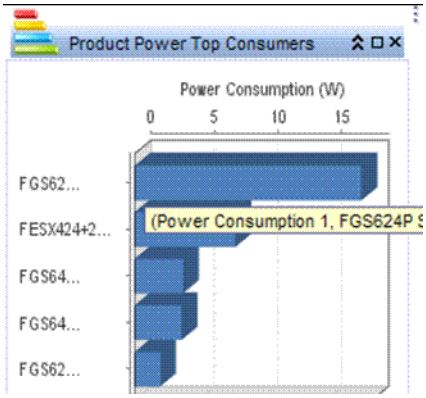


FIGURE 449 Product Power Top Consumers stacked bar graph

Displays the top five products with the highest power consumption values in Watts in a stacked bar graph.

Click a bar in the chart to display the products panel and highlight the corresponding product.

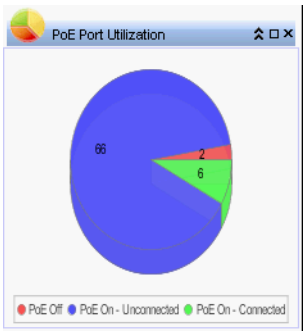


FIGURE 450 PoE Port Utilization pie chart

Displays how many ports with PoE turned on and how many with connected devices in a pie chart using the following colors:

- PoE Off = Red
- PoE On - Unconnected = Blue
- PoE On - Connected = Green

Click the pie chart to display the products panel and highlight the All Products row.

4. Click **Close** to close the **Power Center** dialog box.

Refreshing PoE data

To refresh the PoE data for all products in the **Group/Product** list, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Click **Refresh**.
3. Click **Yes** on the "Are you sure you want to refresh the data of all *n* products?" message.

   The PoE data for all products is updated in the **Power Center** dialog box.

4. Click **Close** to close the **Power Center** dialog box.

To refresh the PoE data for specific products, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select one or more products for which you want to refresh the PoE data in the **Group/Product** list.

   The PoE data for the selected products is updated in the **Power Center** dialog box.

3. Click **Refresh**.
4. Click **Close** to close the **Power Center** dialog box.

Configuring automatic data refresh

To configure automatic refresh the PoE data, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select the **Auto refresh** check box to refresh the data automatically at a specified interval.
3. Select the auto refresh interval from the **Interval (min)** list.

   Options include: 15, 30, or 60.

4. Click **Close** to close the **Power Center** dialog box.

PoE power on demand

You can use the Management application to power up on one or more PoE-capable ports on demand or in a deployment schedule. If you need to periodically power up PoE-capable ports at specific time, you can define a deployment schedule.

Powering up PoE-capable ports on demand

To immediately power up on one or more PoE- capable ports, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select **PoE Products** from the **View** list.

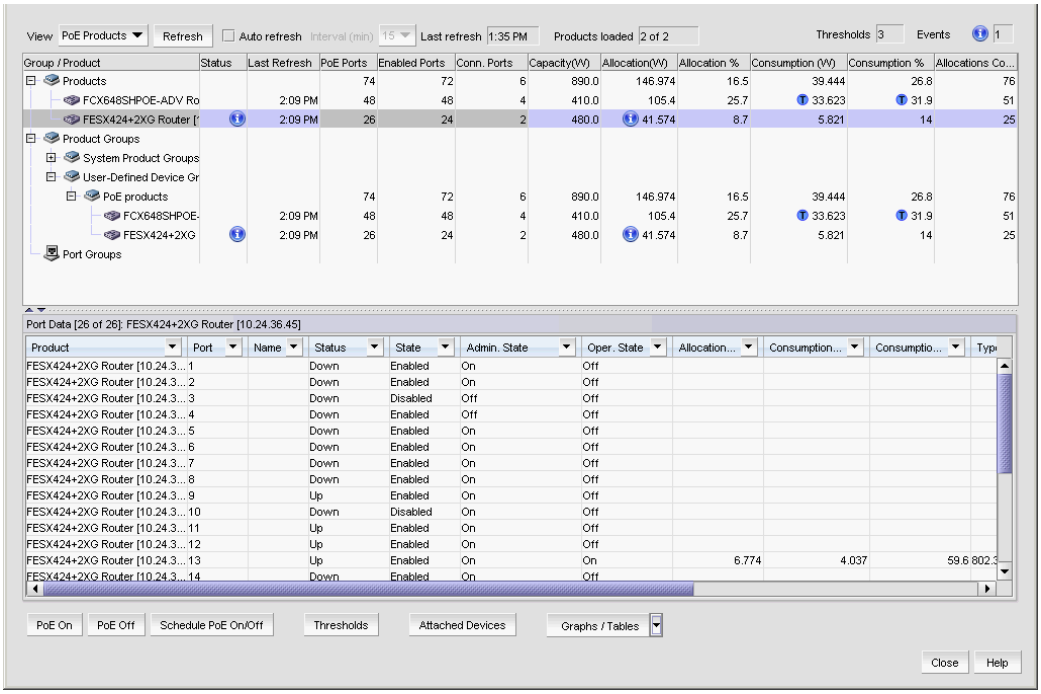


FIGURE 451 **Power Center dialog box**

3. Select a product in the PoE Product list.

   The selected Product's PoE ports display in the Port Data list. The PoE operational state (On or Off) for each port displays in the **Admin State** column.

4. Select one or more ports and click **PoE On**.

5. Click **Yes** on the confirmation message.

   The **Deployment Status** dialog box displays, which allows you to view the progress and status of the deployment.

   Click **Abort** to stop the deployment.

   NOTE
   The abort action does not stop the tasks that have already started.

6. Click **Close** to close the **Deployment Status** dialog box.

   NOTE
   Closing the **Deployment Status** dialog box does not stop deployment.

   The updated PoE operational state of the selected port displays in the **Admin State** column.

7. Click **Close** to close the **Power Center** dialog box.

Powering down PoE-capable ports on demand

To immediately power down on one or more PoE-capable ports, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select **PoE Products** from the **View** list.

3. Select a product in the PoE Product list.

   The PoE-capable ports display in the Port Data list. The PoE operational state (On or Off) of a port displays in the **Admin State** column.

4. Select one or more ports and click **PoE Off**.

5. Click **Yes** on the confirmation message.

   The **Deployment Status** dialog box displays, which allows you to view the progress and status of the deployment.

   Click **Abort** to stop the deployment.

   NOTE
   The abort action does not stop the tasks that have already started.

6. Click **Close** to close the **Deployment Status** dialog box.

NOTE
Closing the **Deployment Status** dialog box does not stop deployment.

The updated PoE operational state of the selected port displays in the **Admin State** column.

7. Click **Close** to close the **Power Center** dialog box.

Schedule PoE power deployment

You can define a deployment schedule on a port, product, port group, or product group. However, when you schedule a deployment on a product, port group, or product group, the schedule is only configured on the ports present when you create the schedule. If you add ports to the productor products to the product group, the deployment schedule is not configured on the new ports. To configure the deployment schedule on the new ports, refer to *"Updating a power deployment schedule"* on page 1083.

Scheduling an power up deployment

To schedule a power up deployment, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select **PoE Products** from the **View** list.

3. Select a port, product, port group, or product group in the PoE Product list and click **Schedule PoE On/Off**.

   The **Schedule PoE On/Off** dialog box displays.

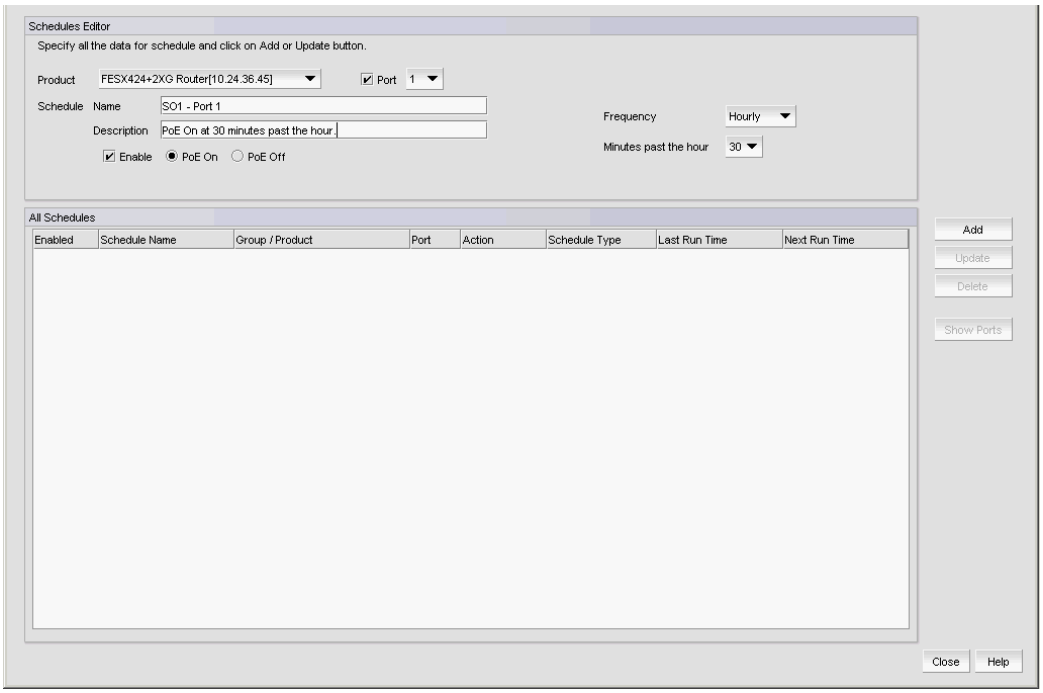


FIGURE 452 Schedule PoE On/Off dialog box

4. (Ports only) Select a port from the **Port** list.
5. Enter a name for the schedule in the **Schedule Name** field.
6. Enter a description for the schedule in the **Description** field.
7. Select the **Enable** check box to enable the schedule.
8. Select the **PoE On** option to enable PoE.
9. Choose one of the following options to configure the frequency at which deployment runs for the schedule:
   - To configure deployment to run only once, refer to "Configuring a one-time deployment schedule" on page 1079.
   - To configure hourly deployment, refer to "Configuring an hourly deployment schedule" on page 1079.
   - To configure daily deployment, refer to "Configuring a daily deployment schedule" on page 1080.
   - To configure weekly deployment, refer to "Configuring a weekly deployment schedule" on page 1080.
   - To configure monthly deployment, refer to "Configuring a monthly deployment schedule" on page 1081.
   - To configure yearly deployment, refer to "Configuring a yearly deployment schedule" on page 1081.
10. Click **Add**.
11. Click **Close** to close the **Schedule PoE On/Off** dialog box.
12. Click **Close** to close the **Power Center** dialog box.

Configuring a one-time deployment schedule

To configure a one-time schedule, complete the following steps.

1. Select **One Time** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
3. Click the **Date** list to select a date from the calendar.

   To finish configuring the deployment schedule, return to one of the following procedures:

   - To configure an power on PoE schedule, refer to step 10 of "Scheduling an power up deployment" on page 1077.
   - To configure an power off PoE schedule, refer to step 10 of "Scheduling a power down deployment" on page 1082.
   - To update a PoE schedule, refer to step 10 of "Updating a power deployment schedule" on page 1083

Configuring an hourly deployment schedule

To configure an hourly schedule, complete the following steps.

1. Select **Hourly** from the **Frequency** list.
2. Select the minute past the hour you want deployment to run from the **Minutes past the hour** list.

   Where the minute value is from 00 through 59.

   To finish configuring the deployment schedule, return to one of the following procedures:

   - To configure an enable PoE schedule, refer to step 10 of "Scheduling an power up deployment" on page 1077.
   - To configure an disable PoE schedule, refer to step 10 of "Scheduling a power down deployment" on page 1082.
   - To update a PoE schedule, refer to step 10 of "Updating a power deployment schedule" on page 1083

Configuring a daily deployment schedule

To configure a daily deployment schedule, complete the following steps.

1. Select **Daily** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

   To finish configuring the deployment schedule, return to one of the following procedures:

   - To configure an enable PoE schedule, refer to step 10 of "Scheduling an power up deployment" on page 1077.
   - To configure an disable PoE schedule, refer to step 10 of "Scheduling a power down deployment" on page 1082.
   - To update a PoE schedule, refer to step 10 of "Updating a power deployment schedule" on page 1083

Configuring a weekly deployment schedule

To configure a weekly schedule, complete the following steps.

1. Select **Weekly** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Select the day you want deployment to run from the **Day of the Week** list.

   To finish configuring the deployment schedule, return to one of the following procedures:

   - To configure an enable PoE schedule, refer to step 10 of "Scheduling an power up deployment" on page 1077.
   - To configure an disable PoE schedule, refer to step 10 of "Scheduling a power down deployment" on page 1082.
   - To update a PoE schedule, refer to step 10 of "Updating a power deployment schedule" on page 1083

Configuring a monthly deployment schedule

To configure a monthly schedule, complete the following steps.

1. Select **Monthly** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
3. Select the day you want deployment to run from the **Day of the Month** list (1 through 31).

   To finish configuring the deployment schedule, return to one of the following procedures:

   - To configure an enable PoE schedule, refer to step 10 of "Scheduling an power up deployment" on page 1077.
   - To configure an disable PoE schedule, refer to step 10 of "Scheduling a power down deployment" on page 1082.
   - To update a PoE schedule, refer to step 10 of "Updating a power deployment schedule" on page 1083

Configuring a yearly deployment schedule

To configure a yearly schedule, complete the following steps.

1. Select **Yearly** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
3. Click the **Date** list to select a date from the calendar.

   To finish configuring the deployment schedule, return to one of the following procedures:

   - To configure an enable PoE schedule, refer to step 10 of "Scheduling an power up deployment" on page 1077.
   - To configure an disable PoE schedule, refer to step 10 of "Scheduling a power down deployment" on page 1082.
   - To update a PoE schedule, refer to step 10 of "Updating a power deployment schedule" on page 1083

Scheduling a power down deployment

To schedule a power down deployment on one or more PoE-capable ports, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select **PoE Products** from the **View** list.
3. Select a port, product, port group, or product group in the PoE Product list and click **Schedule PoE On/Off**.

   The **Schedule PoE On/Off** dialog box displays.

4. (Ports only) Select a port from the **Port** list.
5. Enter a name for the schedule in the **Schedule Name** field.
6. Enter a description for the schedule in the **Description** field.
7. Select the **Enable** check box to enable the schedule.
8. Select the **PoE Off** option.
9. Choose one of the following options to configure the frequency at which deployment runs for the schedule:
   - To configure deployment to run only once, refer to "Configuring a one-time deployment schedule" on page 1079.
   - To configure hourly deployment, refer to "Configuring an hourly deployment schedule" on page 1079.
   - To configure daily deployment, refer to "Configuring a daily deployment schedule" on page 1080.
   - To configure weekly deployment, refer to "Configuring a weekly deployment schedule" on page 1080.
   - To configure monthly deployment, refer to "Configuring a monthly deployment schedule" on page 1081.
   - To configure yearly deployment, refer to "Configuring a yearly deployment schedule" on page 1081.
10. Click **Add**.
11. Click **Close** to close the **Schedule PoE On/Off** dialog box.
12. Click **Close** to close the **Power Center** dialog box.

Updating a power deployment schedule

To update a power deployment on one or more PoE-capable ports, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select **PoE Products** from the **View** list.

3. Select a port, product, port group, or product group in the PoE Product list and click **Schedule PoE On/Off**.

   The **Schedule PoE On/Off** dialog box displays.

4. Select the schedule you want to update from the **All Schedules** list.

   If you need to make changes to the deployment schedule, continue with step 5.

   If new PoE-capable ports have been added to the product or group for which this deployment is configure, go to step 10.

5. (Ports only) Select a port from the **Port** list.

6. Change the name for the schedule in the **Schedule Name** field.

7. Change the description for the schedule in the **Description** field.

8. Select the **Enable** check box to enable the schedule.

9. Choose one of the following options to configure the frequency at which deployment runs for the schedule:

   - To configure deployment to run only once, refer to "Configuring a one-time deployment schedule" on page 1079.
   - To configure hourly deployment, refer to "Configuring an hourly deployment schedule" on page 1079.
   - To configure daily deployment, refer to "Configuring a daily deployment schedule" on page 1080.
   - To configure weekly deployment, refer to "Configuring a weekly deployment schedule" on page 1080.
   - To configure monthly deployment, refer to "Configuring a monthly deployment schedule" on page 1081.
   - To configure yearly deployment, refer to "Configuring a yearly deployment schedule" on page 1081.

10. Click **Update**.

11. Click **Close** to close the **Schedule PoE On/Off** dialog box.

12. Click **Close** to close the **Power Center** dialog box.

Viewing the configured ports for a power deployment schedule

To view all ports to which a power deployment schedule is configured, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select **PoE Products** from the **View** list.

3. Select a port, product, port group, or product group in the PoE Product list and click **Schedule PoE On/Off**.

   The **Schedule PoE On/Off** dialog box displays.

4. Select the schedule for which you want to view the configured ports from the **All Schedules** list.

5. Click **Show Ports**.

   The **Scheduled Ports** [*Schedule_Name*] dialog box displays.

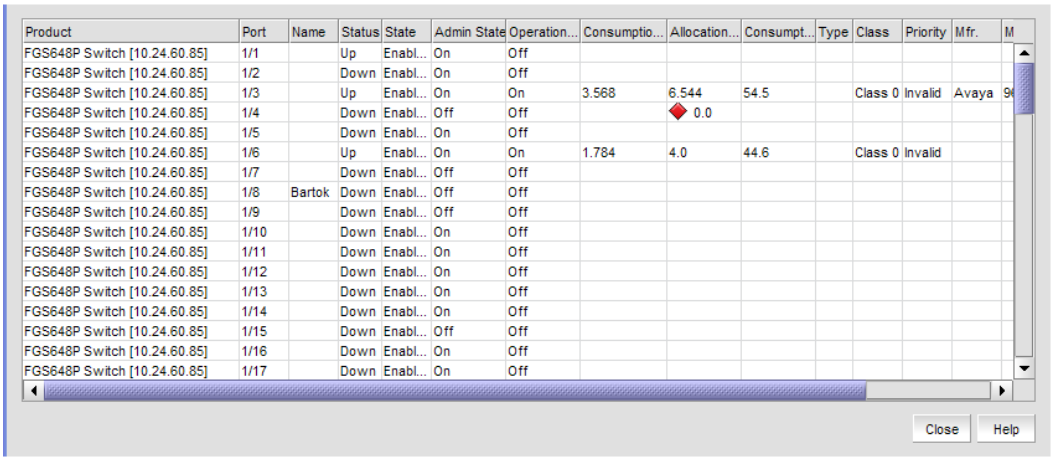


FIGURE 453 Scheduled Ports [*Schedule_Name*] dialog box

6. Review the following information:

   - **Product** — The name of the Product.
   - **Port** — The port identifier.
   - **Name** — The port name.
   - **Status** — The Ethernet status of the port. Values include: Up and Down.
   - **State** — The Ethernet state of the port. Values include: Enabled and Disabled.
   - **Admin State** — The PoE administrative state of the port. Values include: On (enabled) and Off (disabled).
   - **Oper. State** — The PoE operational state of a port. Values include: On (connected to a powered device) and Off (not connected to a powered device).

     NOTE
     The administrative state must be On for operational state to be On.

   - **Allocation (W)** — The amount of allocated power to the port in Watts.
   - **Consumption (W)** — The power consumed by the device connected to the port in Watts.

- **Consumption %** — The power consumed as a percentage of allocated power.
- **Type** — The type of the device connected to the port. Values include: 802.3af and 802.3at.
- **Class** — The class of the device connected to the port. Values include: Class 0 through Class 4.
- **Priority** — The priority of the device connected to the port. Values include: invalid, critical, high, low, medium, and other.
- **Mfr.**. — The manufacturer of the device connected to the port. This information is obtained using LLDP neighbor details command.
- **Model** — The model of the device connected to the port. This information is obtained using LLDP neighbor details command.
- **Software** — The software version on the attached device.

7. Click **Close** to close the **Scheduled Ports** [*Schedule_Name*] dialog box.
8. Click **Close** to close the **Schedule PoE On/Off** dialog box.
9. Click **Close** to close the **Power Center** dialog box.

Deleting a power deployment schedule

To delete a power deployment schedule, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select **PoE Products** from the **View** list.
3. Select a port, product, port group, or product group in the PoE Product list and click **Schedule PoE On/Off**.

   The **Schedule PoE On/Off** dialog box displays.

4. Select the schedule you want to delete from the **All Schedules** list.

   To delete more than one deployment schedule, press Ctrl and click each schedule you want to delete.

5. Click **Delete**.
6. Click **Yes** on the confirmation message.
7. Click **Close** to close the **Schedule PoE On/Off** dialog box.
8. Click **Close** to close the **Power Center** dialog box.

PoE thresholds

Power Center enables you to define a threshold on a product or port. You cannot define a threshold on a product group or port group.

You can define Product thresholds using the following measures:

- PoE Capacity — The total PoE capacity of the product in Watts.

  NOTE
  PoE capacity requires the product to be running agent version 7.2.2 or later.

- PoE Allocation — The amount of allocated power to the product in Watts.
- Allocation % — The percentage of available capacity.

  NOTE
  PoE capacity requires the product to be running agent version 7.2.2 or later.

- Consumption % — The current power consumed as a percentage of allocated power.
- Allocations Count — The number of times power is allocated to the powered devices. Use this value to determine when a powered device requests multiple power allocations.

  NOTE
  Allocations Count requires the product to be running agent version 7.2.2 or later.

You can define Port thresholds using the following measures:

- Port allocation — The amount of allocated power to the port in Watts.
- Port consumption — The amount of allocated power to the port in Watts.
- Port consumption % — The power consumed as a percentage of allocated power

Adding a PoE product threshold

To create a threshold for a PoE product, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select a product in the PoE Product list and click **Thresholds**.

   The **Thresholds** dialog box displays.

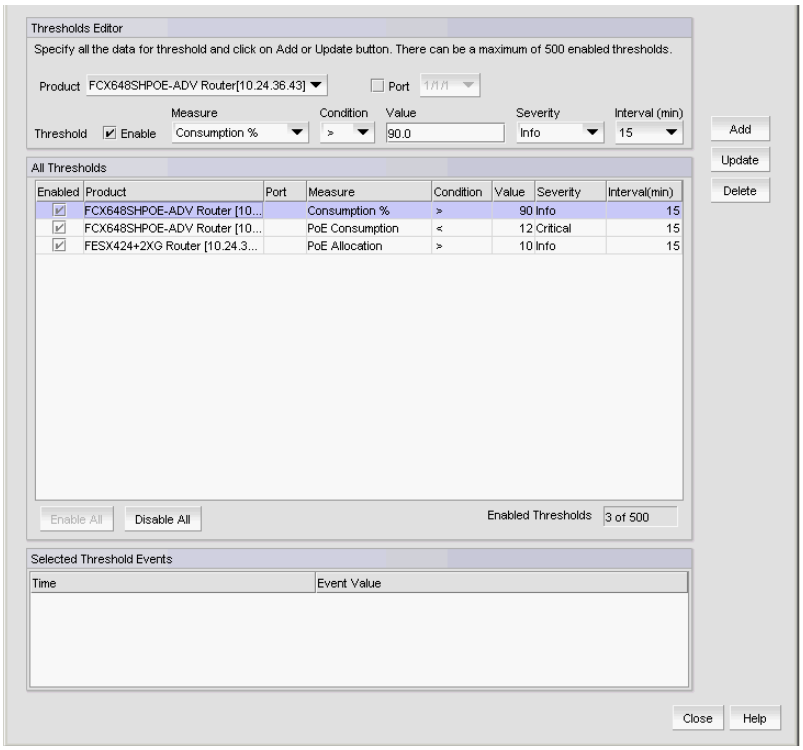


FIGURE 454 Thresholds dialog box

3. Choose one of the following measures:
   - **PoE Capacity** (The product must be running agent version 7.2.2 or later.)
   - **PoE Allocation**
   - **Allocation %** (The product must be running agent version 7.2.2 or later.)
   - **PoE Consumption**
   - **Consumption %**
   - **Allocations Count** (The product must be running agent version 7.2.2 or later.)
4. Select one of the following from the **Conditions** list:
   - >
   - <
   - ==
5. Enter the number of events that must be generated to trigger the threshold event in the **Value** field.

   The value should not exceed the capacity of the product.

   If you select a percentage measure, the value should be less than or equal to 100.
6. Select the severity level for the threshold event from the Severity list.
   - Info
   - Warning
   - Critical

7. Select the time period to be monitored for the number of threshold events in the Interval (min) list.

   The time period starts with the first event and runs its full duration if the event limit is not reached. Interval values, in minutes, include:

   - 15
   - 30
   - 60

   Click **Refresh** on the **Power Center** dialog box to determine if any thresholds are triggered.

8. Click **Add**.

   The new threshold displays in the **All Thresholds** list.

9. Select the **Enabled** check box of the new threshold in the **All Thresholds** list to enable the threshold on the product.

10. Click **Close** to close the **Thresholds** dialog box.

11. Click **Close** to close the **Power Center** dialog box.

Adding a PoE port threshold

To create a threshold for a PoE port, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select a port in the PoE Product list and click **Thresholds**.

   The **Thresholds** dialog box displays.

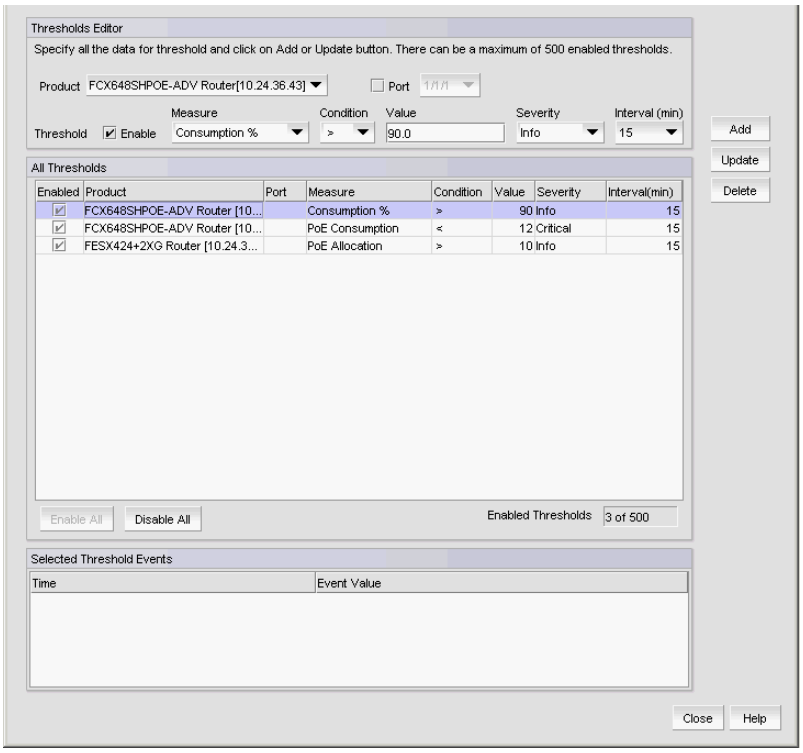


FIGURE 455 Thresholds dialog box

3. Choose one of the following measures:
   - **Port allocation**
   - **Port consumption**
   - **Port consumption %**
4. Select one of the following from the **Conditions** list:
   - >
   - <
   - ==
5. Enter the number of events that must be generated to trigger the threshold event in the **Value** field.

   The value should not exceed the capacity of the product.

   If you select a percentage measure, the value should be less than or equal to 100.
6. Select the severity level for the threshold event from the Severity list.
   - Info
   - Warning
   - Critical

7. Select the time period to be monitored for the number of threshold events in the Interval (min) list.

   The time period starts with the first event and runs its full duration if the event limit is not reached. Interval values, in minutes, include:

   - 15
   - 30
   - 60

8. Click **Add**.

   The new threshold displays in the **All Thresholds** list.

9. Select the **Enabled** check box of the new threshold in the **All Thresholds** list to enable the threshold on the product.
10. Click **Close** to close the **Thresholds** dialog box.
11. Click **Refresh** on the **Power Center** dialog box to determine if any thresholds are triggered.
12. Click **Close** to close the **Power Center** dialog box.

Viewing PoE thresholds

To view PoE thresholds, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select a product in the PoE Product list and click **Thresholds**.

   The **Thresholds** dialog box displays with the thresholds defined for that product.

3. Review the following information in the **All Threshold** list.

   - **Enabled** check box — Checked when the threshold is enabled. Clear when the threshold is disabled.
   - **Product** — The Product for which the threshold is configured.
   - **Port** — The Port for which the threshold is configured.
   - **Measure** — The power measure on which you defined the threshold condition.
   - **Condition** — The condition you defined for the threshold.
   - **Value** — The value you defined for the threshold.
   - **Severity** — The severity you defined for the threshold.
   - **Interval (min)** — The time period in minutes you defined for the threshold.
   - **Enabled Threshold** — The number of enabled thresholds.

4. Select a threshold in the **All Threshold** list to review the following information in the **Selected Threshold Events** list.

   - **Time** — The date and time that the event was triggered.
   - **Event Value** — The value of the triggered event.

5. Click **Close** to close the **Thresholds** dialog box.
6. Click **Close** to close the **Power Center** dialog box.

Updating a PoE threshold

To update a PoE threshold, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select a product in the PoE Product list and click **Thresholds**.

   The **Thresholds** dialog box displays with the thresholds defined for that product.

3. Select the threshold you want to edit in the **All Thresholds** list.

   The selected threshold displays in the **Thresholds Editor** area.

4. Select the **Enabled** check box to enable the threshold on the product.

5. Choose one of the following measures:

   - **Port allocation**
   - **Port consumption**
   - **Port consumption %**

6. Select one of the following from the **Conditions** list:

   - >
   - <
   - ==

7. Enter the number of events that must be generated to trigger the threshold event in the **Value** field.

   The value should not exceed the capacity of the product.

   If you select a percentage measure, the value should be less than or equal to 100.

8. Select the severity level for the threshold event from the Severity list.

   - Info
   - Warning
   - Critical

9. Select the time period to be monitored for the number of threshold events in the Interval (min) list.

   The time period starts with the first event and runs its full duration if the event limit is not reached. Interval values, in minutes, include:

   - 15
   - 30
   - 60

10. Click **Update**.

    The updated threshold displays in the **All Thresholds** list.

11. Click **Close** to close the **Thresholds** dialog box.

12. Click **Refresh** on the **Power Center** dialog box to determine if any thresholds are triggered.
13. Click **Close** to close the **Power Center** dialog box.

Enabling PoE thresholds

To enable PoE thresholds, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select a product in the PoE Product list and click **Thresholds**.

   The **Thresholds** dialog box displays with the thresholds defined for that product.

3. Choose one of the following options:

   - Click **Enable All** to enable all thresholds in the list.
   - Select a threshold in the **All Thresholds** list, select the **Enabled** check box in the **Thresholds Editor** area, and click **Update** to enable the threshold on the product.

4. Click **Close** to close the **Thresholds** dialog box.
5. Click **Close** to close the **Power Center** dialog box.

Disabling PoE thresholds

To disable PoE thresholds, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select a product in the PoE Product list and click **Thresholds**.

   The **Thresholds** dialog box displays with the thresholds defined for that product.

3. Choose one of the following options:

   - Click **Disable All** to disable all thresholds in the list.
   - Select a threshold in the **All Thresholds** list, clear the **Enabled** check box in the **Thresholds Editor** area, and click **Update** to disable the threshold on the product.

4. Click **Close** to close the **Thresholds** dialog box.
5. Click **Close** to close the **Power Center** dialog box.

Deleting PoE thresholds

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select a product in the PoE Product list and click **Thresholds**.

   The **Thresholds** dialog box displays with the thresholds defined for that product.

3. Select the threshold you want to delete and click **Delete**.

   Select more than one threshold to delete by pressing Ctrl and clicking each threshold you want to delete.

4. Click **Close** to close the **Thresholds** dialog box.

5. Click **Close** to close the **Power Center** dialog box.

Viewing PoE performance

To view PoE performance, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select one of the following from the **Graphs/Tables** list.

   - **Real Time Power Graphs/Tables** — Select to show power-related information in a real-time graph or table. Refer to IP Real time performance monitoring.
   - **Real Time Performance Graphs/Tables** — Select to show performance-related information in a real-time graph or table. Refer to "IP real-time performance monitoring" on page 983.
   - **Historical Performance Graphs/Tables** — Select to show performance-related historical information in a historical graph or table. Refer to "IP historical performance monitoring" on page 995.

   The **Select Sources** dialog box displays.

3. Click **Close** to close the **Power Center** dialog box.

Monitoring real time power performance on products

To view real time power performance graphs or tables, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select a product from the Product list.

3. Select **Real Time Power Graphs/Tables** from the **Graphs/Tables** list.

   The **Real Time Power Graphs/Tables** dialog box displays.

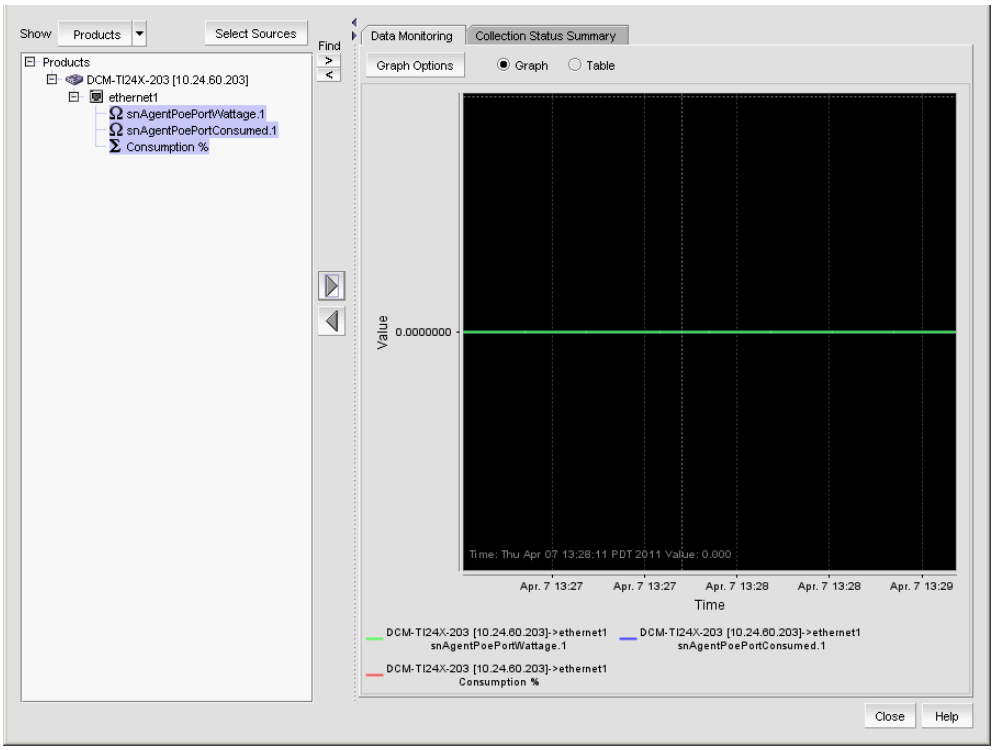


FIGURE 456 Real Time Power Graphs/Tables dialog box

4. Select the measures you want to include and click the right arrow button to display it on the **Data Monitoring** tab.

   Product power measures include the following:

   - Allocation (W)
   - Allocation %

5. Click the **Data Monitoring** tab to view a performance monitoring graph or table.

   - Click the **Graph** option to view a performance graph.

     The legend under the graph shows what data each color represents. To configure graph options, refer to "Configuring the performance graph" on page 989.

   - Click the **Table** option to view a performance table.

     The first column displays the time of the collection. The remaining columns display the value of each collectible at the specified time. There is one column for every collectible you selected to display.

6. Click the **Collection Status Summary** tab to view the following information:

   The **Collection Status Summary** tab provides a high level overview of all defined collectors. The information is displayed in the following columns:

   - **Product** - Shows the product name and IP address. There maybe multiple instances of the product name for each collectible assigned to the product.
   - **Port** - The port name when a port is selected.
   - **Collectible** - The MIB objects and expressions used by the data collector.
   - **Status** - The status field uses the following icons.

     
     Failed. No value was ever collected for this collectible.

     
     Warning: Data collection failed in the last polling cycle.

     
     Successful: Last collection successful.

     
     Scheduled but not currently active.

   - **Last Value** - The last (most current) value collected.
   - **Last Time Polled** - The time that the collector was last polled.

7. Click **Select Sources** to add product and ports to or remove product and ports from real time power performance monitoring. Refer to "Adding products and ports to real-time performance" on page 985 and "Removing products and ports from real-time performance" on page 985.
8. Click **Close** to close the dialog box.

Monitoring real time power performance on ports

To view real time power performance graphs or tables, complete the following steps.

1. Select **Monitor > Power Center**.

   The **Power Center** dialog box displays.

2. Select a a port from the Port Data list.

3. Select **Real Time Power Graphs/Tables** from the **Graphs/Tables** list.

   The **Real Time Power Graphs/Tables** dialog box displays.

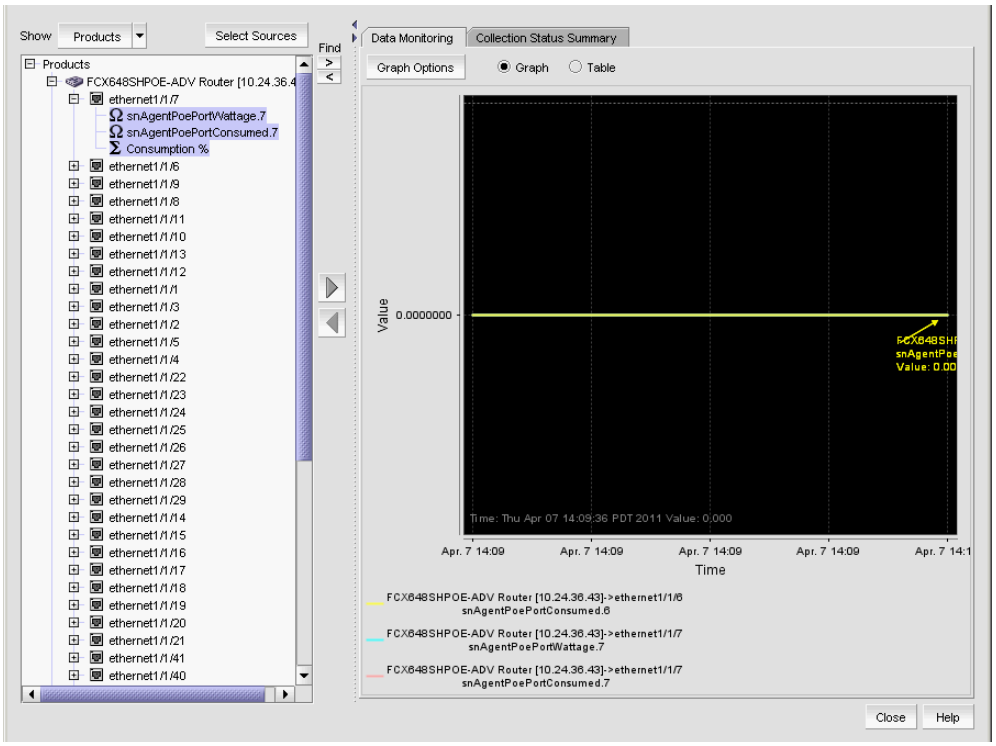


FIGURE 457 Real Time Power Graphs/Tables dialog box

4. Select the measures you want to include and click the right arrow button to display it on the **Data Monitoring** tab.

   Port power measures include the following:

   - Allocation (W) — snAgentPoePortWattage
   - Consumption (W) — snAgentPoePortConsumed
   - Consumption %

5. Click the **Data Monitoring** tab to view a performance monitoring graph or table.
   - Click the **Graph** option to view a performance graph.

     The legend under the graph shows what data each color represents. To configure graph options, refer to "Configuring the performance graph" on page 989.
   - Click the **Table** option to view a performance table.

     The first column displays the time of the collection. The remaining columns display the value of each collectible at the specified time. There is one column for every collectible you selected to display.
6. Click the **Collection Status Summary** tab to view the following information:

   The **Collection Status Summary** tab provides a high level overview of all defined collectors. The information is displayed in the following columns:
   - **Product** - Shows the product name and IP address. There maybe multiple instances of the product name for each collectible assigned to the product.
   - **Port** - The port name when a port is selected.
   - **Collectible** - The MIB objects and expressions used by the data collector.
   - **Status** - The status field uses the following icons.

     
     Failed. No value was ever collected for this collectible.

     
     Warning: Data collection failed in the last polling cycle.

     
     Successful: Last collection successful.

     
     Scheduled but not currently active.
   - **Last Value** - The last (most current) value collected.
   - **Last Time Polled** - The time that the collector was last polled.
7. Click **Select Sources** to add product and ports to or remove product and ports from real time power performance monitoring. Refer to "Adding products and ports to real-time performance" on page 985 and "Removing products and ports from real-time performance" on page 985.
8. Click **Close** to close the dialog box.

Chapter

Policy Monitor

36

In this chapter

Policy monitor overview

Use the Policy Monitor feature to provide best practice guidelines for network setup at the fabric, switch, port, and device level, as well as software configurations at the Fabric OS, Ironware, Network OS, and the Management application level.

Configuring policy monitors enables you to perform the following:

- Provide selectable and configurable built-in rules to check for best practices
- Schedule policies to run periodically
- Run a policy manually (on demand)
- Generate a report that will detail any issues found by the policy

Fabric policy monitors

Fabric policy monitors enable you to set the following policy monitors on Ethernet fabrics (refer to "Adding a policy monitor" on page 1108):

- **Check zoning status —** This fabric policy monitor enables you to determine if zoning is enabled or disabled on the fabric.

  Zoning plays a key role in the management of device communication. When you enforce zoning, devices not in the same zone cannot communicate. Zoning provides protection from disruption in the fabric (putting bounds on the scope of RSCNs). The best practice is always to enable zoning.

  Rule Violation Fix — If the policy monitor report shows a violation, the Administrator can use the **Zoning** dialog box (**Configure > Zoning > Fabric**) to fix the violation. Refer to "Zoning" on page 637.

  For example, if you use the policy monitor to make sure that the zoning status is enabled, you can fix the violation through the **Zoning** dialog box by locating the target fabric, defining a zone configuration, and activating the zone configuration.

- **Check that all zones belong to at least one zone config —** This fabric policy monitor enables you to determine if there are any orphaned zones in the fabric zone database.

  Too many orphaned zones can fill up the fabric zone database and complicate other ongoing administrative tasks.

  Rule Violation Fix — If the policy monitor report shows a violation, the Administrator can use the **Zoning** dialog box (**Configure > Zoning > Fabric**) to fix the violation. Refer to "Zoning" on page 637.

  For example, the Administrator can fix the violation through the **Zoning** dialog box using one of the following methods:

  - Defining a new zone configuration and moving the orphaned zones to the new zone configuration.
  - Moving the orphaned zones to an existing zone configuration.
  - Cleaning up unused orphaned zones.

- **Check the number of initiator ports zoned to each storage port —** This fabric policy monitor enables you to determine the total number of initiator ports zoned to each storage port.

  When too many initiators share the same connection (share the bandwidth of the storage port), congestion can occur.

  There are four possible zone member types: device port WWN, device node WWN, (D,I), and Fabric Assigned WWN.

  - Device port WWN — The application counts the connected device ports and uses them for the ratio calculation.
  - Device node WWN zone member — The application finds the corresponding device ports and uses them for the ratio calculation.
  - D,I — If the switch port is connected to a device, the application finds the connected device ports and uses them for the ratio calculation.
  - Fabric Assigned WWN — If the switch or Access Gateway (AG) port has a connected device port, the application finds the connected device ports and uses them for the ratio calculation.

Some devices can function as both initiator and target. If the application finds this type of device as one of the active zone members, this device port is treated as both initiator and target:

- Target (storage port) — The application counts the number of initiator ports zoned to this storage port.
- Initiator — The application counts this device as an initiator port for other storage ports in the same zone.

Rule Violation Fix — If the policy monitor report shows a violation, the Administrator must make sure the initiator port limit is under the recommended number.

- **Check zones that do not contain any online member —** This fabric policy monitor enables you to identify zones in which all zone members are offline.

NOTE
The application does not count end devices which are missing from the fabric and D,PI zone members (online or offline) as online zone members. The application only counts zones with online WWN members as online zone members.

Rule Violation Fix — If the policy monitor report shows a violation, you can use the **Zoning** dialog box (**Configure > Zoning > Fabric**) to bring the devices back online (refer to "Zoning" on page 637).

For example, if you use the policy monitor to determine when all WWN members in a zone are offline, you can fix the violation through the **Zoning** dialog box by locating the target fabric and bringing the devices back online.

- **Check that all profiles are the same on each RBridge in an Ethernet fabric** — This fabric policy monitor enables you to determine if all RBridge profiles in a Ethernet fabric are the same. The first check is to determine if the name matches. If the name matches, policy monitor checks the other profile content (such as VLAN, QoS, and Security), and then the MAC associations.

  A port profile is a collection of network policies supported by the switch. By configuring port profiles on the VDX switch, the virtual machine (VM) that is configured on the virtual network interface card (vNIC) can migrate to any other port on that switch, but still retain the same network policies.

  Use this check during VM migration to make sure that the migrated VM behaves the same way on the next host.

  Rule Violation Fix — If the policy monitor report shows a violation, compare the port profiles (refer to "Comparing port profiles" on page 437) to find the mismatches and then fix the discrepancies.

Switch and router policy monitors

Switch and router policy monitors enable you to set the following policy monitors on switches and routers.

- **Check for HTTPS (secure HTTP) configuration** — This switch and router policy monitor enables you to check each target to see if HTTPS is active for device data transmission.

  NOTE
  Not supported on Network OS products and the following IronWare products: Ethernet Core routers, Ethernet Carrier Routers, Ethernet Edge router, and Data Center switch, as well as the 6650 Ethernet switch, router, and L3 router.

  The preferred Management application product communication must be HTTPS for this check to pass.

  Rule Violation Fix — If the policy monitor report shows a violation, enable HTTPS on the device. Disable HTTP settings on the device, if enabled.

- **Check if the product is configured to send events to this server** — This switch and router policy monitor enables you to determine if the Management application server is registered as an SNMP recipient and Syslog recipient.

  If the server has multiple NICs, the server uses an IP address reachable from the switch for event registration. This policy cannot determine if the server is using a reachable IP address for the event registration.

  If the Management application server fails to register as a listener for SNMP, Syslog, and other events, the Management application server cannot notify you of changes to the fabric or device. If a fabric or switch fails, the Management application cannot provide notification, log, or support data. Therefore, you may not realize that there is an inconsistency between the physical device status and the device status in the Management application for some time. This policy cannot determine if the SNMP trap or syslog listener ports are available or working.

  Rule Violation Fix — If the policy monitor report shows an "SNMP not registered as recipient" violation, the Administrator can register the Management server as an SNMP recipient through the **SNMP Trap Recipients** dialog box (**Monitor > SNMP Setup > Product Trap Recipients**). Refer to "Fault Management" on page 1141.

  If the policy monitor report shows an "Syslog not registered as recipient" violation, the Administrator can register the Management server as an Syslog recipient through the **Syslog Recipients** dialog box (**Monitor > Syslog Configuration > Product Syslog Recipients**). Refer to "Fault Management" on page 1141.

- **Check for SSH (secure Telnet) configuration** — This switch and router policy monitor enables you to check each target to see if SSH is enabled for device data transmission.

  NOTE
  Not supported on the following IronWare products: Application products running 12.3.X or earlier and the 6910 Ethernet switch.

  The preferred Management application product communication must be SSH for this check to pass.

  For Network OS verifies SSH access is enabled and telnet access is disabled through the IP ACL active or applied policy rules. You should verify that the IP ACL active rules deny telnet access to all.

  For IronWare products, verifies SSH access is enabled and telnet access is disabled through CLI commands.

Rule Violation Fix — If the policy monitor report shows a violation, enable SSH on the device. Disable Telnet settings on the device, if enabled.

- **Check for SNMPv3 (secure SNMP) configuration** — This switch and router policy monitor enables you to check each target to see if SNMPv3 is active for device data transmission and SNMPv1 and SNMPv2 are not configured.

NOTE
For this check to pass, you must discover the products using SNMPv3 credentials.

Rule Violation Fix — If the policy monitor report shows a violation, configure SNMPv3 on the device. Remove SNMPv1 and SNMPv2 settings on the device, if configured.

- **Check for VLAN configurations match for each connection (IP only) —** This switch and router policy monitor enables you to determine the consistency of VLAN configurations for each connection on the selected IP devices.

  Rule Violation Fix — If the policy monitor report shows a violation, configure VLANs on each device to contain the same interface membership.

- **Configuration Rules** — This switch and router policy monitor enables you to use predefined rules or create your own rules to compare content against a baseline (such as a product's backup configuration file). A configuration rule is a logical expression built with configuration conditions and blocks. For more information, refer to "Viewing a predefined configuration rule" on page 1116.
  - Predefined rules — The predefined rules include the following:
    - **No Interface Shutdown Rule** — Fails if any of the interfaces in the device are shut down.
    - **Port Profile Interface Rule** — Fails if any of the interfaces on the device do not have a port profile.
  - User-defined rules — You can configure your own configuration rules using predefined conditions and blocks (refer to "Adding a configuration rule" on page 1120).

Host policy monitors

Host policy monitors enable you to set the following checks on host devices.

- **Check for multiple fabrics connections —** This host policy monitor enables you to determine if each host is connected to multiple fabrics to prevent a single point of failure.

  Available hosts include both automatic hosts and manual hosts. Automatic hosts are those hosts discovered through Host or VM Manager discovery. Manual hosts are those host enclosures that are manually created through Host Port Mapping in the fabric topology.

  The Management application determines if the host has redundant connections to different fabrics based on discovery type and connection knowledge that the Management application collects; however, there is no guarantee that redundant paths exist to the same storage target.

  Depending on how you discover the hosts, there are recommended configurations you should complete to avoid inaccuracy:

  - Fabric discovery for manual host enclosures to fabric connections.

    Make sure there are Brocade HBAs on the host.

Make sure to configure the host port mapping. (refer to "Host port mapping overview" on page 419)

- Host adaptor discovery with 2.1 or later driver for host to unmanaged fabric connections (refer to "Host discovery" on page 93)

  Make sure there are Brocade HBAs on the host.

- Fabric plus Host adapter discovery with 2.1 or earlier driver (refer to "Host discovery" on page 93)

  Make sure there are Brocade HBAs on the host.

- Fabric plus VM Manager for hosts discovered through vCenter (refer to "VM Manager discovery" on page 103)

  Make sure there are Brocade HBAs on the host.

  Make sure you discover the associated fabrics.

- VM Manager plus Host adapter discovery (refer to "VM Manager discovery" on page 103)

  Make sure there are Brocade HBAs on the host.

  Make sure you discover the associated fabrics.

Rule Violation Fix — If the policy monitor report shows a violation, the Administrator can add a host connection to additional fabrics.

- **Check for connections through two fabrics to each target LUN** — This host policy monitor enables you to determine if there are redundant connections between the host group and the target LUN.

  To prevent a single point of failure, the host should have a redundant connection to the target LUN. Available hosts include both automatic hosts and manual hosts. An automatic host is a host discovered through Host adapter discovery or VM Manager discovery. A manual host is a host enclosure manually created through host port mapping in the fabric topology. Depending on how you discover the hosts, there are recommended configurations you should complete to avoid inaccuracy:

  - Host adapter discovery (refer to "Host discovery" on page 93)

    Make sure there are Brocade HBAs (with a 2.1 or later driver) on the host.

  - Fabric plus Host discovery

    Make sure there are Brocade HBAs on the host connected to the fabric.

    Make sure to configure the host port mapping (refer to "Host port mapping overview" on page 419).

  - Fabric plus VM Manager discovery

    Make sure there are Brocade HBAs (with a 2.1 or later driver) on the host connected to the fabric.

  - VM Manager plus Host discovery (refer to "VM Manager discovery" on page 103)

    Make sure there are Brocade HBAs (with a 2.1 or later driver) on the host.

    Make sure you discover the associated fabrics.

Rule Violation Fix — If the policy monitor report shows a violation, the Administrator can add redundant connections (either a host to attached fabrics or attached fabrics to a target LUN or more inter-fabric routes) to establish a complete path from host to target LUN.

Management policy monitor

The management policy monitor enables you to set a policy monitor on the Management application.

Check to see if the server backup is enabled and working — This management policy monitor enables you to determine if backup is enabled for the Management application server and if the backup output directory is accessible and writable.

Server backup automatically backs up the Management application database on a user-defined schedule.

Rule Violation Fix — If the policy monitor report shows a violation, the Administrator can edit the backup configuration through the **Options** dialog box, **Server Backup** pane (**Server > Options**). Refer to "Management server backup" on page 129.

Preconfigured policy monitors

The Management application provides preconfigured policy monitors. The preconfigured policy monitors include the following:

Default IP Policy — Available for SAN products and contains the following values:

- **Name** — Default IP Policy
- **Description** — Default policy to run on all IP targets
- **Frequency** — Weekly
- **Next Run** — Next time the policy will run using the format: *<Day_of_Week><Month><Date><Time_in_24_Hour_Format><Time_Zone><Year>*. For example, Fri Jun 08 08:00:00 PDT 2012.
- **Last Run** — Empty
- **Result** — Empty
- **Rule** — The default IP policy is configured with the following rules:
  - All profiles are the same on each RBridge in an Ethernet fabric
  - Event registration
  - Predefined rules – "No Interface Shutdown Rule" and "Port Profile Interface Rule"
  - Management application backup enabled
- **Targets** — The default IP policy is configured with the following targets:
  - Fabric Checks — All Fabrics
  - Switch/Router Checks — IP Wired Products and Wireless Controllers product groups

Viewing policy monitor status

You can view policy monitor status from the main Management application window or from the **Policy Monitor** dialog box.

The Management application enables you to view the policy monitor status at a glance by providing a policy monitor status icon on the Status Bar. The following table illustrates and describes the icons that indicate the current status of the policy monitor function.

TABLE 92 Policy Monitor Icons

Icon	Description
	Passed — Displays when all policy monitors, excluding un-alerted and acknowledged monitors, pass. Pause on icon to display flyover detail: Policy monitor is OK.
	Failed — Displays when at least one policy monitor failed. Pause on icon to display flyover detail: The last run of *number* policy monitor(s) has one or more failures.

To view more detail regarding policy monitor status, click the **Policy Monitor** icon. The **Policy Monitor** dialog box displays. For more information, refer to "Viewing existing policy monitors" on page 1107

Viewing existing policy monitors

To view existing policy monitors, complete the following steps.

1. Select **Monitor > Policy Monitor** (Figure 458).

   The **Policy Monitor** dialog box displays.

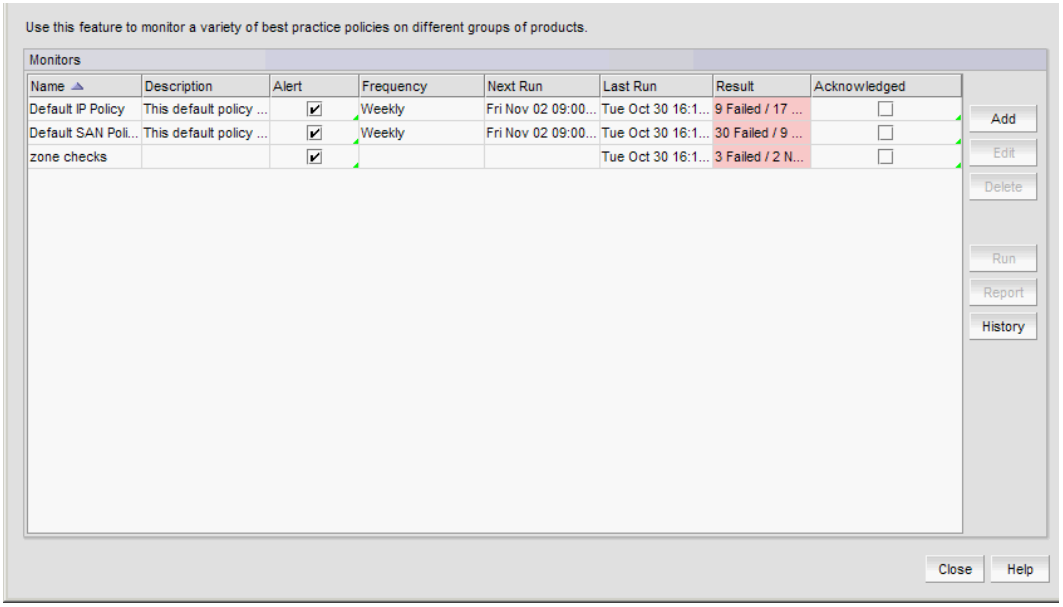


FIGURE 458 Policy Monitor dialog box

2. Review the policy monitor details:
   - **Name** — The user-defined name of the policy.
   - **Description** — A description of the policy.
   - **Alert** — Select to receive e-mail alerts and have the policy monitor status icon display in the Status bar when the monitor fails or partially fails.
   - **Frequency** — The frequency (one time, hourly, daily, weekly, or monthly) at which the policy is scheduled.
   - **Next Run** — The time the policy will run again.
   - **Last Run** — The time the policy ran last.
   - **Result** — The result of last policy monitor run. There are four possible results: Passed, Partially Failed, Failed, and Not Applicable.
   - **Acknowledged** — Whether the policy is acknowledged or not. Select the check box to acknowledge the policy. Disabled when the associated **Alert** check box is cleared.
3. To add a policy monitor, click **Add** (refer to "Adding a policy monitor" on page 1108).
4. To edit the selected policy monitor, click **Edit** (refer to "Editing a policy monitor" on page 1115).
5. To delete the selected policy monitor, click **Delete** (refer to "Deleting a policy monitor" on page 1115).
6. To run the selected policy and view the report, click **Run** (refer to "Running a policy monitor" on page 1135).

7. To open the last executed report for a selected policy monitor, select a policy monitor and click **Report** (refer to "Viewing a policy monitor report" on page 1136).
8. To view the report history for all policy monitors, click **History** (refer to "Viewing historical reports for a policy monitor" on page 1139).
9. To view the report history for a selected policy monitor, select a policy monitor and click **History** (refer to "Viewing historical reports for a policy monitor" on page 1139).
10. Click **Close** on the **Policy Monitor** dialog box.

Adding a policy monitor

To view existing policy monitors, complete the following steps.

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Click **Add**.

   The **Add Monitor** dialog box displays (Figure 459).

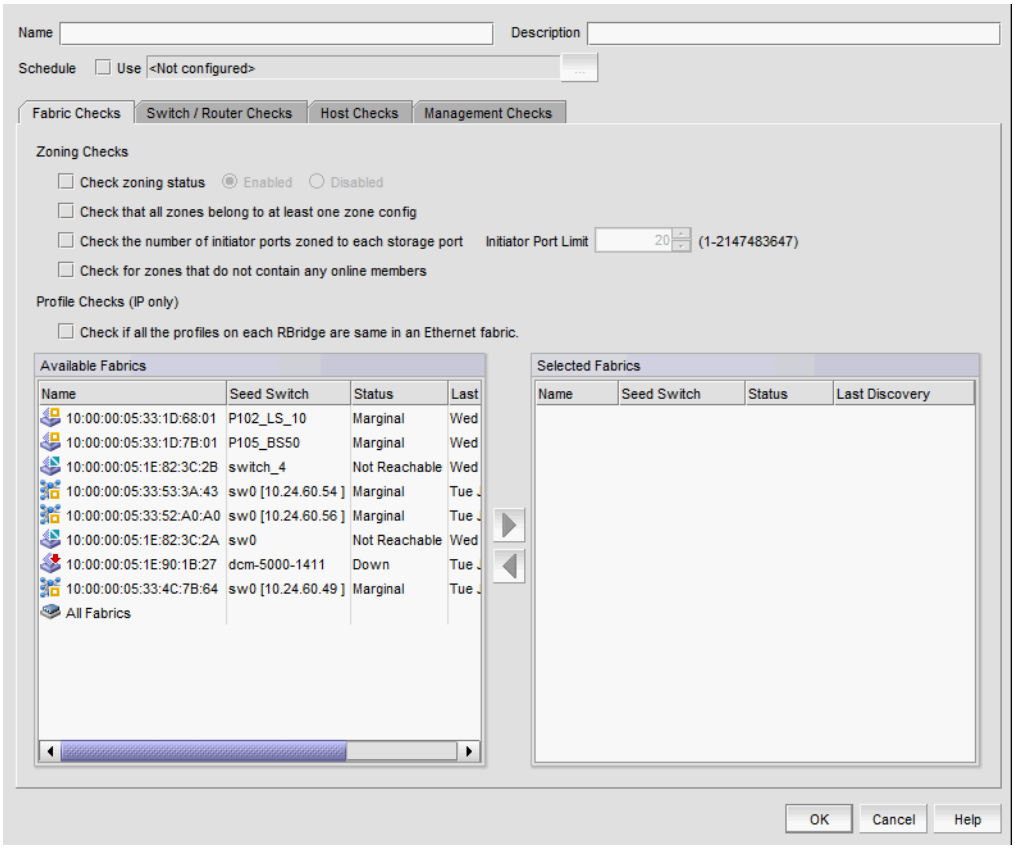


FIGURE 459 Add Policy Monitor dialog box, Fabric Checks tab

3. Enter a user-defined name for the policy in the **Name** field.

   The name must be unique. It cannot be over 64 characters, nor can the field be empty. It cannot include asterisks.

4. Enter a description of the policy in the **Description** field.

   The description cannot be over 128 characters. It cannot include asterisks.

5. Click the **Schedule Use** check box and choose one of the following options:

   - To use the default frequency (one time, runs at current system time plus fifteen minutes), go to step 6.
   - To configure the frequency, click the ellipsis button and choose one of the following options to configure the frequency at which deployment runs for the policy monitor:
     - To configure deployment to run only once, refer to "Configuring a one-time policy monitor schedule" on page 1113.
     - To configure hourly deployment, refer to "Configuring an hourly policy monitor schedule" on page 1114.
     - To configure daily deployment, refer to "Configuring a daily policy monitor schedule" on page 1114.
     - To configure weekly deployment, refer to "Configuring a weekly policy monitor schedule" on page 1114.
     - To configure monthly deployment, refer to "Configuring a monthly policy monitor schedule" on page 1114.

6. To set policy monitors for fabrics, select the **Fabric Checks** tab and complete the following steps.

   a. Select the **Check zoning status** check box to determine if zoning is enabled or disabled on the fabric.

      - Select the **Enabled** option to determine if zoning is enabled.
      - Select the **Disabled** option to determine if zoning is disabled.

      For more information about this check and a fix for rule violations, refer to "Fabric policy monitors" on page 1100.

   b. Select the **Check that all zones belong to at least one zone config** check box to determine if there are orphaned zones in the fabric zone database.

      For more information about this check and a fix for rule violations, refer to "Fabric policy monitors" on page 1100.

   c. Select the **Check the number of initiator ports zoned to each storage port** check box to determine the total number of initiator ports zoned to each storage port.

      For more information about this check and a fix for rule violations, refer to "Fabric policy monitors" on page 1100.

   d. Select the **Check zones that do not contain any online member** check box to identify zones in which all zone members are offline.

      For more information about this check and a fix for rule violations, refer to "Fabric policy monitors" on page 1100.

   e. Enter the initiator port limit in the **Initiator Port Limit** field.

The default recommended threshold ratio is 20:1 (20 initiator ports to 1 target port). Therefore, if the ratio for the storage port is equal to or higher than 20:1, the policy monitor considers it as a violation and logs it in the report.

f. Select the **Check that all profiles are the same on each RBridge in an Ethernet fabric** check box to determine if all RBridge profiles in an Ethernet fabric are the same.

For more information about this check and a fix for rule violations, refer to "Fabric policy monitors" on page 1100.

g. Select the fabrics to which you want to apply this policy in the **Available Fabrics** list and click the right arrow button.

NOTE
You can use the All Fabrics target in the **Available Fabrics** table for future provisioning. Select All Fabrics and click the right arrow button to apply this policy to all discovered fabrics.

The selected fabrics display in the **Selected Fabrics** list.

7. To set policy monitors for switches, select the **Switch/Router Checks** tab (Figure 460) and complete the following steps.

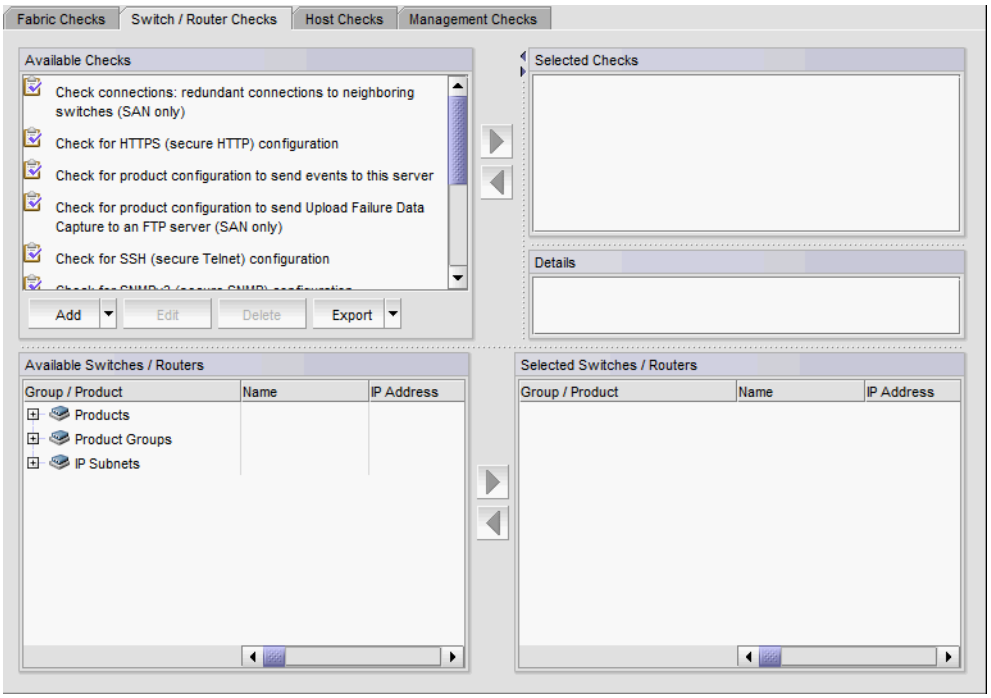


FIGURE 460 Add Policy Monitor dialog box, Switch/Router Checks tab

a. Select one or more of the following checks in the **Available Checks** list to include them in the policy monitor:

For more information about these checks and fixes for rule violations, refer to "Switch and router policy monitors" on page 1101.

NOTE
The **Check for HTTPS (secure HTTP) configuration** are not supported on Network OS products and the following IronWare products: Ethernet Core routers, Ethernet Carrier Routers, Ethernet Edge router, and Data Center switch, as well as the 6650 Ethernet switch, router, and L3 router..

NOTE
The **Check for Secure SSH (secure Telnet) configuration** checks are not supported on the following IronWare products: Application products running 12.3.X or earlier and the 6910 Ethernet switch.

- Select the **Check if the product is configured to send events to this server** check to determine if the Management application server is registered as an SNMP recipient and Syslog recipient.
- Select the **Check for HTTPS (secure HTTP) configuration** check to check each target to see if HTTPS is active for device data transmission.
- Select the **Check for SSH (secure Telnet) configuration** check to check each target to see if SSH is enabled for device data transmission.
- Select the **Check for SNMPv3 (secure SNMP) configuration** check to check each target to see if SNMPv3 is active for device data transmission and SNMPv1 and SNMPv2 are not configured.
- Select the **Check for VLAN configurations match for each connection (IP only)** check to determine the consistency of VLAN configurations for each connection on the selected IP devices.

b. Click the right arrow button to move the selected checks to the **Selected Checks** list.

c. Select the switches or routers to which you want to apply this policy in the **Available Switches/Routers** list and click the right arrow button.

NOTE
You can use the All Fabrics targets (under the Product Groups > System Product Groups node) in the **Available Switches/Routers** list) for future provisioning. Select All Fabrics and click the right arrow button to apply this policy to all discovered fabrics.

The selected switches display in the **Selected Switches/Routers** list.

8. To set policy monitors for hosts, select the **Host Checks** tab (Figure 461) and complete the following steps.

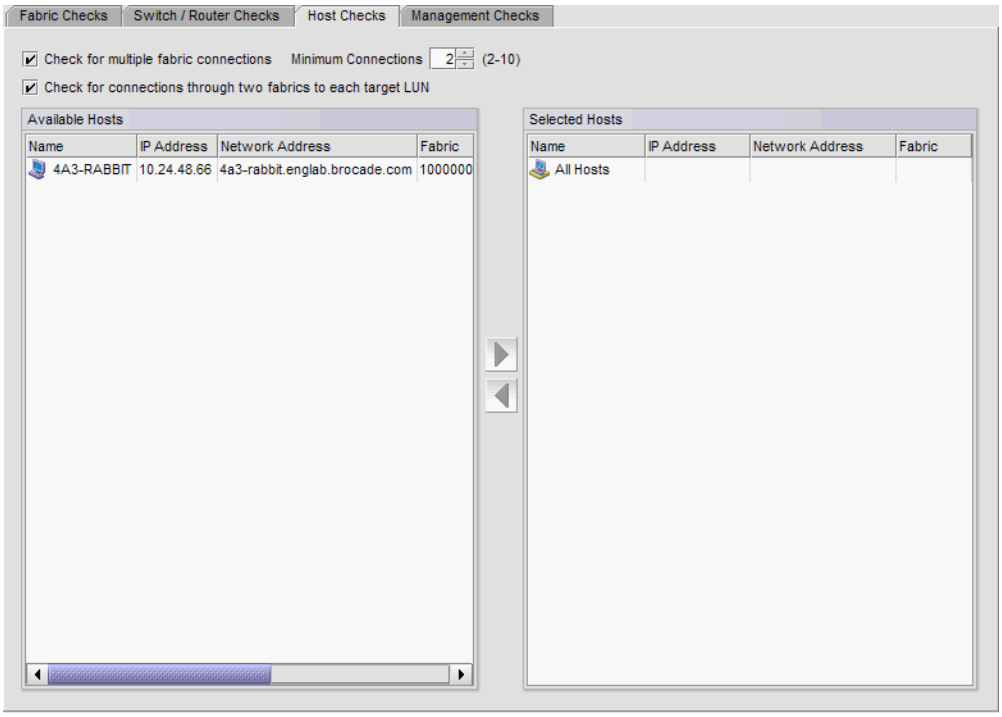


FIGURE 461 Add Policy Monitor dialog box, Hosts Checks tab

a. Select the **Check for redundant connections to attached fabrics** check box to determine if there are at least the minimum number of configured physical connections between the host and the attached fabric.

   The default is 2. For more information about this check and a fix for rule violations, refer to "Host policy monitors" on page 1103.

b. Enter the minimum number of connections between the host and the attached fabric in the **Minimum Connections** field.

   The default is 2.

c. Select the **Check for connections through two fabrics to each target LUN** check box to determine if there are redundant connections between the host group and the target LUN.

   For more information about this check and a fix for rule violations, refer to "Host policy monitors" on page 1103.

d. Select the hosts to which you want to apply this policy in the **Available Hosts** list and click the right arrow button.

   NOTE
   You can use the All Host target in the **Available Hosts** list for future provisioning. Select All Hosts and click the right arrow button to apply this policy to all discovered hosts.

   The selected hosts display in the **Selected Hosts** list.

9. To set policy monitors for the Management application (Figure 462), complete the following steps.

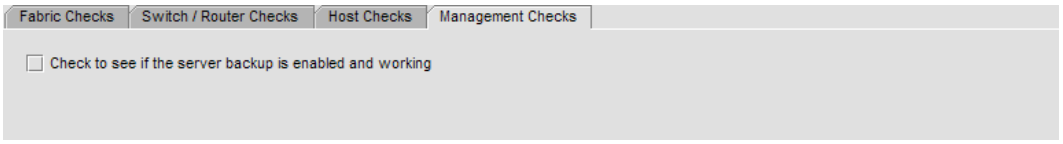


FIGURE 462 Add Policy Monitor dialog box, Management Checks tab

a. Select the **Management Checks** tab.

b. Select the **Check to see if the server backup is enabled and working** check box to determine the following configurations:

- Backup enabled for the Management application server.
- Backup output directory is accessible and writable.

This policy only applies to scheduled backup, not manual (on demand) backup.

For more information about this check and a fix for rule violations, refer to "Management policy monitor" on page 1105.

10. Click **OK** on the **Add Monitor** dialog box.

The **Policy Monitor** dialog box displays with the new policy monitor in the **Monitors** list.

11. Click **Close** on the **Policy Monitor** dialog box.

Policy monitor scheduling

You can schedule a policy monitor to run automatically. For step-by-step instructions, refer to the following procedures:

- "Configuring a one-time policy monitor schedule" on page 1113
- "Configuring an hourly policy monitor schedule" on page 1114
- "Configuring a daily policy monitor schedule" on page 1114
- "Configuring a weekly policy monitor schedule" on page 1114
- "Configuring a monthly policy monitor schedule" on page 1114

Configuring a one-time policy monitor schedule

To configure a one-time schedule, complete the following steps.

1. Select **One Time** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
3. Click the **Date** list to select a date from the calendar.
4. Click **OK** on the **Schedule Properties** dialog box.

   To finish configuring the policy monitor, return to step 6 of "Adding a policy monitor" on page 1108.

Configuring an hourly policy monitor schedule

To configure an hourly schedule, complete the following steps.

1. Select **Hourly** from the **Frequency** list.
2. Select the minute past the hour you want deployment to run from the **Minutes past the hour** list.

   Where the minute value is from 00 through 59.

3. Click **OK** on the **Schedule Properties** dialog box.

   To finish configuring the policy monitor, return to step 6 of "Adding a policy monitor" on page 1108.

Configuring a daily policy monitor schedule

To configure a daily deployment schedule, complete the following steps.

1. Select **Daily** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Click **OK** on the **Schedule Properties** dialog box.

   To finish configuring the policy monitor, return to step 6 of "Adding a policy monitor" on page 1108.

Configuring a weekly policy monitor schedule

To configure a weekly schedule, complete the following steps.

1. Select **Weekly** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Select the day you want deployment to run from the **Day of the Week** list.
4. Click **OK** on the **Schedule Properties** dialog box.

   To finish configuring the policy monitor, return to step 6 of "Adding a policy monitor" on page 1108.

Configuring a monthly policy monitor schedule

To configure a monthly schedule, complete the following steps.

1. Select **Monthly** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Select the day you want deployment to run from the **Day of the Month** list (1 through 31).
4. Click **OK** on the **Schedule Properties** dialog box.

   To finish configuring the policy monitor, return to step 6 of "Adding a policy monitor" on page 1108.

Editing a policy monitor

To edit an existing policy monitor, complete the following steps.

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.
2. Select the policy you want to edit in the **Monitors** list and click **Edit**.

   The **Edit Policy Monitor** dialog box displays. The **Edit Policy Monitor** dialog box has the same fields and components as the **Add Policy Monitor** dialog box.
3. Change the user-defined name for the policy in the **Name** field.

   The name must be unique. It cannot be over 64 characters, nor can the field be empty. It cannot include asterisks.
4. Change the description of the policy in the **Description** field.

   The description cannot be over 128 characters. It cannot include asterisks.
5. To edit the policy monitor checks, repeat step 5 through step 9 of "Adding a policy monitor" on page 1108.
6. Click **OK** on the **Edit Monitor** dialog box.

   The updated policy monitor displays in the **Monitors** list of the **Policy Monitor** dialog box.
7. Click **Close** on the **Policy Monitor** dialog box.

Deleting a policy monitor

To delete an existing policy monitor, complete the following steps.

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.
2. Select the policy you want to delete in the **Monitors** list.
3. Click **Delete**.
4. Click **Yes** on the confirmation message.
5. Click **Close** on the **Policy Monitor** dialog box.

Configuration rules

A configuration rule is a logical expression built with configuration conditions and blocks. You can use configuration rules to perform a configuration compliance check against a baseline (such as a product's backup configuration file).

Viewing a predefined configuration rule

You can view detailed information about predefined configuration rules on the **Add Monitor** or **Edit Monitor** dialog box.

1. Select the predefined configuration rule you want to view.

   The configuration rule displays in the **Details** area.

2. Review the configuration rule.

   For specific detailed information about the predefined rules, refer to "Predefined configuration rules" on page 1116.

Predefined configuration rules

The Management application provides the following predefined configuration rules:

- **No Interface Shutdown Rule** — The rule fails when any interface (10 Gbps port or LAG) on the device shuts down. Table 93 defines the logical expressions for this rule.

TABLE 93 No Interface Shutdown Rule expressions

AND/OR	(	Block/Condition Name	)	Details - Description/Condition/Configuration
		Start: Network OS Ten Gigabit Ethernet Interfaces		Processes all 10 Gigabit Ethernet interfaces on a Network OS device.
				interface TenGigabitEthernet .*
		Network OS Interface NOT shutdown		Condition test fails if the interface is shut down.
				Not Matches - Lines in any order
				shutdown
		End: Network OS Ten Gigabit Ethernet Interfaces		!
AND		Start: Network OS LAG Interfaces		Processes all LAG interfaces on a Network OS device.
				interface Port-channel .*
		Network OS Interface NOT shutdown		Checks whether the interface is configured as shutdown. This condition should be used within an interface block.
				Not Matches - Lines in any order
				shutdown
		End: Network OS LAG Interfaces		!

- **Port Profile Interface Rule** — The rule fails when any interface (10 Gbps port or LAG) on the device does not have a port profile. Table 94 defines the logical expressions for this rule.

TABLE 94 Port Profile Interface Rule expressions

AND/OR	(	Block/Condition Name	)	Details - Description/Condition/Configuration
		Start: Network OS Ten Gigabit Ethernet Interfaces		Processes all 10 Gigabit Ethernet interface on a Network OS device.
				interface TenGigabitEthernet .*
		Network OS Interface Port Profiled		Checks whether the interface port profiled. This condition should be used with in an interface block.
				Matches - Lines in any order
				port-profile-port
		End: Network OS Ten Gigabit Ethernet Interfaces		!
AND		Start: Network OS LAG Interfaces		Processes all LAG Interfaces on a Network OS device
				interface Port-channel .*
		Network OS Interface Port Profiled		Checks whether the interface port profiled. This condition should be used with in an interface block.
				Matches - Lines in any order
				port-profile-port
		End: Network OS LAG Interfaces		!

Viewing configuration rule details

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Click **Add**.

   The **Add Monitor** dialog box displays.

3. Click the **Switch/Router Checks** tab.

4. Select **Add > Configuration Rule**.

   The **Add Configuration Rule** dialog box displays (Figure 463).

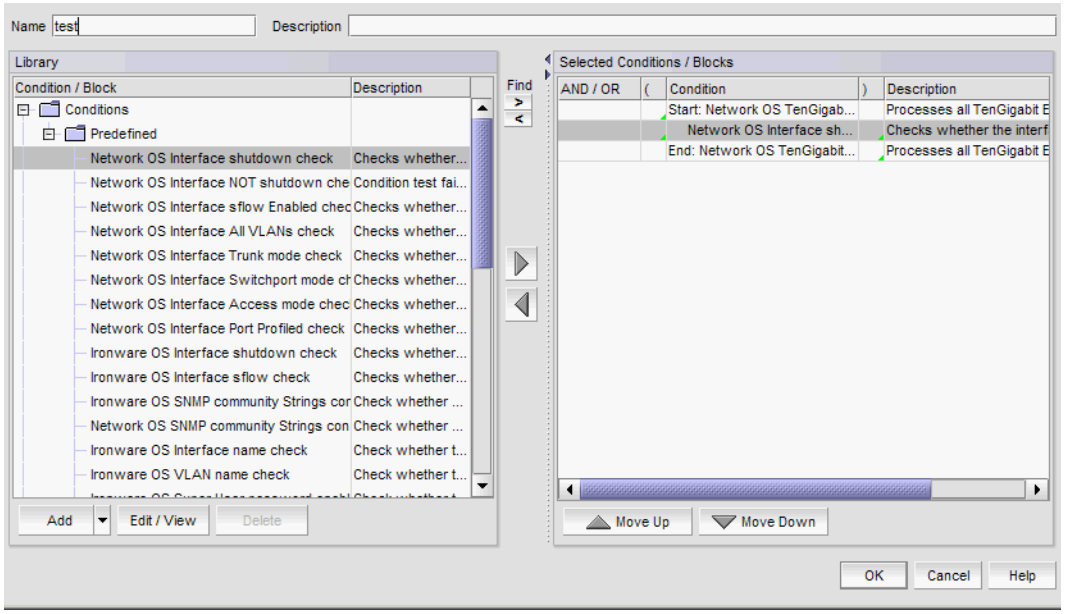


FIGURE 463 Add Configuration Rule dialog box

This **Add Configuration Rule** dialog box contains the following fields and components:

- **Name** — A unique name for the rule.

  The name cannot be over 128 characters. The only special characters allowed are an underscore (_) or space.

- **Description** — A description for the rule.

  The description cannot be over 1024 ASCII characters.

- **Library** list — Contains a list of predefined and user-defined conditions or blocks. You cannot modify or delete predefined conditions or blocks. For more information, about predefined conditions and blocks, refer to "Predefined conditions" on page 1128 and "Predefined blocks" on page 1134.

  The **Library** list contains the following details:

  - **Condition/Block** — Conditions or blocks in a folder structure. For example, the predefined conditions use the following structure: Conditions/Predefined/*Condition_Name*.
  - **Description** — Description of condition or block. This field is blank for folders.
  - **Add** button — Click and select **Condition** or **Block** to add a condition or block. For more information, refer to "Adding a configuration condition" on page 1124 or "Adding a configuration block" on page 1131.
  - **Edit / View** button — Select a user-defined condition or block and click to edit. Select a predefined condition or block and click to view. For more information, refer to "Editing a user-defined configuration condition" on page 1127, "Editing a user-defined configuration block" on page 1133, "Viewing predefined configuration conditions" on page 1124, or "Viewing a predefined configuration block" on page 1130.
  - **Delete** button — Select one or more user-defined conditions or blocks and click to delete. For more information, refer to "Deleting conditions and blocks" on page 1134.

- **Find >** (right arrow) button — To find a condition or block in the **Selected Conditions/Blocks** list, select a condition or block in the **Library** list and click.

  The condition or block is highlighted in the **Selected Conditions/Blocks** list.

- **Find <** (left arrow) button — To find a condition or block in the **Library** list, select a condition or block in the **Selected Conditions/Blocks** list and click.

  The condition or block is highlighted in the **Library** list.

- Right arrow button — To add a condition or block to a rule, select the condition or block in the **Library** list and click to add it to the **Selected Conditions/Block** list.

  When you add a condition to a block, it is prefixed with an OR connector, except for the first condition in the block. The first condition in the block cannot have any connector operator.

  If you select a mixture of blocks and conditions in the **Library** list and you select one or more blocks in the **Selected Conditions/Blocks** list, when you click the right arrow, conditions are added to the selected blocks in the list and any new blocks are added at the end of the logical expression.

  You cannot add a condition or block more than once at the logical expression level. However, you can add the same condition to one or more blocks. You cannot add a condition more than once to a single block.

- Left arrow button — To remove a condition or block from a rule, select a one or more conditions and blocks in the **Selected Conditions/Blocks** list and click the left arrow button.

- **Selected Conditions/Block** list — Contains the logical expression of one or more conditions and blocks for the rule.

  The **Selected Conditions/Block** list contains the following details:

  - **AND/OR** — To change the logical operator separator, select **AND** or **OR** from the **AND/OR** column.
    Valid values include AND and OR. The first item in a rule and the first connector in a block display empty fields and cannot be edited. Each condition or block you add displays with an AND connector (except the first item) in the list of conditions or blocks. If you add one or more conditions to a block, each condition displays with an OR connector (except the first condition) in the block.
    Fields containing a green triangle ( ) in the lower right corner are editable.
  - **(** — Enter an open parenthesis to start a group (a set of conditions and blocks).
    You can create up to three groups. You can nest groups. To ungroup a group, clear the **(** and **)** columns that delineate the group.
  - **Condition** — A list of conditions and blocks included in the rule.
  - **)** — Enter a close parenthesis to close a group (a set of conditions and blocks).
    You can create up to three groups. You can nest groups. To ungroup a group, clear the **(** and **)** columns that delineate the group.
  - **Move Up** button — Use to move a condition or block up in the rule (except the first item).
    You can only move one item (condition or entire block) up at a time. If you move a condition to the first position in the rule or in a block, the logical operator (**AND/OR** column) is cleared. You can move a condition into a block by moving it between the start and end of a block. If the condition is already part of the block, it skips the block and moves above the block.

- **Move Down** button — Use to move a condition or block down in the rule (except the last item).
  You can only move one item (condition or entire block) down at a time. If you move a condition from the first position in the rule or in a block, the logical operator (**AND/OR** column) is automatically populated. You can move a condition into a block by moving it between the start and end of a block. If the condition is already part of the block, it skips the block and moves below the block.

5. Click **Cancel** on the **Add Configuration Rule** dialog box.
6. Click **Cancel** on the **Add Monitor** dialog box.
7. Click **Close** on the **Policy Monitor** dialog box.

Adding a configuration rule

You can create your own rules to compare content against a baseline.

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Click **Add**.

   The **Add Monitor** dialog box displays.

3. Click the **Switch/Router Checks** tab.
4. Select **Add > Configuration Rule**.

   The **Add Configuration Rule** dialog box displays (Figure 463).

5. Enter a name for the rule in the **Name** field.

   The name cannot be over 128 characters. The only special characters allowed are an underscore (_) or space.

6. Enter a description for the rule in the **Description** field.

   The description cannot be over 1024 ASCII characters.

7. Select one or more conditions and blocks in the **Library** list and click the right arrow button to add the conditions and blocks to the rule.

   The **Library** list contains a list of predefined and user-defined conditions or blocks. You cannot modify or delete predefined conditions or blocks. For more information, about predefined conditions and blocks, refer to "Predefined conditions" on page 1128 and "Predefined blocks" on page 1134.

   To add a condition, refer to "Adding a configuration condition" on page 1124.

   To add a block, refer to "Adding a configuration block" on page 1131.

   To delete a condition or block, refer to "Deleting conditions and blocks" on page 1134.

8. To add conditions to a block, select a block in the **Selected Conditions/Block** list, then select the conditions (one or more) you want to add to the block in the **Library** list and click the right arrow button.

9. To change the logical operator separator, select **AND** or **OR** from the **AND/OR** column.

   Valid values include AND and OR. The first item in a rule and the first connector in a block display empty fields. Each condition or block you add displays with an AND connector (except the first item) in the list of conditions or blocks. If you add one or more conditions to a block, each condition displays with an OR connector (except the first condition) in the block.

   Fields containing a green triangle ( ) in the lower right corner are editable.

10. To group a set of conditions and blocks, enter an open parenthesis in the **(** column of the condition or block where you want to start a grouping and enter a close parenthesis in the **)** column after the last condition or block you want to include in the group.

    You can create up to three groups. You can nest groups. To ungroup a group, clear the **(** and **)** columns that delineate the group.

11. To move a condition or block up in the rule, select one condition or block (except the first item) and click **Move Up**.

    You can only move one item (condition or entire block) up at a time. If you move a condition to the first position in the rule or in a block, the logical operator (**AND/OR** column) is cleared. You can move a condition into a block by moving it between the start and end of a block. If the condition is already part of the block, it skips the block and moves above the block.

12. To move a condition or block down in the rule, select one condition or block (except the last item) and click **Move Down**.

    You can only move one item (condition or entire block) down at a time. If you move a condition from the first position in the rule or in a block, the logical operator (**AND/OR** column) is automatically populated. You can move a condition into a block by moving it between the start and end of a block. If the condition is already part of the block, it skips the block and moves below the block.

13. To find a condition or block in the **Selected Conditions/Blocks** list, select a condition or block in the **Library** list and click **Find >** (right arrow).

    The condition or block is highlighted in the **Selected Conditions/Blocks** list.

14. To find a condition or block in the **Library** list, select a condition or block in the **Selected Conditions/Blocks** list and click **Find <** (left arrow).

    The condition or block is highlighted in the **Library** list.

15. To remove a condition or block from a rule, select one or more conditions and blocks in the **Selected Conditions/Blocks** list and click the left arrow button.

16. Click **OK** on the **Add Configuration Rule** dialog box.

17. Click **OK** on the **Add Monitor** dialog box.

    The updated policy monitor displays in the **Monitors** table of the **Policy Monitor** dialog box.

18. Click **Close** on the **Policy Monitor** dialog box.

Duplicating a configuration rule

You can create a new configuration rule based on a predefined or user-defined configuration rule.

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Click **Add**.

   The **Add Monitor** dialog box displays.

3. Click the **Switch/Router Checks** tab.

4. Select the configuration rule (either predefined rule or user-defined) you want to duplicate in the **Available Checks** list or **Selected Checks** list.

5. Click **Add > Configuration Rule**.

   The **Add Configuration Rule** dialog box displays.

6. Change the name for the rule in the **Name** field.

   The name cannot be over 128 characters. The only special characters allowed are an underscore (_) or space.

7. Change the description for the rule in the **Description** field.

   The description cannot be over 1024 ASCII characters.

8. To edit the configuration rule, repeat step 7 through step 15 of "Adding a configuration rule" on page 1120.

9. Click **OK** on the **Add Configuration Rule** dialog box.

10. Click **OK** on the **Add Monitor** dialog box.

    The updated policy monitor displays in the **Monitors** table of the **Policy Monitor** dialog box.

11. Click **Close** on the **Policy Monitor** dialog box.

Editing a configuration rule

You can edit your own rules to compare content against a baseline.

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Click **Edit**.

   The **Edit Monitor** dialog box displays.

3. Click the **Switch/Router Checks** tab.

4. Select the configuration rule you want to edit in the **Available Checks** list and click **Edit**.

   The **Edit Configuration Rule** dialog box displays.

5. Change the name for the rule in the **Name** field.

   The name cannot be over 128 characters. The only special characters allowed are an underscore (_) or space.

6. Change the description for the rule in the **Description** field.

   The description cannot be over 1024 ASCII characters.

7. To edit a configuration rule, repeat step 7 through step 15 of "Adding a configuration rule" on page 1120.

8. Click **OK** on the **Edit Configuration Rule** dialog box.
9. Click **OK** on the **Edit Monitor** dialog box.

   The updated policy monitor displays in the **Monitors** table of the **Policy Monitor** dialog box.
10. Click **Close** on the **Policy Monitor** dialog box.

Exporting a configuration rule

You can export user-defined configuration rules from one instance of the Management application to another.

1. From the **Add Monitor** or **Edit Monitor** dialog box, select Export from the Export list.

   The **Export Configuration Rule** dialog box displays.
2. Browse to the location where you want to export the configuration rule (xml format) file and click **Export**.
3. Click **OK** on the **Add Monitor** or **Edit Monitor** dialog box.

Importing a configuration rule

You can import user-defined configuration rules (xml format) one at a time.

Imported rules must meet the following criteria:

- The rule cannot have the same name as a predefined configuration rule.
- The rule cannot have any invalid rule or condition parameters.
- The rule cannot have any invalid block parameters.

1. From the **Add Monitor** or **Edit Monitor** dialog box, select **Import** from the **Export** list.

   The **Import Configuration Rule** dialog box displays.
2. Browse to the configuration rules (xml format) file and click **Import**.
3. Click **Yes** on the confirmation message, if necessary.
4. Click **OK** on the **Add Monitor** or **Edit Monitor** dialog box.

Deleting a configuration rule

You can only delete user-defined configuration rules.

1. From the **Add Monitor** or **Edit Monitor** dialog box, select one or more user-defined configuration rules you want to delete.
2. Click **Delete**.
3. Click **Yes** on the confirmation message.
4. Click **OK** on the **Add Monitor** or **Edit Monitor** dialog box.

Viewing predefined configuration conditions

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Click **Add**.

   The **Add Monitor** dialog box displays.

3. Click the **Switch/Router Checks** tab.

4. Select **Add > Configuration Rule**.

   The **Add Configuration Rule** dialog box displays.

5. Select the predefined condition you want to view and click **Edit/View**.

   The **View Condition** dialog box displays. This dialog box contains the following fields and components:

   - **Product** field and ellipsis button — Not editable in the **View Condition** dialog box.
   - **Configuration** list — Not available in the **View Condition** dialog box.
   - **Name** — The name of the selected condition.
   - **Description** — The description of the selected condition.
   - **Use regular expression** check box — Not available in the **View Condition** dialog box.
   - **Configuration the lines below** list — Not available in the **View Condition** dialog box.
   - **Configuration** text box — The configuration lines with which you want to compare the product configuration.
   - **Lines in exact order** check box — Not available in the **View Condition** dialog box.
   - **Remediation** text box — Details how to correct the failure, if the condition fails.

     Remediation content displays in the Configuration Rule Report for each failed condition. The remediation detail cannot be over 1024 ASCII characters.

6. Click **Cancel** on the **View Condition** dialog box.

7. Click **Cancel** on the **Add Configuration Rule** dialog box.

8. Click **Cancel** on the **Add Monitor** dialog box.

9. Click **Close** on the **Policy Monitor** dialog box.

Adding a configuration condition

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Click **Add**.

   The **Add Monitor** dialog box displays.

3. Click the **Switch/Router Checks** tab.

4. Select **Add > Configuration Rule**.

   The **Add Configuration Rule** dialog box displays.

5. Select **Add > Condition**.

   The **Add Condition** dialog box displays (Figure 464).

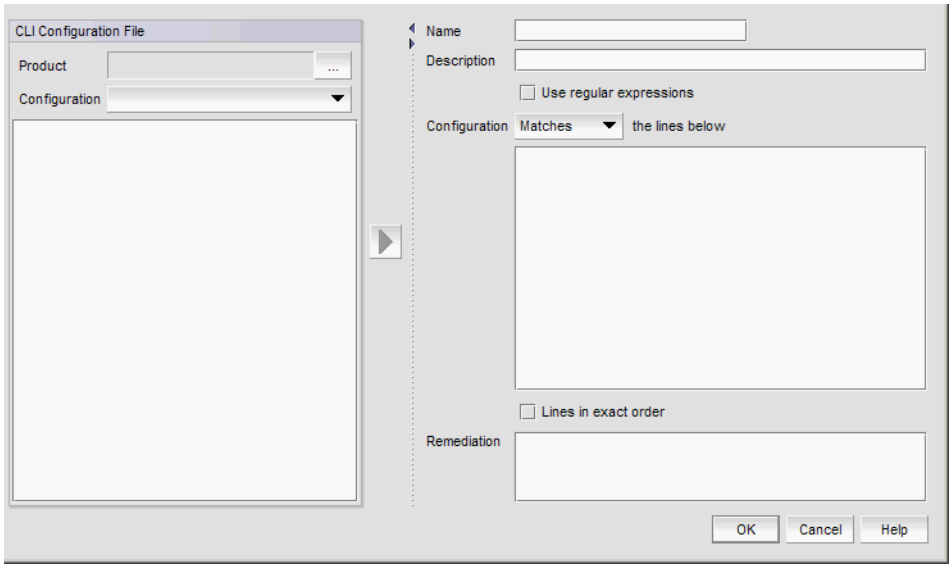


FIGURE 464 Add Condition dialog box

6. Enter a user-defined name for the rule in the **Name** field.

   The name must be unique. The name cannot be over 128 characters. The only special character allowed is an underscore (_).

7. Enter a description of the rule in the **Description** field.

   The description cannot be over 1024 ASCII characters.

8. Select the backup configuration file you want to use by completing the following steps.

   a. Click the **Product** ellipsis button complete the steps in "Selecting a product" on page 1126.

      If the product has no configuration files, the **Configuration** list is empty. You can manually trigger configuration file back up for the products to populate this list.

      If the product has multiple configuration files, the latest configuration file is selected and displays in the **Configuration** list by default.

   b. Select the backup configuration file you want to use from the **Configuration** list.

      The contents of the backup configuration file display in the **CLI Configuration File** text box. Select the lines you want to use in the **CLI Configuration File** text box and click the right arrow to move the lines to the **Configuration** text box.

9. Check the **Use regular expressions** check box to enter a regular expression in the **Configuration** text box.

10. Select one of the following options to determine whether the configuration lines should match or not match from **Configuration the lines below** list:

    - **Matches** — Select this option from the list if you want the configuration line to match the line in the device configuration file.

- **Not Matches** — Select this option from the list if you do not want the configuration line to match the line in the device configuration file.

11. Enter one or more configuration lines with which you want to compare the device configuration in the **Configuration** text box.
12. Select the **Lines in exact order** check box to match the configuration lines in the same order in the **Configuration** text box as the device configuration.

    Clear the **Lines in exact order** check box to search and match each configuration line in the **Configuration** text box.
13. Enter details to correct the failure, if the condition fails, in the **Remediation** text box.

    Remediation content displays in the Configuration Rule Report for each failed condition. The remediation detail cannot be over 1024 ASCII characters.
14. Click **OK** on the **Add Condition** dialog box.
15. Click **OK** on the **Add Configuration Rule** dialog box.
16. Click **OK** on the **Add Monitor** dialog box.

    The updated policy monitor displays in the **Monitors** table of the **Policy Monitor** dialog box.
17. Click **Close** on the **Policy Monitor** dialog box.

Selecting a product

You can only select one product at a time.

1. From the **Add Condition** dialog box, click the **Product** ellipsis button to select a product.

   The **Select Product** dialog box displays.
2. Select a product from the **Available Products** list, and click the right arrow button to move the product to the **Selected Product** table.

   The **Available Products** list contains the same fields as the IP Product list (refer to "IP Product List" on page 284).
3. To remove a product from the **Selected Product** list, select the product and click the left arrow button to move the product to the **Available Products** list.

   The **Selected Product** list contains the same fields as the IP Product list (refer to "IP Product List" on page 284).
4. Click **OK** on the **Select Product** dialog box.

Duplicating a configuration condition

Enables you to create a new condition based on a predefined or user-defined condition.

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.
2. Click **Edit**.

   The **Edit Monitor** dialog box displays.
3. Click the **Switch/Router Checks** tab.

4. Select the configuration rule you want to edit in the **Available Checks** list and click **Edit**.

   The **Edit Configuration Rule** dialog box displays.

5. Select the predefined or user-defined condition you want to edit and click **Add > Condition**.

   The **Add Condition** dialog box displays.

6. Change the user-defined name for the rule in the **Name** field, if necessary.

   The name must be unique. The name cannot be over 128 characters. The only special character allowed is an underscore (_).

7. Change the description of the rule in the **Description** field, if necessary.

   The description cannot be over 1024 ASCII characters.

8. To edit a configuration condition, repeat step 8 through step 13 of "Adding a configuration condition" on page 1124.

9. Click **OK** on the **Add Condition** dialog box.

10. Click **OK** on the **Edit Configuration Rule** dialog box.

11. Click **OK** on the **Edit Monitor** dialog box.

    The updated policy monitor displays in the **Monitors** table of the **Policy Monitor** dialog box.

12. Click **Close** on the **Policy Monitor** dialog box.

Editing a user-defined configuration condition

NOTE
You cannot edit a predefined configuration condition.

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Click **Edit**.

   The **Edit Monitor** dialog box displays.

3. Click the **Switch/Router Checks** tab.

4. Select the configuration rule you want to edit in the Available Checks list and click **Edit**.

   The **Edit Configuration Rule** dialog box displays.

5. Select the user-defined condition you want to edit and click **Edit**.

   The **Edit Condition** dialog box displays.

6. Change the user-defined name for the rule in the **Name** field, if necessary.

   The name must be unique. The name cannot be over 128 characters. The only special character allowed is an underscore (_).

7. Change the description of the rule in the **Description** field, if necessary.

   The description cannot be over 1, 024 ASCII characters.

8. To edit a configuration condition, repeat step 8 through step 13 of "Adding a configuration condition" on page 1124.

9. Click **OK** on the **Edit Condition** dialog box.
10. Click **OK** on the **Edit Configuration Rule** dialog box.
11. Click **OK** on the **Edit Monitor** dialog box.

    The updated policy monitor displays in the **Monitors** table.
12. Click **Close** on the **Policy Monitor** dialog box.

Predefined conditions

The Management application provides predefined conditions. Table 95 lists the predefined conditions that can be used in a block or at the configuration rule level. For example, interface conditions should be used in a port or LAG interface block and SNMP conditions can be used at the rule level.

TABLE 95 Predefined conditions

Name	Description	Use regular expression	Matches/ Not Matches	Configuration	Lines in exact order
Network OS Interface shutdown check	Checks whether the interface is configured as shutdown. This condition should be used within an interface block.	No	Matches	shutdown	No
Network OS Interface NOT shutdown check	Condition test fails if the interface is shutdown.	No	Not Matches	shutdown	No
Network OS Interface sflow Enabled check	Checks whether sFlow is enabled on the interface. This condition should be used within an interface block.	No	Matches	sflow enable sflow sample-rate 32768	Yes
Network OS Interface All VLANs check	Checks whether the interface is configured to be part of all VLANs. This condition should be used within an interface block.	No	Matches	switchport trunk allowed vlan all	No
Network OS Interface Trunk mode check	Checks whether the interface is configured to be in trunk mode. This condition should be used within an interface block.	No	Matches	switchport switchport mode trunk	Yes
Network OS Interface Switchport mode check	Checks whether the Network OS interface is configured to be a switchport or not. If not configured, the test will fail.	No	Matches	switchport	No
Network OS Interface Access mode check	Checks whether the interface is configured to be in access mode. This condition should be used within an interface block.	No	Matches	switchport switchport mode access	Yes
Network OS Interface Port Profiled check	Checks whether the interface port is profiled. This condition should be used within an interface block.	No	Matches	port-profile-port	No

TABLE 95 Predefined conditions (Continued)

Name	Description	Use regular expression	Matches/ Not Matches	Configuration	Lines in exact order
IronWare OS Interface shutdown check	Checks whether the IronWare device port is in shutdown state. (This is not applicable for Ethernet router products.) This condition should be used within an interface block.	No	Matches	disable	No
IronWare OS Interface sflow check	Checks whether sFlow is configured on the IronWare device port. This condition should be used within an interface block.	No	Matches	sflow-forwarding sflow sample 32768	Yes
IronWare OS SNMP community Strings configured check	Checks whether SNMP community strings are configured.	Yes	Matches	snmp-server community .*	No
Network OS SNMP community strings configured check	Checks whether SNMP community strings are configured.	Yes	Matches	snmp-server community private rw snmp-server community public	No
IronWare OS Interface name check	Checks whether the port is named or not.	Yes	Matches	port-name.*	No
IronWare OS VLAN name check	Checks whether the VLAN is named or not.	Yes	Matches	vlan(.)+name(.)+$	No
IronWare OS Super User password enabled check	Checks whether the super user password is enabled on the device or not.	Yes	Matches	^enable super-user-password	No
IronWare OS Password min length enabled check	Checks whether the password minimum length is enabled or not. The range allowed is from 8 through 255 characters.	Yes	Matches	^enable password-min-length ([8-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])$	No
IronWare OS AAA Console Enabled check	Checks whether the AAA console is enabled or not	Yes	Matches	^enable aaa console$	No
IronWare OS SSH timeout check	Checks whether the IP SSH timeout value has been configured for the device in the range [1 - 120].	Yes	Matches	'^ip ssh +timeout (0*([1-9][0-9]?|1[01][0-9]|120))$'	No
IronWare OS SSH idle-time check	Checks whether the IP SSH idle-timeout is less than or equal to 10 minutes.	Yes	Matches	^ip ssh +idle-time ([0-9]|10)$	No
IronWare OS SSH Client Allowed check	Checks to see if the SSH client is allowed or not.	Yes	Matches	ip ssh +client.*	No
RFS with Configuration Auto Install Disabled	Checks whether auto-installation of the configuration is disabled in a user-specified profile. This condition should be used inside the profile block. If the profile name is not specified in the configuration or if the user selects all the profiles (profile.*), then it will match against the first available profile.	No	Matches	no autoinstall configuration	No

TABLE 95 Predefined conditions (Continued)

Name	Description	Use regular expression	Matches/ Not Matches	Configuration	Lines in exact order
RFS with Firmware Auto Install Disabled	Checks whether auto-installation of the firmware is disabled in user-specified profile. This condition should be used inside the profile block. If the profile name is not specified in configuration or if user selects all the profiles (profile.*) then it will match against first available profile	No	Matches	no autoinstall firmware	No
RFS Radio Interface check	Checks whether the specified profile is configured with Radio interfaces. This condition should be used inside the profile block. If the profile name is not specified in the configuration or if the user selects all the profiles (profile.*), then it will match against the first available profile.	Yes	Matches	interface radio.*	No
RFS Gigabit Ethernet Interface check	Checks whether the specified profile is configured with Gigabit Ethernet interfaces. This condition should be used inside the profile block. If the profile name is not specified in the configuration or if the user selects all the profiles (profile.*), then it will match against the first available profile.	Yes	Matches	interface ge.*	No
RFS Fast Ethernet Interface check	Checks whether the specified profile is configured with Fast Ethernet interfaces. This condition should be used inside the profile block. If the profile name is not specified in the configuration or if the user selects all the profiles (profile.*), then it will match against the first available profile.	Yes	Matches	interface fe.*	No
RFS AAA policy Health Check Interval	Checks whether the health check interval has been configured in the AAA policy.	No	Matches	health-check interval	No

Viewing a predefined configuration block

A configuration block is a continuous group of lines within a configuration file within which conditions will be checked. The block is defined by the line that starts the block and the line that ends the block.

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Click **Add**.

The **Add Monitor** dialog box displays.

3. Click the **Switch/Router Checks** tab.
4. Select **Add > Configuration Rule**.

   The **Add Configuration Rule** dialog box displays.

5. Select the predefined block you want to view and click **Edit/View**.

   The **View Block** dialog box displays. This dialog box contains the following fields and components:

   - **Name** — The name of the selected block.
   - **Description** — The description of the selected block.
   - **Use regular expression** check box — Not available for the **View Block** dialog box.
   - **Block Start** — The start of the selected block used to match a block start label in the device configuration.
   - **Block End** — The end of the selected block used to match (up to and including this string) in the device configuration.

6. Click **Cancel** on the **View Block** dialog box.
7. Click **Cancel** on the **Add Configuration Rule** dialog box.
8. Click **Cancel** on the **Add Monitor** dialog box.
9. Click **Close** on the **Policy Monitor** dialog box.

Adding a configuration block

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Click **Add**.

   The **Add Monitor** dialog box displays.

3. Click the **Switch/Router Checks** tab.
4. Select **Add > Configuration Rule**.

   The **Add Configuration Rule** dialog box displays.

5. Select **Add > Block**.

   The **Add Block** dialog box displays (Figure 465).

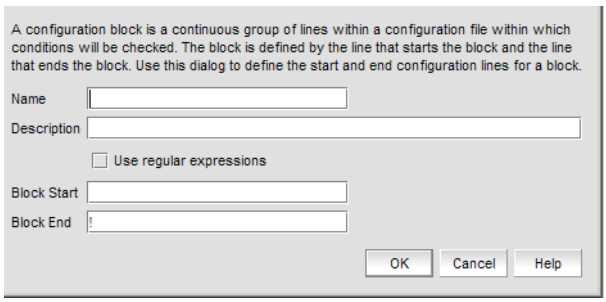


FIGURE 465 Add Block dialog box

6. Enter a user-defined name for the block in the **Name** field.

   The name must be unique. The name cannot be over 128 characters. The only special character allowed is an underscore (_).

7. Enter a description of the block in the **Description** field.

   The description cannot be over 1024 ASCII characters.

8. Select the **Use regular expression** check box to use a regular expression in the **Block Start** field.

   This enables you to match one or more blocks in the device configuration.

9. Enter the start of a block that you want to match to a block start label in the device configuration in the **Block Start** field.

   The block start cannot be over 256 characters.

10. Enter the block end that you want to use to match (up to and including this string) in the device configuration in the **Block End** field.

    The block end cannot be over 256 characters. By default, this field contains an exclamation point (!). Do not use a regular expression as a block end.

11. Click **OK** on the **Add Block** dialog box.
12. Click **OK** on the **Add Configuration Rule** dialog box.
13. Click **OK** on the **Add Monitor** dialog box.

    The updated policy monitor displays in the **Monitors** table of the **Policy Monitor** dialog box.

14. Click **Close** on the **Policy Monitor** dialog box.

Duplicating a configuration block

Enables you to create a new configuration block based on a predefined or user-defined configuration block .

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Click **Edit**.

   The **Edit Monitor** dialog box displays.

3. Select the **Switch/Router Checks** tab.
4. Select the configuration rule you want to edit in the **Available Checks** list and click **Edit**.

   The **Edit Configuration Rule** dialog box displays.

5. Select the predefined or user-defined block you want to duplicate and click **Add > Block**.

   The **Add Block** dialog box displays.

6. Change the user-defined name for the rule in the **Name** field, if necessary.

   The name must be unique. The name cannot be over 128 characters. The only special character allowed is an underscore (_).

7. Change the description of the rule in the **Description** field, if necessary.

   The description cannot be over 1024 ASCII characters.

8. To edit a configuration block, repeat step 8 through step 10 of "Adding a configuration block" on page 1131.

9. Click **OK** on the **Add Block** dialog box.

10. Click **OK** on the **Edit Configuration Rule** dialog box.

11. Click **OK** on the **Edit Monitor** dialog box.

    The updated policy monitor displays in the **Monitors** table of the **Policy Monitor** dialog box.

12. Click **Close** on the **Policy Monitor** dialog box.

Editing a user-defined configuration block

NOTE
You cannot edit a predefined configuration block.

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Click **Edit**.

   The **Edit Monitor** dialog box displays.

3. Select the **Switch/Router Checks** tab.

4. Select the configuration rule you want to edit in the **Available Checks** list and click **Edit**.

   The **Edit Configuration Rule** dialog box displays.

5. Select the user-defined block you want to edit and click **Edit**.

   The **Edit Block** dialog box displays.

6. Change the user-defined name for the rule in the **Name** field, if necessary.

   The name must be unique. The name cannot be over 128 characters. The only special character allowed is an underscore (_).

7. Change the description of the rule in the **Description** field, if necessary.

   The description cannot be over 1, 024 ASCII characters.

8. To edit a configuration block, repeat step 8 through step 10 of "Adding a configuration block" on page 1131.

9. Click **OK** on the **Edit Block** dialog box.

10. Click **OK** on the **Edit Configuration Rule** dialog box.

11. Click **OK** on the **Edit Monitor** dialog box.

    The updated policy monitor displays in the **Monitors** table of the **Policy Monitor** dialog box.

12. Click **Close** on the **Policy Monitor** dialog box.

Deleting conditions and blocks

You can only delete user-defined conditions or blocks. Before you delete a user-defined condition or block, you must remove it from any rules.

1. From the **Add Configuration Rule** or **Edit Configuration Rule** dialog box, select one or more user-defined conditions or blocks you want to delete.
2. Click **Delete**.
3. Click **Yes** on the confirmation message.
4. Click **OK** on the **Add Configuration Rule** or **Edit Configuration Rule** dialog box.

Predefined blocks

The Management application provides predefined blocks.

Table 96 lists the predefined blocks that can be used in a configuration rule.

TABLE 96 Predefined blocks

Name	Description	Use regular expression	Block Start	Block End
Network OS TenGigabit Ethernet Interfaces	Processes all 10 Gigabit Ethernet Interfaces on a Network OS device.	Yes	interface TenGigabitEthernet .*	!
Network OS Gigabit Ethernet Interfaces	Processes all Gigabit Ethernet Interfaces on a Network OS device.	Yes	interface GigabitEthernet .*	!
Network OS Vlan Interfaces	Processes all VLAN Interfaces on a Network OS device.	Yes	interface Vlan .*	!
Network OS LAG Interfaces	Processes all LAG Interfaces on a Network OS device.	Yes	interface Port-channel .*	!
Network OS Protocol LLDP	Processes the protocol LLDP block.	No	protocol lldp	!
IronWare OS Ethernet Interfaces	Processes all Ethernet ports on the IronWare device.	Yes	interface ethernet .*	!
IronWare OS VLAN Interface	Processes VLANs on the IronWare device.	Yes	vlan .*	!
RFS AAA Policies	Processes all the AAA policies available for the RFS device.	Yes	aaa-policy.*	!
RFS Profile	Processes all the profiles available for RFS device.	Yes	profile.*	!

Running a policy monitor

Before you run a policy monitor, make sure your policy monitors are valid. Valid policy monitors must have at least one policy selected with one or more targets. Management checks do not require a target.

To run an existing policy monitor, complete the following steps.

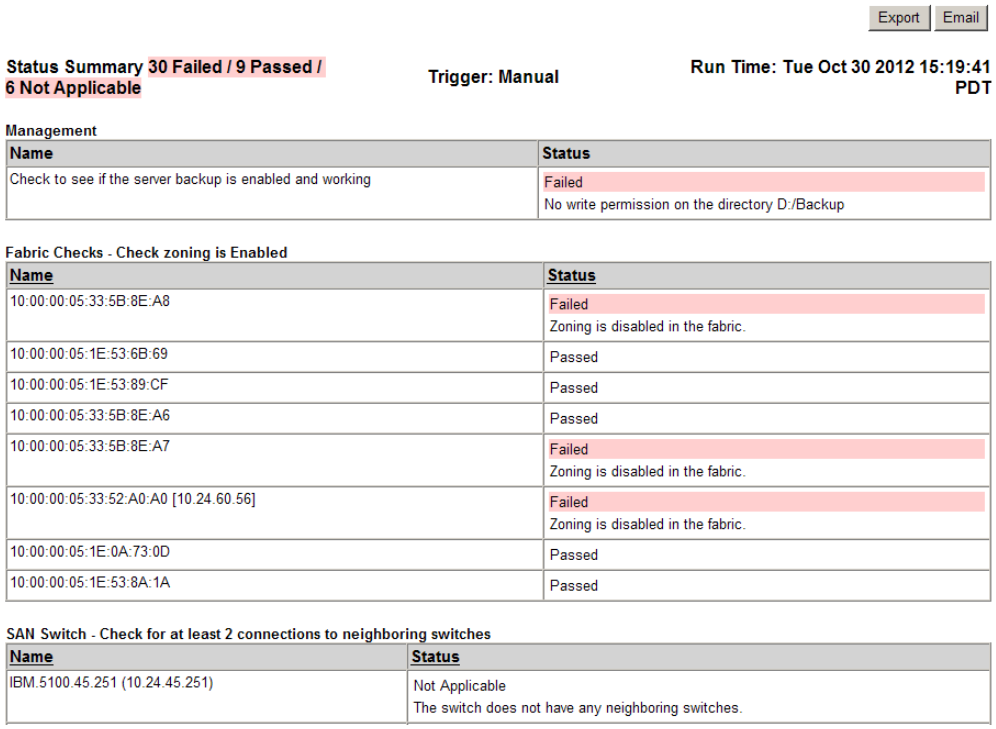
1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Select the policy you want to run in the **Monitors** list.

3. Click **Run**.

   When the policy monitor check is complete, the *Policy_Name* - **Policy Monitor Report** displays (Figure 466) in a web browser.



Export Email

Status Summary 30 Failed / 9 Passed / 6 Not Applicable **Trigger: Manual** **Run Time: Tue Oct 30 2012 15:19:41 PDT**

Management

Name	Status
Check to see if the server backup is enabled and working	Failed No write permission on the directory D:/Backup

Fabric Checks - Check zoning is Enabled

Name	Status
10:00:00:05:33:5B:8E:A8	Failed Zoning is disabled in the fabric.
10:00:00:05:1E:53:6B:69	Passed
10:00:00:05:1E:53:89:CF	Passed
10:00:00:05:33:5B:8E:A6	Passed
10:00:00:05:33:5B:8E:A7	Failed Zoning is disabled in the fabric.
10:00:00:05:33:52:A0:A0 [10.24.60.56]	Failed Zoning is disabled in the fabric.
10:00:00:05:1E:0A:73:0D	Passed
10:00:00:05:1E:53:8A:1A	Passed

SAN Switch - Check for at least 2 connections to neighboring switches

Name	Status
IBM.5100.45.251 (10.24.45.251)	Not Applicable The switch does not have any neighboring switches.

FIGURE 466 *Policy_Name* - Policy Monitor Report

4. Review the report details (refer to "Viewing a policy monitor report" on page 1136).

   To export a report, refer to "Exporting a policy monitor report" on page 1138.

   To e-mail a report, refer to "Exporting IP reports to e-mail recipients" on page 1232.

5. Click the close button (**X**) on the *Policy_Name* - **Policy Monitor Report** browser window.

6. Click **Close** on the **Policy Monitor** dialog box.

Viewing a policy monitor report

NOTE
You must run the policy monitor at least once before you can view a report.

To view an existing policy monitor report, complete the following steps.

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Select the policy for which you want to view a report in the **Monitors** list.

3. Click **Report**.

   NOTE
   If you have run this policy more than once, the latest report displays.

   The *Policy_Name* **- Policy Monitor Report** displays (Figure 466) in a web browser.

4. Review the report details:

   - **Name** — Name of the policy monitor report.
   - **Date** — Date and time the report was finished.
   - **Export** button — To export a report, refer to "Exporting a policy monitor report" on page 1138.
   - **E-Mail** button — To e-mail a report, refer to "Exporting IP reports to e-mail recipients" on page 1232.
   - **Status Summary —** Number of checks that passed, partially failed, failed, not applicable, or unknown.

     When a policy status fails or partially fails, the status is highlighted in pink.
   - **Trigger** — Trigger for the report. Valid results include Manual, Event Action, and Scheduled.
   - **Run Time** — Date and time the report was triggered.
   - *Individual_Policy_Checks* — Name of the policy check and a table displaying the results of the check. The following information is included in the report data for each policy check:

     Management Check — Displays the status of the management check. The management check provides the following information:

     - **Name** — Name of the management check.
     - **Status** — Result of the check and reason for failure if known. Valid results include Passed, Partially Failed, Failed, Not Applicable, and Unknown.

     Fabric Checks — Fabric checks provide the following information for each selected check:

     - **Name** — Fabric name.
     - **Status** — Result of the check and reason for failure if known. Valid results include Passed, Partially Failed, Failed, Not Applicable, and Unknown.

Fabric checks include the following options:

- Check zoning is enabled
- Check that all zones belong to at least one zone configuration
- Check the number of initiator ports zoned to each storage port is less than *Configured_Value*. This check provides the following additional detail for this check:
  - **Storage Port** — WWN of the storage port.
  - **Initiator Count** — Number of initiator ports zoned to the storage port.
  - **Initiator Port** — WWN of the initiator port.
  - **Zone** — Zone name containing the initiator/storage port zoning pair.
- Check zones that do not contain any online member. This check lists the zones that contain only offline members.
- Ethernet Fabric — Checks that all profiles are the same on each RBridge in an Ethernet fabric. This check provides the following additional detail for this check:
  - **Profile —** Name of the profile.
  - **Status —** Whether the profile matched (Passed) or did not match (Failed).
  - **RBridge ID (Matching Sets)** — Number of matching or missing sets. For example, (Missing: 73) (Matching: 2).

Switch Checks — Switch checks provide the following information for each selected check:

- **Name** — Product name.
- **Status** — Result of the check and reason for failure if known. Valid results include Passed, Partially Failed, Failed, Not Applicable, and Unknown.

Switch Checks include the following options:

- Switch — Check for HTTPS (secure HTTP) configuration. This check provides the following additional detail for this check:
  - **HTTPs Status —** Whether HTTPS is enabled or disabled on the product.
  - **HTTP Status —** Whether HTTP is enabled or disabled on the product.
- Switch — Check if the product is configured to send events to this server.
- Switch - Check for SSH (secure Telnet) configuration.This check provides the following additional detail for this check:
  - **SSH Status —** Whether SSH is enabled or disabled on the product.
  - **Telnet Status —** Whether Telnet is enabled or disabled on the product.
- Switch - Check for SNMPv3 (secure SNMP) configuration. This check provides the following additional detail for this check:

- **SNMPv3 Status —** Whether SNMPv3 is enabled or disabled on the product.
- **SNMP Status —** Whether SNMP is enabled or disabled on the product.

- Switch - Check for VLAN configurations match for each connection (IP only). This check provides the following additional detail for this check:
  - **Local Switch Port —** Name of the local switch port.
  - **Local VLANs** — Local VLAN number
  - **Status** — Whether the configurations matched (Passed) or did not match (Failed).
  - **Remote VLANs** — Remote VLAN number.
  - **Remote Port** — Name of the remote switch port.
  - **Remote Switch** — Name and IP address of the remote switch.
- Configuration Rule Checks — Switch checks provide the following information for each selected check:
  - **Block/Condition Name —** Name of the block or condition.
  - **Matched Block —** Name of the matched block.
  - **Status** — Whether the configurations matched (Passed) or did not match (Failed).
  - **Failed Condition —** Name of the failed condition.
  - **Match/Not Match —** Whether the configurations matched (Match) or did not match (Not Match).
  - **Condition Details —** Details about the condition.
  - **Remediation —** Details how to correct the failure, if the condition fails.

Host Checks — Switch checks provide the following information for each selected check:

- **Name** — Product name.
- **Status** — Result of the check and reason for failure if known. Valid results include Passed, Partially Failed, Failed, Not Applicable, and Unknown.

Displays the Host name and status of the policy check for the following option:

- Host — Check for at least *Configured_Minimum_Value* connections to attached fabrics
- Host — Check for connections through two fabrics to each target LUN. This check provides the following additional detail for this check:
  - **LUN Serial #** — LUN serial number.
  - **Adaptor Port** — Host adapter port number.
  - **Fabric** — Fabric name.
  - **Storage Port** — Storage port number.

5. Click the close button (X) on the *Policy_Name* - **Policy Monitor Report** browser window.
6. Click **Close** on the **Policy Monitor** dialog box.

Exporting a policy monitor report

1. Click **Export**.

   The **File Download** dialog box displays.

2. Click **Save**.

The **Save** dialog box displays.

3. Browse to the file location where you want to save the report and click **Save**.
4. Click the close button (X) on the *Policy_Name* - **Policy Monitor Report** browser window.

Viewing historical reports for all policy monitors

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Click **History.**

   The **Report History** dialog box displays the last 10 reports run for all monitors. The **Report History** dialog box retains up to 10 reports for each policy monitor.

   - **Name** — Name of the policy monitor.
   - **Date** — Date and time the report was finished.
   - **Result** — Result of the policy monitor run. Valid results include Passed, Partially Failed, Failed, Not Applicable, and Unknown.

3. Select the report you want to view and click **Display**.

   The *Policy_Name* - **Policy Monitor Report** displays in a web browser. For detailed information about reports, refer to "Viewing a policy monitor report" on page 1136.

4. Click the close button (X) on the *Policy_Name* - **Policy Monitor Report** browser window.
5. Click **Close** on the **Report History** dialog box.

Viewing historical reports for a policy monitor

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Select the policy for which you want to view the report history and click **History.**

   The **Report History** dialog box displays. The **Report History** dialog box displays up to 10 reports for the selected policy monitor.

   - **Name** — Name of the policy monitor.
   - **Date** — Date and time the report was finished.
   - **Result** — Result of the policy monitor run. Valid results include Passed, Partially Failed, Failed, Not Applicable, and Unknown.

3. Select the report you want to view and click **Display**.

   The *Policy_Name* - **Policy Monitor Report** displays in a web browser. For detailed information about reports, refer to "Viewing a policy monitor report" on page 1136.

4. Click the close button (X) on the *Policy_Name* - **Policy Monitor Report** browser window.
5. Click **Close** on the **Report History** dialog box.

Chapter

37

Fault Management

In this chapter

Fault management overview

Fault management enables you to monitor your managed SAN and IP networks using the following methods:

- Listen, forward, and process SNMP traps for SAN and IP devices, which eliminates the need to poll devices for events.
- Receive and forward Syslog messages from Fabric OS switches, IP devices, and Brocade adapters — HBAs and CNAs are managed using the Host Connectivity Manager (HCM) Agent.
- Manage pseudo events.
- Configure the following event actions:
  - Logging policy
  - E-mail alerts
  - Scripts
  - Broadcast to clients
  - Special events handling
  - Deploy CLI configurations (IP only)
- Monitor audit logs and event logs for specified conditions.
- Support application events.

Restrictions

The following items affect Fault Management operation.

Supported IP address types

The Management application receives traps and syslog messages for physical IP addresses only.

Event Purging

The default maximum number of days that historical events are stored is 365. You can select a different default (from 1 to 365) in the Options dialog box under **Event Storage**.

Event Archiving

The default number of days that purged events are archived is 30. This value cannot be changed.

Event notification

The Management application records the SAN and IP events in the Master Log. You can configure the application to send event notifications to e-mail addresses at certain time intervals. This is a convenient way to keep track of events that occur on the SAN and IP networks. You can also configure products to “call home” for certain events, notifying the service center of product problems. For instructions about configuring call home for events, refer to “Call Home” on page 343.

Configuring e-mail notification

To send e-mail notification of events to users, complete the following steps.

1. Select **Monitor > Event Notification > E-mail**.

   The **E-mail Event Notification Setup** dialog box (shown in Figure 467) displays.

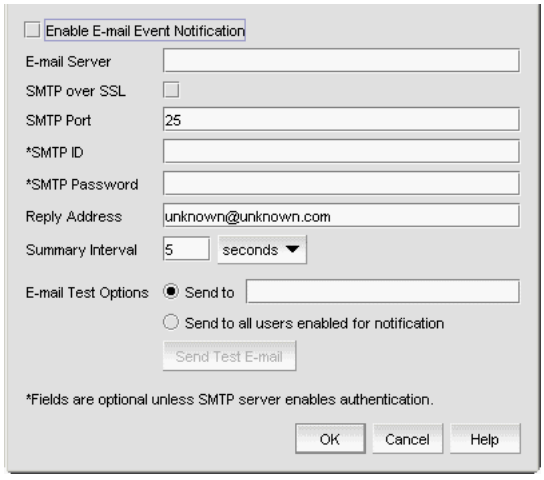


FIGURE 467 E-mail Event Notification Setup dialog box

2. Select the **Enable E-mail Event Notification** check box to enable the application to send e-mail messages in case of event notifications.
3. Enter the IP address or the name of the SMTP mail server that the server can use to send the e-mail notifications in the **E-mail Server** field.

   The Management application accepts IP addresses in IPv4 and IPv6 formats. The IPv4 format is valid when the operating system has IPv4 mode only or dual stack mode. The IPv6 format is valid when the operating system has IPv6 mode only or dual stack mode.
4. Select the **SMTP over SSL** check box to enable secure communication.
5. Enter the port number of the SMTP mail server in the **SMTP Port** field.

   If SMTP over SSL is not enabled, the default is 25.

   If SMTP over SSL is enabled, the default is 465.
6. Enter the authentication ID of the SMTP mail server in the **SMTP ID** field.

   NOTE
   The **SMTP ID** field is optional unless the SMTP server enables authentication.
7. Enter the authentication password of the SMTP mail server in the **SMTP Password** field.

   NOTE
   The **SMTP Password** field is optional unless the SMTP server enables authentication.
8. Enter the sender's e-mail address in the **Reply Address** field.
9. Enter the length of time the application should wait between notifications in the **Summary Interval** field and list.

   Notifications are combined into a single e-mail message and sent at each interval setting. An interval setting of zero causes notifications to be sent immediately.

   ATTENTION
   Setting too short an interval can cause the recipient's e-mail inbox to fill *very* quickly.
10. Select one of the following e-mail test options:
    - Select **Send to** and enter an e-mail address for a user to send a test e-mail message to a specific user.
    - Select **Send to all users enabled for notification** to send a test e-mail message to all users already set to receive notification.
11. Click **Send Test E-mail** to test the e-mail server.

    A message displays whether the server was found. If the server was not found, verify that the server address was entered correctly and that the server is running. If you are using an SMTP mail server, also verify that the SMTP ID and password information was entered correctly.
12. Click **OK** to save your work and close the **E-mail Event Notification Setup** dialog box.

Defining filters

The **Define Filter** dialog box, shown in Figure 468, allows you to define event filters by product, event category, and severity. You can define event filters on SAN products, IP products, or hosts.

Setting up basic event filtering

To set up advanced event filtering on the selected events for a user, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select a user in the **Users** list and click **Edit**.

   The **Edit User** dialog box displays.

3. Select the **E-mail Notification Enable** check box and click the **Filter** link.

   The **Define Filter** dialog box, shown in Figure 468, displays.

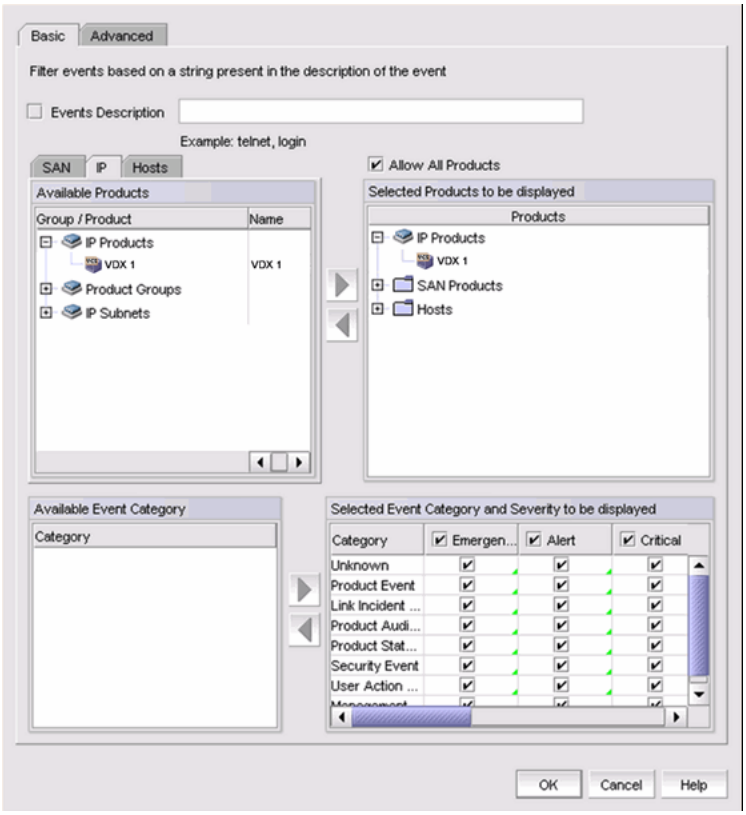


FIGURE 468 Define Filter dialog box

4. Select which product type you are defining (SAN, IP, or Hosts) and click the appropriate tab.
5. Select the **Events Description** check box and enter a description of the event in the field.
6. Select the **Allow Products** check box to control whether or not all products are always displayed.

- When selected (the default), all products, even newly-added products, are added to the **Selected Products to be displayed** list.
- If the check box is cleared, only the products listed in the **Selected Products to be displayed** list are shown in the Master Log and all newly-added products are added to the **Available Products** list.

7. Select one or more event categories from the **Available Event Category** list and click the right arrow button to move it to the **Selected Event Category and Severity to be displayed** list. You can move any or all event categories.
8. Select at least one severity for each event. Severity options include Emergency, Alert, Critical, Error, Warning, Notice, Debug, Info, and Unknown.

NOTE
If you delete event actions that are part of the filtering criteria, they will not display in the Master Log, which displays in the lower left area of the main window, and lists all events and alerts that have occurred on the managed networks.

Setting up advanced event filtering

To set up advanced event filtering on the selected events for a user, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.
2. Select a user in the **Users** list and click **Edit**.

   The **Edit User** dialog box displays.
3. Select the **E-mail Notification Enable** check box and click the **Filter** link.

   The **Define Filter** dialog box displays.
4. Click **Advanced**.

   The **Advanced** tab of the **Define Filter** dialog box, shown in Figure 469, displays.

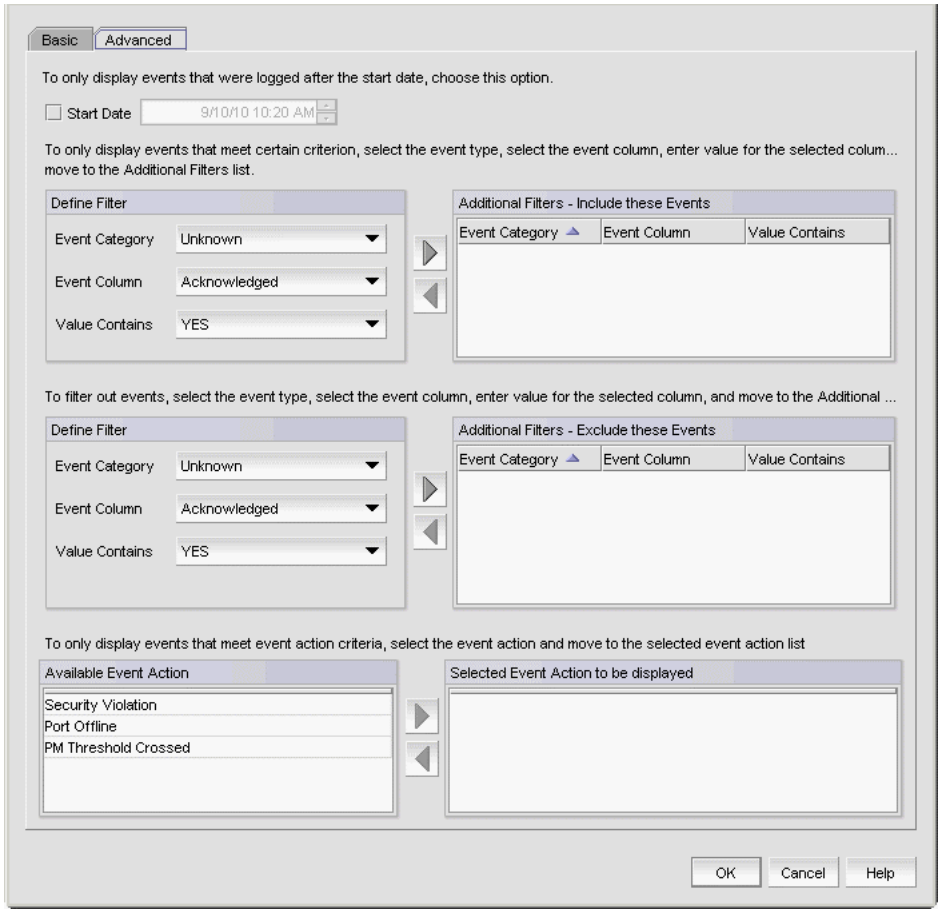


FIGURE 469 Define Filter dialog box - Advanced tab

5. Select the **Start Date** check box to display only the events that were logged after the specified start date. The default start date and time is the current date and time.
6. To include events in the event filter, complete the following steps.
   a. Select the event type you want to include from the **Event Category** list.

      All event types are listed in alphabetical order.

   b. Select the event column for the event from the **Event Column** list.

      All event columns are listed in alphabetical order.

   c. Enter all or part of the event type value in the **Value Contains** field.

   d. Click the right arrow button to move the event type to the **Additional Filters - Include these Events** list.

   e. To add additional filters, repeat step a through step d.
7. To exclude events from the event filter, complete the following steps.

NOTE
You can configure a maximum of ten filters to be included.

a. Select the event type you want to remove from the **Event Category** list.

   All event types are listed in alphabetical order.

b. Select the event column for the event from the **Event Column** list.

   All event columns are listed in alphabetical order.

c. Enter all or part of the event type value in the **Value Contains** field.

d. Click the right arrow button to move the event type to the **Additional Filters - Exclude these Events** list.

e. To remove additional filters, repeat step a through step d.

8. To display events generated by an event action, select the event action from the **Available Event Action** list and click the right arrow button to move it to the **Selected Event Action to be displayed** list.
9. Click **OK** to close the **Define Filter** dialog box.

SNMP traps

Simple Network Management Protocol (SNMP) provides a means to monitor and control network products and to manage configurations, statistics, performance, and security through authentication and privacy protocols.

The Management application allows you to configure SNMP traps. The SNMP configuration tasks are described in the following sections:

Adding a trap recipient to one or more switches

The **SNMP Trap Recipients** dialog box allows you to register any recipient as a trap recipient on selected products. You can register different recipients for different products.

NOTE
You can register and unregister other recipient servers on the Fabric OS switches on a per-switch basis. For IP products, you can perform registration only at the switch level.

To add a trap recipient to one or more switches, complete the following steps.

1. Select **Monitor > SNMP Setup > Product Trap Recipients**.

   The **SNMP Trap Recipients** dialog box, shown in Figure 470, displays.

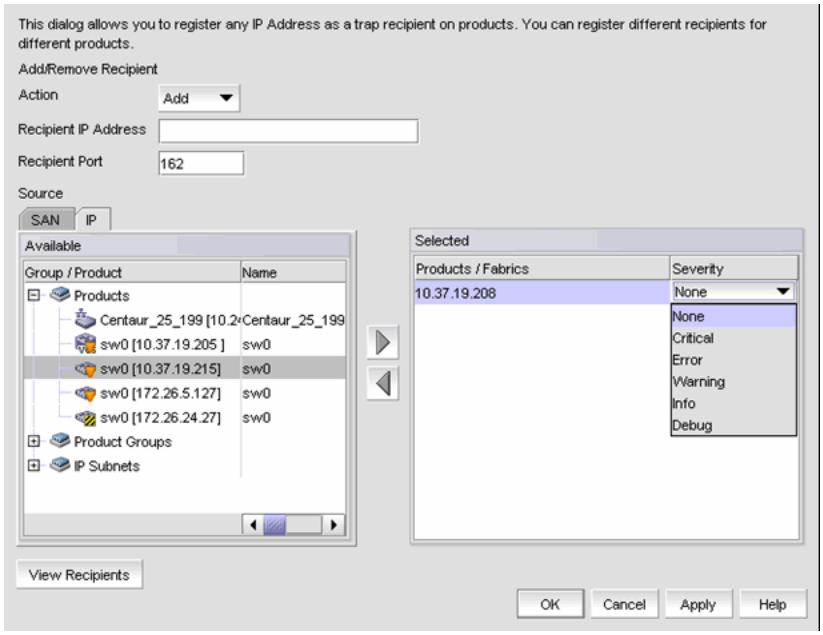


FIGURE 470 SNMP Trap Recipients dialog box

2. Click **Add** from the **Action** list.
3. Enter the IP address of the SNMP trap receiver (the recipient server) in the **Recipient IP Address** field. This is a mandatory field. IPv4 addresses are accepted, but a Domain Name System (DNS) name is not accepted.
4. Enter the SNMP trap port of the recipient in the **Recipient Port** field. This is a mandatory field. Valid numeric values range from 1 through 65535 and 162 is the default.
5. Select the fabric or switches from the **Available** list and click the right arrow button to move it to the **Selected** list. You can select multiple products.

   NOTE
   For IP products and product groups, only switches are available to select.

6. If the selected product is a SAN or Network OS device, select a severity from the **Severity** list. Severity levels can be one of the following: None, Critical, Error, Warning, Info, or Debug. The **Severity** list is disabled for IP products. None is the default.

7. Click the **View Recipients** button to list the recipients that correspond to a selected fabric or product from the **Available** list.

   The **Trap Recipients - Fabric** dialog box or the **Trap Recipients - IP address** dialog box (depending on which product you selected) displays a list of configured recipients.

8. Click **OK**.

   The Management application registers the recipient IP address as an SNMP trap recipient. The SNMP version and credentials from the SNMP profile (for example, SNMP v3) are registered.

Removing a trap recipient from one or more switches

To remove a trap recipient from one or more switches, complete the following steps.

1. Select **Monitor > SNMP Setup > Product Trap Recipients**.

   The **SNMP Trap Recipients** dialog box, shown in Figure 470, displays.

2. Click **Remove** from the **Action** list.
3. Enter the IP address of the SNMP trap port (the recipient server) in the **Recipient IP Address** field.
4. Select the fabric or switches from the **Available** list.

   NOTE
   For IP products, only switches are available to select.

5. Click **OK**.

   The Management application removes the recipient from the managed switches.

SNMP trap forwarding

The **SNMP Trap Forwarding** dialog box allows the Management application to forward received SNMP traps to product trap recipients.

You can use the SNMP Trap Forwarding feature to set up filters to determine which traps will be forwarded. The filters can be one of the following:

- Severity of the trap
- Available products type
- Trap type
- Message types (application messages or pseudo events)

To forward SNMP traps, complete the following steps.

1. Select **Monitor > SNMP Setup > Trap Forwarding**.

   The **SNMP Trap Forwarding** dialog box, shown in Figure 471, displays.

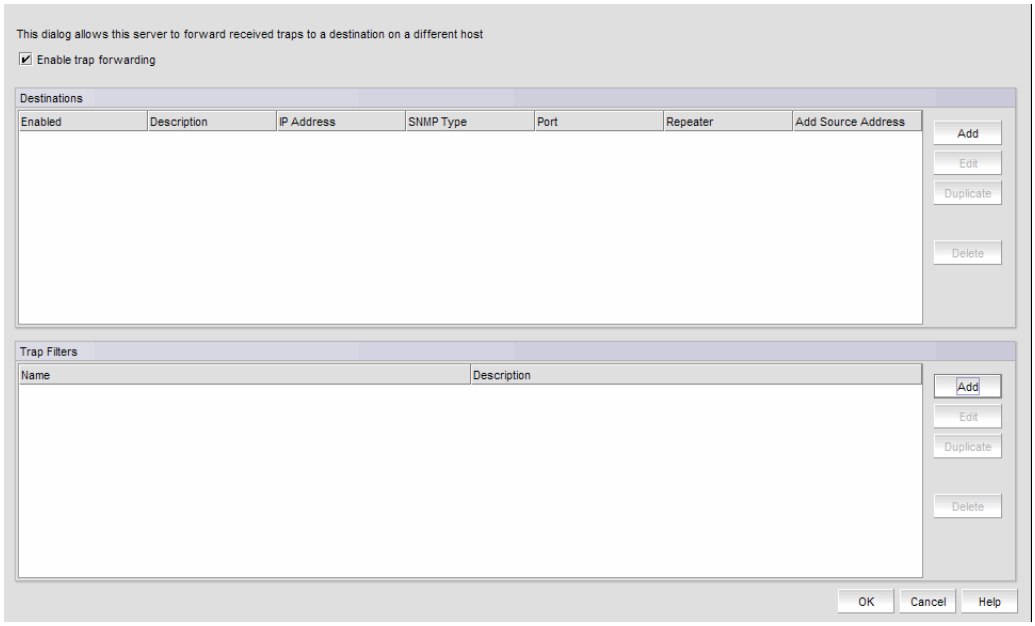


FIGURE 471 SNMP Trap Forwarding dialog box

Adding a trap destination

The **Add Trap Destination** dialog box allows you to configure destinations for forwarding SNMP traps.

To add a trap destination, complete the following steps.

1. Select **Monitor > SNMP Setup > Trap Forwarding**.

   The **SNMP Trap Forwarding** dialog box, shown in Figure 471, displays.

2. Select the **Enable trap forwarding** check box.

3. Click **Add** in the **Destinations** area of the **SNMP Trap Forwarding** dialog box.

   The **Add Trap Destination** dialog box, shown in Figure 472, displays.

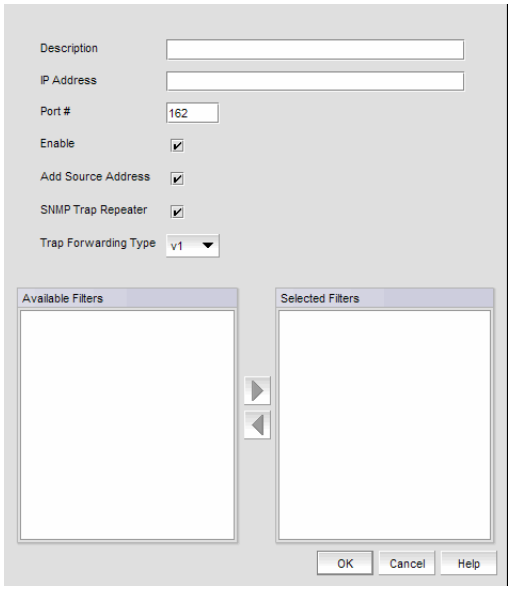


FIGURE 472 Add Trap Destination dialog box

4. Enter a general description of the trap destination in the **Description** field.
5. Enter the IP address of the trap destination in the **IP Address** field. This is a mandatory field. IPv4 and IPv6 addresses are accepted, but a DNS name is not accepted.
6. Enter the SNMP trap listening port of the recipient in the **Port #** field. This is a mandatory field. Valid numeric values range from 1 through 65535.

   The **Enable** check box, **Add Source Address** check box, and **SNMP Trap Repeater** check box are selected by default. When selected, all traps, whether the source is managed or unmanaged, are forwarded. When unselected, only traps from the selected products are forwarded. When selected, the Open View Source Name is added to the variable binding (varbind) value to the trap before forwarding.
7. Select a supported SNMP type from the **Trap Forwarding Type** list. Supported SNMP types are v1, v2c, and v3. The default SNMP type is v1.
8. You can choose not to select a filter (zero), or you can select up to five filters from the **Available Filters** list. Click the right arrow button to move them to the **Selected Filters** list.
9. Click **OK**.

Adding a new trap filter

The **Add Trap Filter** dialog box allows you to configure trap filters for forwarding SNMP traps. You can add trap filters on SAN products, IP products, or hosts. These filters can be on individual switches or the Fabric as a whole.

To add a new trap filter, complete the following steps.

1. Select **Monitor > SNMP Setup > Trap Forwarding**.

   The **SNMP Trap Forwarding** dialog box displays.

2. Click **Add** in the **Trap Filters** area of the **SNMP Trap Forwarding** dialog box.

   The **Add Trap Filter** dialog box, shown in Figure 473, displays.

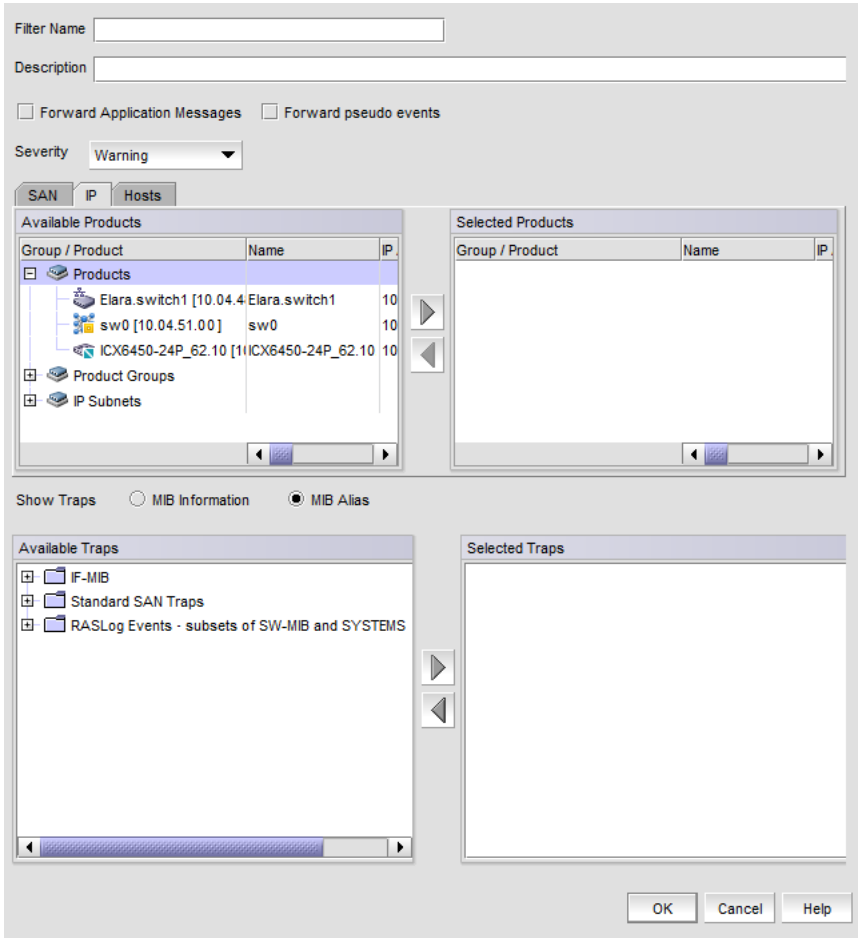


FIGURE 473 Add Trap Filter dialog box

3. Enter a unique name for the trap filter in the **Filter Name** field.
4. Enter a general description of the trap filter in the **Description** field.
5. Select the **Forward Application Messages** check box to forward application events.
6. Select the **Forward pseudo events** check box to forward pseudo events.
7. Select a severity level from the **Severity** pulldown menu. The severity level can be one of the following, and appear in descending order of severity.
   - Emergency
   - Alert
   - Critical
   - Error
   - Warning
   - Notice
   - Info

- Debug

Traps with the selected severity and those with higher severity levels are forwarded. For example, by default, Critical severity is selected. Therefore, traps with Critical, Alert, and Emergency severity levels are forwarded. To have all traps forwarded, select Debug, the lowest severity level.

8. Select the **SAN**, **IP**, or **Hosts** tab. Depending on the tab selected, the products available to which you can add a trap filter display in the **Available Products** list.
9. By default, all traps are listed in the **Available Traps** list, under the folders for the MIB to which they belong. You can limit the list by selecting one of the following MIB types:
    - **MIB Information** - Select this check box if you want the default SNMP name for the traps to be displayed.
    - **MIB Alias** - Select this check box if you want the aliases for traps to be displayed.
10. After limiting the list of available traps, expand the MIB folder to which the trap you want belongs under the **Available Trap Type** list and select that trap. Click the right arrow button to move it to the **Selected Trap Type** list.
11. Click **OK**.

    SNMP Traps and Syslog messages from the selected switches or Fabric will now be forwarded to the configured destination server.

Event reception

The Event Reception feature provides an interface to add the credentials and community strings required to decode traps. You can use the **Event Reception** dialog box to configure the trap message, severity, and alias name that is used by the Event Processor.

The **Event Reception** dialog box contains two tabs:

- The **Trap Credentials** tab allows you to configure the server to accept or drop SNMP traps and add SNMP credentials and community strings for decoding traps.
- The **Trap Configuration** tab allows you to customize the trap description or message, severity, and alias name.

To access the **Event Reception** dialog box, select **Monitor > SNMP > Event Reception**.

The **Event Reception** dialog box, shown in Figure 474, displays.

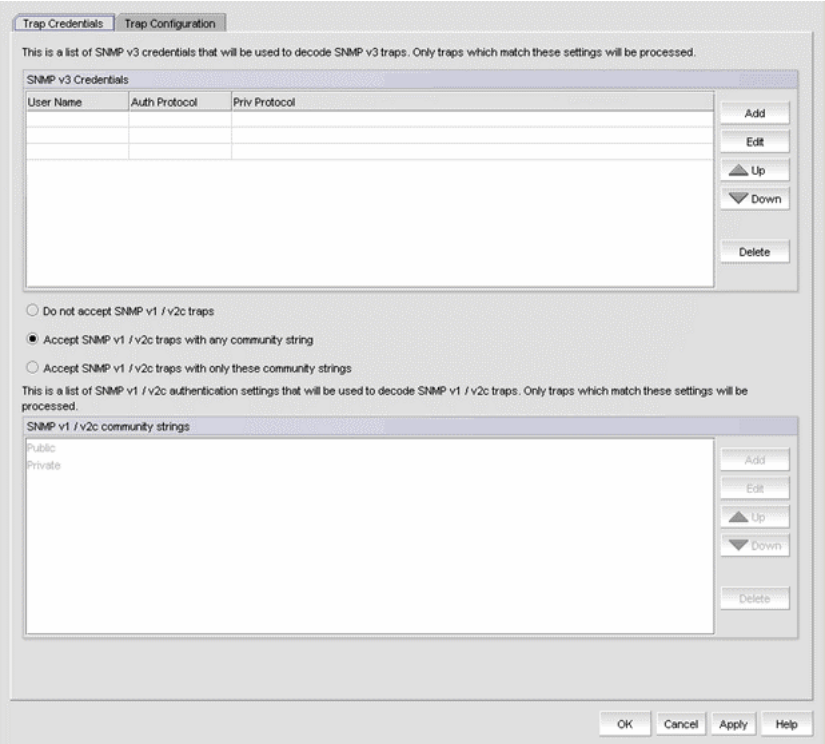


FIGURE 474 Event Reception dialog box - Trap Credentials tab

By default, the Management application receives SNMP v1 and v2c traps from IronWare OS and Network OS IP products that have any SNMP community strings. You can accept or restrict SNMP v1 and v2c traps by selecting one of the following check boxes in the **Event Reception** dialog box:

- **Do not accept SNMP v1/v2c traps**

  Use this option to turn off receiving SNMP v1 and v2c traps.If selected, the Management application will not receive any SNMP v1 and v2c traps.

- **Accept SNMP v1/v2c traps with any community string**

  Use this option to turn on receiving SNMP v1 and v2c traps with any community string.

- **Accept SNMP v1/v2c traps with only these community strings**

  Use this option to turn on receiving SNMP v1 and v2c traps with only the specified community strings.

The Management application can receive SNMP v1 traps from Fabric OS SAN switches and directors that have any SNMP community strings. It can receive SNMP v3 traps and informs from these SAN products.

Table 97 explains the combinations of security and authentication, which will help you when you make your SNMP credentials configuration decisions.

TABLE 97 SNMP security and authentication

SNMP credential type	Privacy protocol	Authentication	Result
v1	No authentication No privacy protocol	Community string	Uses a community string to match for authentication.
v2c	No authentication No privacy protocol	Community string	Uses a community string to match for authentication.
v3	No authentication No privacy protocol	User name	Uses a user name to match for authentication.
v3	Authentication No privacy protocol	MD5 or SHA	Provides authentication based on the HMAC-MD5 (Message Digest Algorithm) or HMAC-SHA algorithms (Secure Hash Algorithm).
v3	Authentication Privacy protocol	MD5 or SHA	Provides authentication based on the HMAC-MD or HMAC-SHA algorithms (Hash-based Message Authentication). Provides privacy based on CBC_DES (Cipher Block Chaining) or CFB_AES_128 (Cipher Feedback).

For information about how to configure SNMP credentials, refer to "Adding an SNMP v3 credential" on page 1155 or "Adding an SNMP v1 or v2c community string" on page 1156.

Adding an SNMP v3 credential

The **SNMP v3 Credentials** dialog box allows you to add the SNMP v3 credentials.

To add an SNMP v3 credential, complete the following steps.

1. Select **Monitor > SNMP Setup > Event Reception**.

   The **Event Reception** dialog box displays.

2. Select an SNMP v3 credential from the **SNMP v3 Credentials** list on the **Event Reception** dialog box.

3. Click **Add**.

   The **Add SNMP v3 Credentials** dialog box, shown in Figure 475, displays.

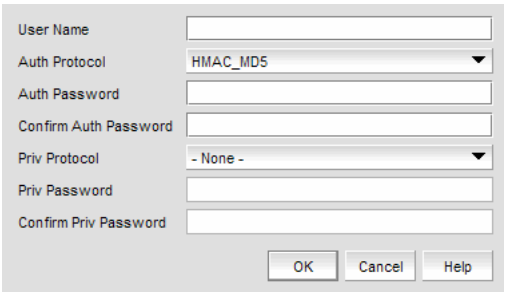


FIGURE 475 Add SNMP v3 Credentials dialog box

4. Type the user name in the **User Name** field.

   For configurations that do not have authentication or privacy, the Management application uses the user name to match for authentication.

5. Select an authentication protocol from the **Auth Protocol** list. You can select -None-, HMAC-MD5, or HMAC_SHA. HMAC_MD5 is the default.

   If you select no authentication, the Management application uses the user name to match for authentication.

6. Type a password in the **Auth Password** field and re-type the password in the **Auth Confirm Password** field.

7. Select a privacy protocol from the **Priv Protocol** list. You can select -None-, CBC_DES, or CFB_AES_128.

   If you select no privacy, the Management application uses the user name to match for authentication.

8. Type a password in the **Priv Password** field and re-type the password in the **Confirm Priv Password** field.

9. Click **OK**.

Adding an SNMP v1 or v2c community string

The **SNMP v1/2 Community String** dialog box allows you to add the SNMP v1 or v2c credentials.

To add an SNMP v1 or v2c community string credential, complete the following steps.

1. Select **Monitor > SNMP Setup > Event Reception**.

   The **Event Reception** dialog box displays.

2. Click the **Accept SNMPv1/v2c traps with only these community strings** button.

3. Click **Add**.

   The **SNMP v1/v2c Community String** dialog box, shown in Figure 476, displays.

FIGURE 476 SNMP v1/v2 Community String dialog box

4. Enter a unique community string in the **Community String** field, which will be used to match for authentication in SNMP v1 and v2c configurations. This field is case-sensitive.

5. Re-enter the string in the **Confirm Community String** field.

6. Click **OK**.

Importing a new MIB into the Management application

The SNMP traps that the Management application receives must be registered in the Management application in order for these traps to be available. To register a trap, you must first identify the MIB file that contains the trap information in the mibs_to_compile.txt file. Then, you must register the traps using the **Event Reception** dialog box.

To add the MIB file that contains the trap you want to register to mibs_to_compile.txt, complete the following steps.

1. Go to <*install-dir*>\conf\mibs\ (Windows) or <*install-dir*>/conf/mibs/ (UNIX) directory and copy the MIB file into that directory. You may want to copy the MIB into a subdirectory of that directory.
2. In the <*install-dir*>\conf\mibs\ (Windows) or <*install-dir*>/conf/mibs/ (UNIX) directory, search for the mibs_to_compile.txt file.
3. Using a text editor, open the mibs_to_compile.txt file and add the MIB information to the document.

   When adding the MIB information, be aware of the following rules:

   - MIBs are compiled in the order that they are listed in the mibs_to_compile.txt file.
   - You can add composite MIB files (more than one MIB in a single file).
   - MIB file names in the mibs_to_compile.txt file are case-sensitive. Make sure the case of the file name you enter matches the case of the actual MIB file. Also, be sure to enter the complete path of the MIB file, or the portion relative to the mibs directory.

   The following is an example of how to add the two Cisco MIB files.

```
#
# Cisco Mibs
#
CISCO-SMI.mib
CISCO-CONFIG-COPY-MIB.mib
#
# End Cisco Mibs
#
```

4. Save the file.

   The Management application recompiles all the MIB files. If compilation is successful, the traps can now be registered in the **Event Reception** dialog box.

   NOTE
   If there are compilation errors, you can view the errors in the server log: <*install dir*>\logs\server\server.log (Windows) or <*install dir*>/logs/server/server.log (UNIX).

5. If you make changes to the MIB file, open the mibs_to_compile.txt file and save the file.

   The Management application recompiles the MIB files and reloads the changes.

Trap customization

The **Trap Configuration** tab of the **Event Reception** dialog box enables you to configure the following settings:

- Register and unregister various Management Information Bases (MIBs)
- Customize trap description messages based on varbinds and severity and specify alias names

Registering traps

Traps must be registered in the **Event Reception** dialog box to make them available.

To register traps, complete the following steps.

1. Select **Monitor > SNMP Setup > Event Reception**.
2. Click the **Trap Configuration** tab.

   The **Trap Configuration** tab of the **Event Reception** dialog box, shown in Figure 477, displays.

   The **Registered** and **Not Registered** buttons at the top of the Traps tree serves as a filter for the traps. If there are unregistered traps, they are listed when you select the **Not Registered** button.

   Traps appear under each MIB folder. The MIB folders correspond to the MIBs identified in the mibs_to_compile.txt file.

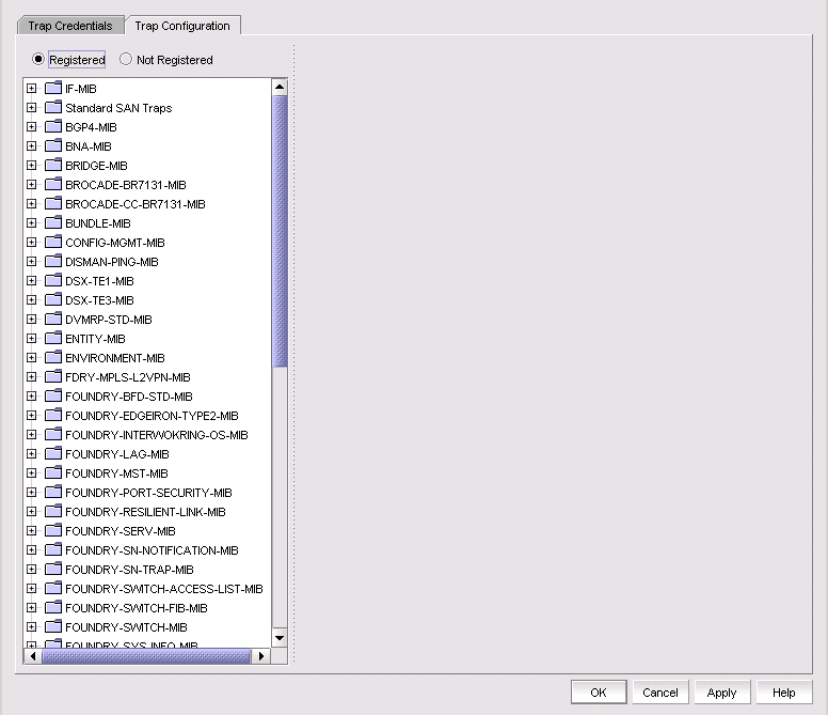


FIGURE 477 Trap Configuration tab of the Event Reception dialog box

3. Expand a folder for a MIB to display the traps in the MIB. If the list is too long, use the Search tool to find a MIB or trap.
4. Select the trap you want to register.

   The SNMP name and Object Identification (OID) of the trap appear at the top line of the configuration pane. Also, the status of the trap shows **Not Registered**, which is the default definition of the trap.

   Details about the trap appear in the fields beneath the **MIB Name** field.

Trap details supply the following information:

- The name of the MIB to which the trap belongs
- Information about the trap
- Any variable bindings (varbinds) that the trap uses. Information about the varbind, its name, OID, and type, is displayed
- Recommended action specified by the user

5. Enter the following information:
   a. Select the severity level you want to assign to the trap from the **Severity** list. If you do not select a severity, it defaults to Emergency.
   b. Enter the message you want to display for this trap in the **Message** field. If the trap has varbinds, use $#, where # represents the varbind number, to indicate the varbind. You must enter a message.
   c. Enter an alias string that serves as a second name for the trap in the **MIB Alias** field. This string might be more understandable to users. This parameter is optional. The Event Processor uses this alias, and this alias is displayed in the Event Action.
   d. Configure the recommended action for the trap.
6. When you have finished, click **OK** to accept your entries.

   The status of the trap changes to **Registered - Customized** and the trap appears in the Event Log.

Unregistering a registered trap

You can unregister only the traps that you have registered. You cannot unregister traps that come with the Management application by default.

To unregister a trap that you have registered, complete the following steps.

1. Select **Monitor > SNMP Setup > Event Reception**.
2. Click the **Trap Configuration** tab.
3. Click the **Registered** button.

   The Trap tree displays the MIBs that contain the registered traps.
4. Expand a MIB folder to display the traps that have been registered for that MIB.
5. Select a trap to display its current definition.
6. Click the **Not Registered** button.
7. Click **OK**.

   Once unregistered, the status of the trap changes to **Not Registered**.

Customizing a registered trap definition

To modify the definitions of registered traps, complete the following steps.

1. Click the **Trap Configuration** tab.
2. Click the **Registered** button.

The Trap tree displays the MIBs that contain the registered traps.

3. Expand a MIB folder to display the traps that have been registered for that MIB.
4. Select a trap to display its current definition. You can change the severity, message, or alias of the trap.
5. When you have finished, click **OK** or **Apply** to accept your entries.

   If you modified a default trap, its status changes from **Registered - Default** to **Registered - Customized**.

Reverting the customization of a registered trap to default

To revert to the default definitions of registered-customized traps, complete the following steps.

1. Click the **Trap Configuration** tab.
2. Click the **Registered** button.

   The Trap tree displays the MIBs that contain the registered traps.
3. Expand a MIB folder to display the traps that have been registered for that MIB.
4. Select a trap to display its current definition.
5. If the trap has been customized, a button labeled **Default** is available. Click **Default** to revert the previous changes to its default.

SNMP informs

The **SNMP Informs** dialog box allows you to enable or disable informs on informs-capable products. SNMP traps are unreliable because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. However, an SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the manager does not receive an inform request, it does not send a response. If the sender (switch) never receives a response, the inform request can be sent again. For this reason, informs are more likely to reach their intended destination.

When using informs, the engine ID must be set to correspond to the management engine IP address to authenticate the inform request. When informs are enabled, the sender sends initial informs **request** for engine ID discovery from any of its ephemeral ports (ranging from 32768 to 65535) to port 161 on the Management server. The sender receives the acknowledgement of the informs requests on these ephemeral ports. If there is a firewall between the Management application and the switches, the ephemeral ports must be open for SNMP informs to work.

Enabling or disabling SNMP informs

To enable or disable SNMP informs, complete the following steps.

1. Select **Monitor > SNMP Setup > Informs**.

   The **SNMP Informs** dialog box displays.
2. Select a product group from the **Fabric / Products** list.

The products display in the **SNMP Informs Capable Products** list, where you can determine if the product's status is enabled or disabled.

3. Select a product in the **SNMP Informs Capable Products** list and click the appropriate **Action** button, depending on whether you want to enable or disable SNMP informs for that product.
4. Click **OK**.

Syslogs

Use the **Options** dialog box to automatically register the Management application server as the syslog recipient on all managed SAN and IP products. The syslog listening port number is 514 by default. If you change the port number from 514, auto-registration is disabled.

NOTE
Network OS products do not support non-default Syslog port registration.

NOTE
IronWare OS 6910 switches are not listed in the **Syslog Recipient** dialog box.

Adding a syslog recipient

The **Syslog Recipients** dialog box allows you to register any recipient as a syslog recipient on selected products. You can register different recipients for different products.

You can register and unregister other recipient servers on the Fabric OS switches on a per-fabric basis. For IP products, you can perform registration only at the switch level.

NOTE
IPv6 Syslog registration is not supported for IronView OS products.

To add a syslog recipient, complete the following steps.

1. Select **Monitor > Syslog Configuration > Product Syslog Recipients**.

   The **Syslog Recipients** dialog box, shown in Figure 478, displays.

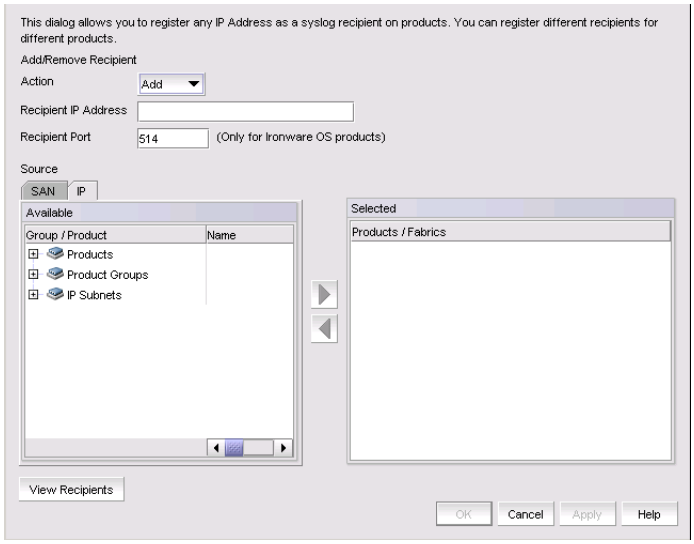


FIGURE 478 Syslog Recipients dialog box

2. Select **Add** from the **Action** list.
3. Enter the IP address of the syslog port (the recipient server) in the **Recipient IP Address** field. This is a mandatory field. IPv4 addresses are accepted, but a DNS name is not accepted.
4. Enter the syslog port of the recipient in the **Recipient Port** field. Valid numeric values range from 1 through 65535. The default value is 514.

NOTE
For IronWare products, a non-default port can be registered. For Network OS and Fabric OS products, non-default ports cannot be registered.

5. Select the fabric or switches from the **Available** list and click the right arrow button to move it to the **Selected** list. You can select multiple products.

NOTE
For IP products, only switches are available to select.

6. Click **OK**.

   The Management application registers the recipient IP address as a syslog recipient.

Removing a syslog recipient

To remove a syslog recipient, complete the following steps.

1. Select **Monitor > Syslog Configuration > Syslog Forwarding**.

   The **Syslog Recipients** dialog box displays.
2. Select **Remove** from the **Action** list.
3. Enter the IP address of the syslog port (the recipient server) in the **Recipient IP Address** field.
4. Select the fabric or switches from the **Available** list.
5. Click **OK**.

The Management application removes the recipient from the managed switches.

Syslog forwarding

The **Syslog Forwarding** dialog box enables the Management application to forward syslog events to a destination on another host. You can use the Syslog Forwarding feature to set up filters to determine which syslog events will be forwarded.

Adding a syslog forwarding destination

The **Add Syslog Destination** dialog box allows you to configure destinations for forwarding syslog events.

To add a syslog destination, complete the following steps.

1. Select **Monitor > Syslog Configuration > Syslog Forwarding**.

   The **Syslog Forwarding** dialog box, shown in Figure 479, displays.

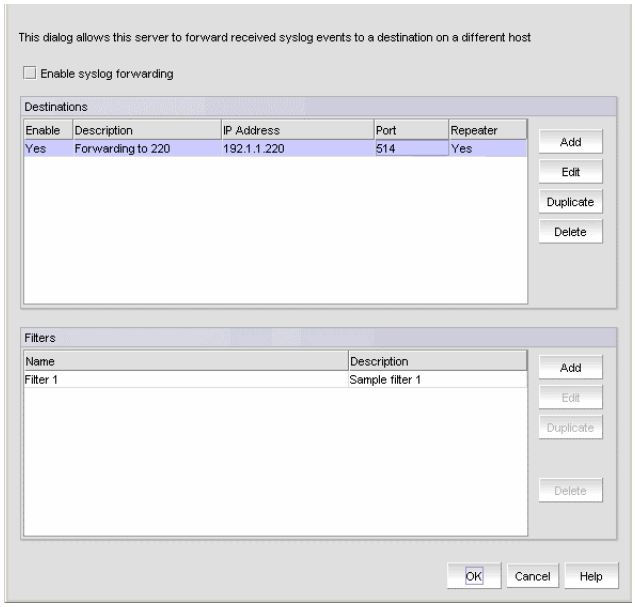


FIGURE 479 Syslog Forwarding dialog box

2. Select the **Enable syslog forwarding** check box.
3. Click **Add**.

   The **Add Syslog Destination** dialog box, shown in Figure 480, displays. The **Enable** and **Syslog Repeater** check boxes are selected by default.

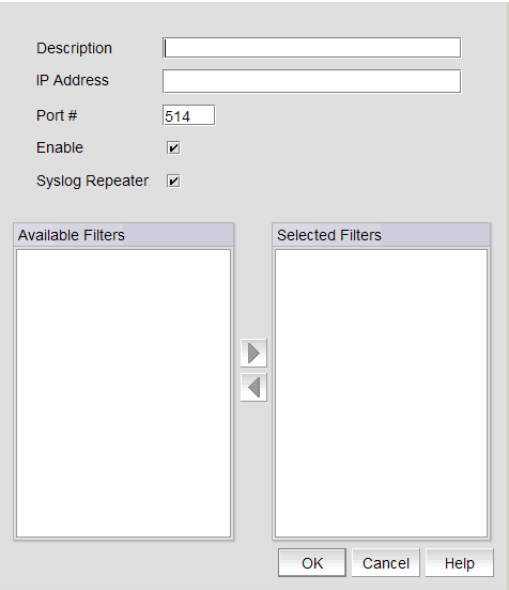


FIGURE 480 Add Syslog Destination dialog box

4. Enter a general description of the syslog destination in the **Description** field.
5. Enter the IP address of the syslog destination in the **IP Address** field. This is a mandatory field. IPv4 and IPv6 addresses are accepted, but a DNS name is not accepted.
6. Enter the syslog listening port of the recipient in the **Port #** field. This is a mandatory field. Valid numeric values range from 1 through 65535. The default is 514.
7. Select the **Enable** check box to enable syslog forwarding to this recipient.
8. Select the **Syslog Repeater** check box if you want to forward all syslogs, whether the source is managed or unmanaged. If the Syslog Repeater check box is unselected, syslogs from the managed products are sent to the server. If no filter is selected, then syslogs from all products are sent.
9. You can choose not to select a filter (zero) or you can select up to five filters from the **Available Filters** list. Click the right arrow button to move them to the **Selected Filters** list. This is enabled only when **Syslog Repeater** is not selected.
10. Click **OK**.

Adding a syslog filter

You can add a syslog filter on SAN products, IP products, or hosts.

To add a syslog filter, complete the following steps.

1. Select **Monitor > Syslog Configuration > Syslog Forwarding**.

   The **Syslog Forwarding** dialog box displays.
2. Select the **Enable syslog forwarding** check box.
3. Select **Add** in the **Filters** area.

   The **Add Syslog Filter** dialog box, shown in Figure 481, displays.

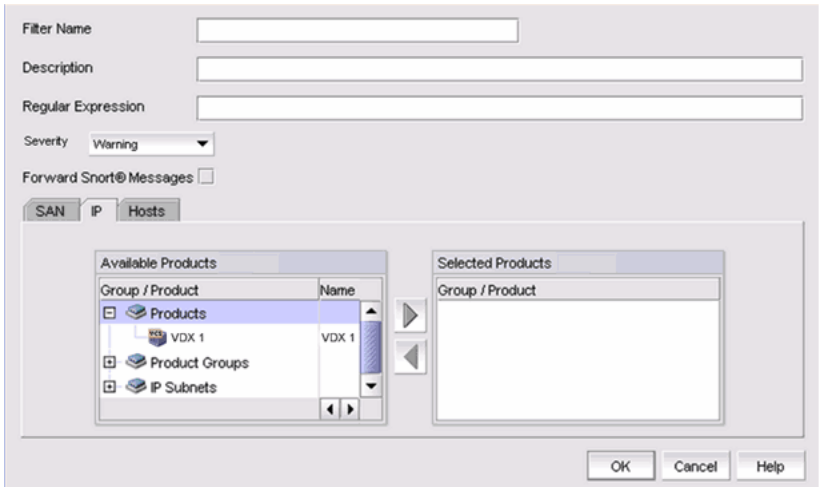


FIGURE 481 Add Syslog Filter dialog box

4. Enter a unique name for the syslog filter in the **Filter Name** field.
5. Enter a general description of the syslog filter in the **Description** field.
6. (Optional) For additional filtering, enter a text string using from 1 through 512 characters or wild card symbols in the **Regular Expression** field. The regular expression is used to describe a pattern in text. You can use an asterisk (*) to indicate a wildcard, as in the following examples:
   - *cdef: Matches a message ending with cdef
   - abc*: Matches a message beginning with abc
   - *abc*: Matches a message that contains abc
7. Select a severity level from the **Severity** pulldown menu. The severity level can be one of the following, and appear in descending order of severity.
   - Emergency
   - Alert
   - Critical
   - Error
   - Warning (Default)
   - Notice
   - Info
   - Debug

   Events with the selected severity and those with higher severity levels are forwarded.
   For example, by default, Critical severity is selected. Therefore, events with Critical, Alert, and Emergency severity levels are forwarded.
   To have all traps forwarded, select Debug, the lowest severity level.
8. Select the **Forward Snort® Messages** check box to turn on Snort message forwarding. Refer to "Snort message forwarding" on page 1166 for more information.
9. Select the **SAN**, **IP**, or **Hosts** tab. Depending on the tab selected, the products available to which you can add a syslog filter display in the **Available Products** list.

10. Select the product from the **Available Products** list and click the right arrow button to move it to the **Selected Products** list.
11. Click **OK**.

Snort message forwarding

Snort is a third-party tool that monitors network traffic in real time. When Snort detects dangerous payloads or other abnormal behavior, it sends an alert to the syslog in real time. You can turn Snort messages on or off using the **Add Syslog Filter** dialog box

By default, the Forward Snort© Messages feature is not enabled. You must enable it to have Snort messages forwarded to the configured syslog destinations.

You can forward Snort messages, by selecting the **Forward Snort® Messages** check box in the **Add Syslog Filter** dialog box (refer to step 8 in "Adding a syslog filter" on page 1164).

Event action definitions

To reduce the amount of events being logged in the Management application database, the **Event Actions** dialog box allows you to control what events the Management application monitors, on which products they are to be monitored, how often they are to be monitored, and what to do when the monitored events are generated. This information can be defined by creating an event action definition.

For example, you can create an event action definition if you want the Management application to monitor link up and link down traps only, and only on products that belong to Product Group 1. Furthermore, you may want these traps to be logged in the Management application database only if they occur 10 times within a 5-minute interval. You may also want an e-mail message sent to a network administrator when these traps are generated.

In another case, you may not want to log any occurrence of Topology Change traps from Product Group 2. You may also want to disable a port on a product if an event that resembles an attack on the network occurs at a certain frequency.

Creating an event action definition

You can configure event policies for events you want to monitor. Use the Event Actions dialog box, shown in Figure 482, to customize the event management policy using triggers and actions.

To customize the event management policy, complete the following steps.

1. Select **Monitor > Event Processing > Event Actions**.

   The **Event Actions** dialog box, shown in Figure 482, displays.

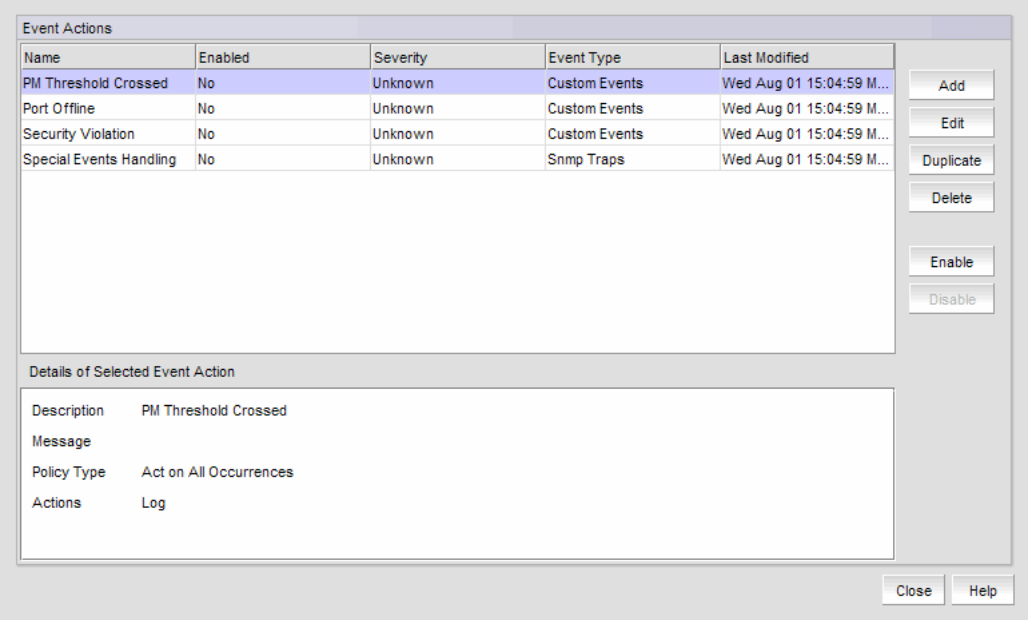


FIGURE 482 Event Actions dialog box

2. Click **Add** to display the **Identification** pane of the Add Event Action dialog box.
3. Enter a name and description for the event action and select the **Enabled** check box.
4. Click **Next** to advance to the **Events** pane.

Selecting an event for an event action

To select an event for an event action, complete the following steps.

1. Select **Monitor > Event Processing > Event Actions**.

   The **Event Actions** dialog box displays.

2. Click **Next** to advance to the **Events** pane.

   By default, the **Events** pane of the **Add Event Action** dialog box displays, shown in Figure 483.

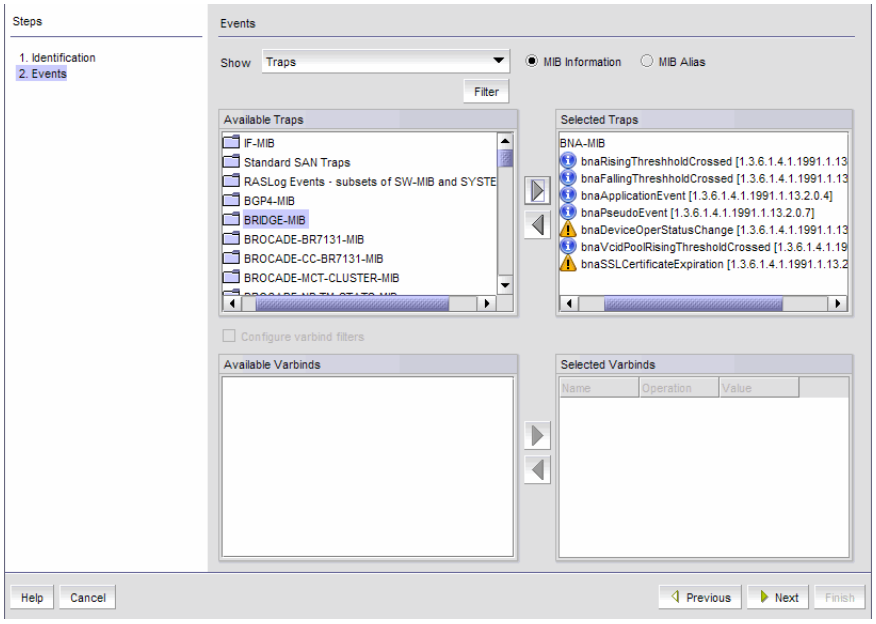


FIGURE 483 Add Event Action dialog box - Events pane

3. Select one of the following event types from the **Show** list:

   - Traps (default)
   - Application Events
   - Pseudo Events
   - Custom Events
   - Snort® Message

   Depending on what event type you select, a box listing the available events or pseudo events displays.

4. By default, all traps are listed in the **Available Traps** list, under the folders for the MIB to which they belong. You can limit the list by doing any of the following:

   - Click one of the following buttons:
     - **MIB Information**, if you want the default SNMP name for the traps to be displayed.
     - **MIB Alias**, if you want the aliases for the traps to be displayed.
   - Use the Trap Filter tool to limit the trap list to the trap severities you want. To use this tool, click the **Filter** button to display the **Trap Filters** dialog box.

5. Click the **Filter** button to launch the **Trap Filters** dialog box, which allows you to find the trap you want.

6. After limiting the list of available traps, expand the MIB folder to which the trap you want belongs under the **Available Traps** list and select that trap. Click the right arrow button to move it to the **Selected Traps** list.

7. If you selected **Application Events** in step 3, select the application events in the left table and use the arrow button to move them to the right.

8. If you selected **Pseudo Events** in step 3, select one or more of the pseudo events you created that you want to include in the definition, then click the right arrow button to move it to the **Selected Pseudo Events** list.
9. If you selected **Custom Events** in step 3, click **Next** to accept the defaults; otherwise, select the Event Category, Severity, Message ID, and Description Contains, as required.
10. If you selected **Snort® Message** in step 3, select the Snort® messages in the left table and use the arrow button to move them to the right.

    To import Snort® rules, click the **Import Snort® Rules** button.
11. Select **Configure varbind filters** to configure filters on varbind values (refer to "Configuring varbind filters" on page 1169 for more information). If you do not want to configure varbind filters, click **Next**.

    The **Sources** pane of the **Add Event Action** dialog box is displayed. You can use the Search tool to search for sources.

Configuring varbind filters

If actions must be confirmed based on a trap variable binding value (varbinds), select the **Configure varbind filters** check box on the **Events** pane of the **Add Event Action** dialog box. This enables you to configure filters on varbind values for this event action.

NOTE
Varbind filter configuration is only available if you selected Traps in step 3 of "Creating an event action definition" on page 1166.

The varbinds for the selected trap are listed in the **Available Varbinds** list, shown in Figure 484.

To configure varbind filters for an event action, complete the following steps.

1. Select **Monitor > Event Processing > Event Actions**.

   The **Event Actions** dialog box displays.
2. Click **Next** to advance to the **Events** pane.

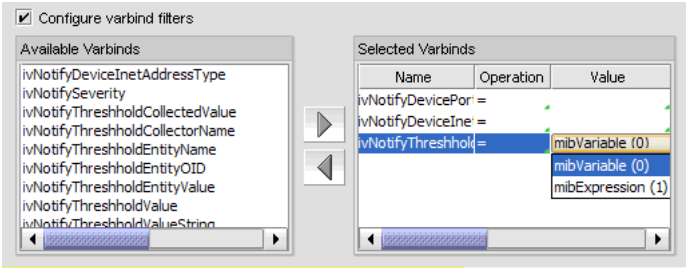


FIGURE 484 **Available Varbinds and Selected Varbinds lists**

3. Select the varbind you want to include in the configuration and click the right arrow button to move it to the **Selected Varbinds** list.

   If you selected more than one trap and those traps have the same varbinds, then their varbinds are listed in the **Available Varbinds** list. However, if the traps you selected have different varbinds, the **Available Varbinds** list is empty.

4. For each varbind in the **Selected Varbinds** list, select one of the following operations for the condition you want to filter:
   - = – Equal to
   - != – Not equal
   - < – Less than
   - > – Greater than
   - >= – Greater than or equal to
   - <= – Less than or equal to
   - In – Matches collection
   - Not_in – Does not match collection
   - ~ – Arbitrary Unicode regular expression
5. Enter the value of the varbind. The value you enter must conform to the data type required by the varbind. For example, if the varbind expects an integer and you enter a text string, your entry will be rejected. Alternatively, you can select values from drop-down lists, shown in Figure 484.
6. Click **Next**.

   The **Sources** pane of the **Add Event Action** dialog box displays. Proceed to "Selecting source address products and ports".

Selecting source address products and ports

The **Sources** pane of the **Add Event Action** dialog box, shown in Figure 485, allows you to enter the IP address, the world wide name, or the name of the source to use as event senders. Alternatively, you can select source address products to use as event senders from the available list of sources. You can select from the available list of SAN products, IP products, or hosts by selecting the appropriate tab.

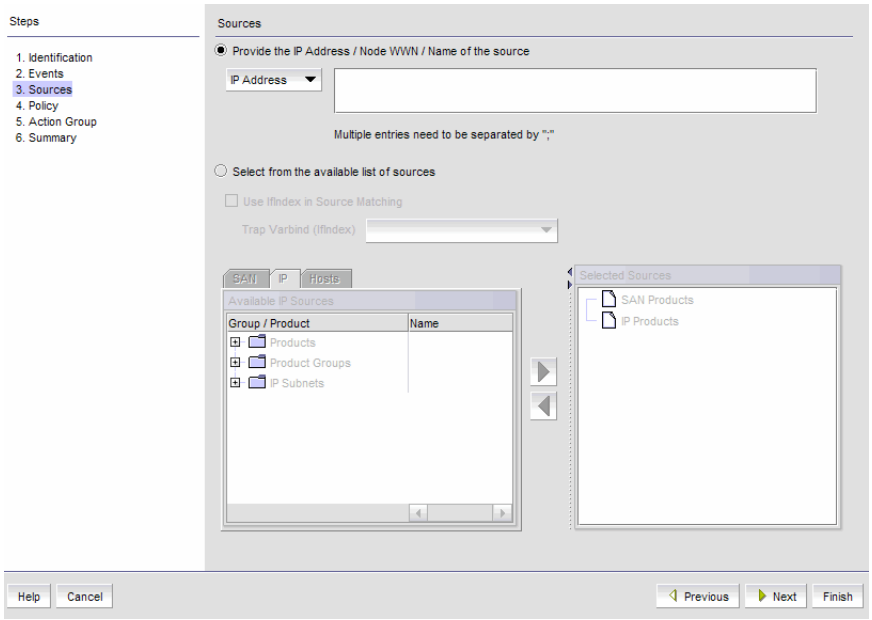


FIGURE 485 Sources pane of the Add Event Action dialog box

To configure the identity of the event action source, complete the following steps.

1. Select **Monitor > Event Processing > Event Actions**.

   The **Event Actions** dialog box displays.

2. Click **Next** to advance to the **Sources** pane.

3. Click the **Provide the IP Address / Node WWN / Name of the source** button if you want to manually enter the IP address, the world wide name (WWN), or the name of the source in the **IP Address** field.

4. Click the **Select from the available list of sources** button as an alternative to manually entering the IP address, WWN, or name of the source. You can select source address products or ports to use as event senders from the available list of sources.

5. Select the **Use If index in source matching** check box if you want to use if Index to filter traps on a specific port of a product; otherwise, the filter is applied globally on a product.

6. If the **Use IfIndex in source matching** check box is selected, select the varbind to be used from the **Trap Varbind (IfIndex)** list.

7. Select the event senders you want from the **Available Sources** list, then click the right arrow button to move them in the **Selected Sources** list.

   - If you selected a non-IronWare OSNetwork OSproduct as the source, that product can send e-mail alerts only.
   - If you selected Pseudo Events from the **Events** pane of the **Add Event Action** dialog box, and there is only one pseudo event available, double-click the pseudo event in the **Available Sources** list.
   - If you selected a product group or port group as event senders, select a group from the list.

   NOTE
   The selected source count cannot exceed 100.

8. Click **Next**.

   The **Policy** pane of the **Add Event Action** dialog box displays. Proceed to "Configuring event action policies".

Configuring event action policies

The **Policy** pane of the **Add Event Action** dialog box, shown in Figure 486, allows you to define the frequency of the event, enter a message for an event that will be displayed in the event log, and specify the event severity.

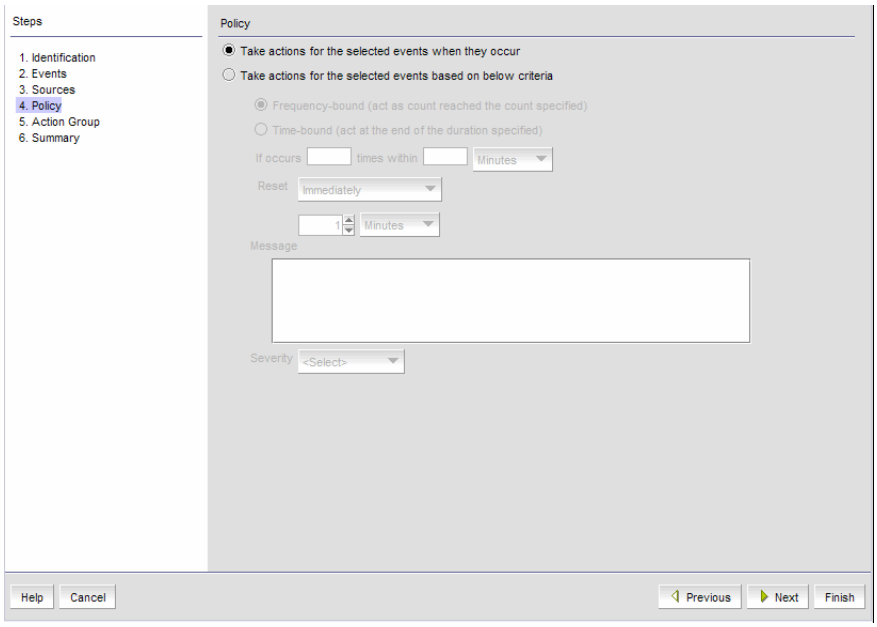


FIGURE 486 Policy pane of the Add Event Action dialog box

To configure the event action policies, complete the following steps.

1. Click **Take actions for the selected events when they occur** (default) if you want the action to be triggered each time the selected events occur.
2. Click **Take actions for the selected events based on below criteria** if you want the action to be triggered only when the occurrence of the event meets the specified criteria.
   - Click **Frequency bound (act as count reaches the count specified)** if you want the Management application to perform the specified action once the specified number of occurrences has occurred *during* the specified duration. For example, if you want the action to be applied when 10 link down traps occur during a one-minute interval, then the specified action will be applied as soon as 10 link down traps occur, even though the one-minute duration has not elapsed.
   - Click **Time bound (act at the end of the duration specified)** if you want the Management application to perform the specified action once the specified number of occurrences has occurred *and* the specified duration has elapsed. For example, if you want the action to be applied when 10 link down traps occur during a one-minute duration, the Management application waits until 10 link down traps occur and one minute has elapsed before the defined action is applied. There is a one-second delay for the action to be applied.

   For either option, if the number of occurrences has not been met and the time duration has elapsed, the observation window is advanced to the next occurrence after the first occurrence on the current window.
3. Enter values in the **If occurs __ times within __** fields and select a value from the **Minutes** list if you want the action to be applied only if the event occurs at a certain frequency.

4. Indicate how often the policy is to be reset. You can choose one of the following options:
   - **Reset immediately** - Repeats the policy as soon as the specified action has been applied.
   - **Wait until ____ seconds or minutes** - If this parameter is selected, the policy will not be applied to the product for the specified duration of time. Enter the duration in minutes or hours. You can suppress the policy just for the events specified in the policy or for any event that occurs on the product. Once the duration expires, the policy can be repeated.
5. In the **Message** field, enter the message that will be displayed in the Event Log for the generated event. This entry replaces the default message that is displayed for a trap. Also, this message is used as the Event Action message and is displayed in single quotes on the Event Log report.
6. From the **Severity** list, select the severity you want to assign to the generated event.
7. Click **Next.**
8. The **Actions Group - Actions** pane of the **Add Event Action** dialog box displays. Proceed to "Editing event actions".

Editing event actions

The **Action Group - Actions** pane of the **Edit Event Action** dialog box, shown in Figure 487, defines what action the Management application takes when the criteria are met.

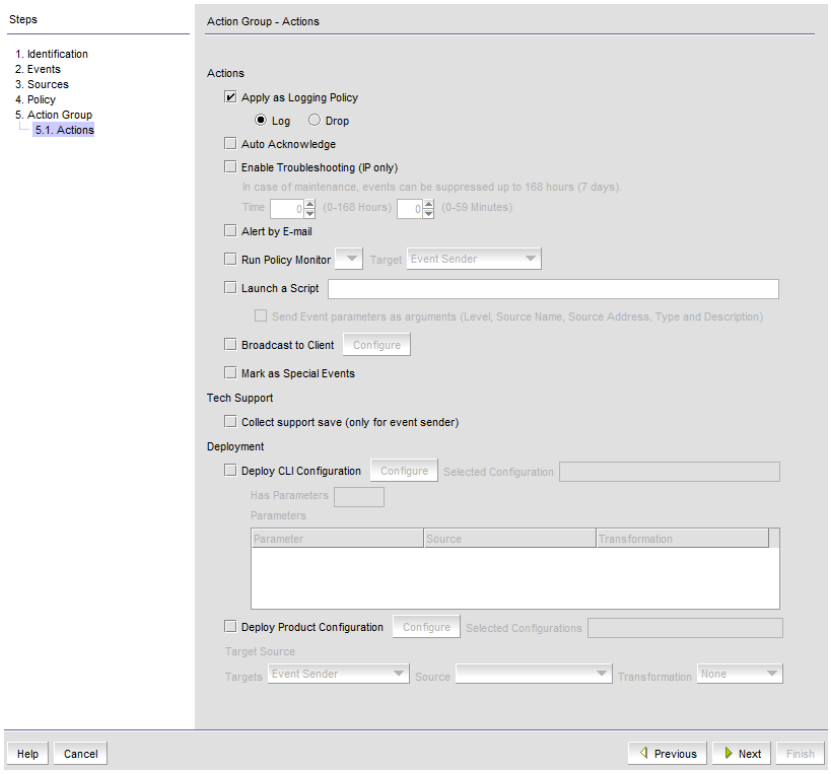


FIGURE 487 Action Group - Actions pane of the Edit Event Action dialog box

To configure the policies for the event action, complete the following steps.

1. Select **Apply as a Logging Policy** to indicate whether or not you want the event occurrence to be logged in the Management application database:
   - Select **Log** to log the occurrence in the Management application database and Master Log.
   - Select **Drop** to not log the occurrence in the Management application database or Master Log.

   NOTE
   If the policy specifies **Act as specified** on the **Policy** pane of the **Add Event Action** dialog box, and you select **Log** for this parameter, only events that meet the criteria defined in the **Act as specified** area are logged. For example, if the event is logged when 10 link down traps occur during a one-minute interval, then one record will be logged after 10 link down traps occur. If you want all 10 link down traps to be logged, then create a policy where **Act on all occurrences** is selected on the **Policy** pane of the **Add Event Action** dialog box.

2. Select the **Auto Acknowledge** check box to suppress events without being in troubleshooting mode. Activating this also helps to avoid cluttering Master Log with unwanted messages without modifying filters.

   NOTE
   Auto Acknowledge is enabled only when **Take actions for the selected events when they occur** is selected in the Policy step of the Event Actions Wizard. If you edit an Event Action that has Auto Acknowledge selected and change this option in the Policy step to **Time-bound** or **Frequency-bound**, you will be required to confirm your choice.

3. Select the **Enable Troubleshooting** check box to suppress events based on user-entered criteria. You can suppress events for up to 168 hours (7 days). This action is applicable to IP devices only.
4. Select the **Alert by E-mail** check box if you want an e-mail message to be sent to an administrator if the policy criteria have been met.
5. Select the **Run Policy Monitor** check box to execute a policy monitor as an action based on a selected event, and then select the target for the policy monitor from the list. Target options include **Event Sender** and **Specified in Config**.
6. Select the **Launch a Script** check box if you want to execute to an external script file when the matching criteria have been met, and then enter the script in the accompanying field.
7. Select the **Broadcast to Client** check box, and click **Configure** to broadcast a message to all the clients when the matching criteria have been met.

   NOTE
   The remaining parameters are not available if a non-IronWare OSNetwork OS product is selected as an event sender.

   The **Broadcast Message** dialog box displays.

   a. Select a severity level from the list.
   b. Type a message in the **Message Content** field.
   c. Click **OK**.

8. The **Mark as Special Events** check box is unselected by default. Leave it this way if you want the event action to be added to the Special Event Handling event action category. Refer to "Special events handling" for more complete information.
9. Click the **Collect support save** check box to enable SupportSave on the event. The check box is unselected by default.
10. Select the **Deploy CLI Configuration** check box and click **Configure** if you want to deploy a configuration from CLI Configuration Manager to products if the policy criteria have been met. You can only deploy a CLI configuration for IP products.

NOTE
If the CLI configuration you chose from CLI Configuration Manager contains a non-IronWare OS or Network OS product as a target, the configuration will not be deployed to the non-IronWare OS or Network OS product.

11. You can either select an existing CLI configuration or create a new one and select that configuration. After selecting a CLI configuration, the name of the CLI configuration is displayed in the **Selected Configuration** field.
    - **Has Parameters** - Displays **Yes** if the CLI configuration has parameters that require values to be entered before it can be deployed, and displays **No** if no parameter needs to be defined.
    - The **Parameters** list lists the parameters that need to be defined in the configuration.
        - The **Parameter** column displays the parameter and its variables in the CLI configuration.
        - The **Source** column lists the appropriate SNMP attributes for the parameters. Each attribute contains a specific parameter value, such as an IP address. Select the attribute you want from the list.
        - The **Transformation** column uses the product IP addresses and MAC addresses listed in the Address Finder. If the Address Finder list is empty, the product or port will not be found. From this column, specify what you want Event Processor to do with the value in the attribute:
            - **Find Device**: Find the product with the IP address in the attribute and deploy the CLI configuration to that product.
            - **Find Port**: Find the port on a product with the IP address in the attribute and deploy the CLI configuration to that port.
            - **Find Intruder MAC**: Find the product with the IP address in the attribute that matches the intruder MAC address and deploy the CLI configuration to that product.
            - **None**: Event Processor only reports occurrence of the products.
12. Select the **Deploy Product Configuration** check box if you want to deploy a payload from the Configuration Wizard to the products if the policy criteria have been met.

NOTE
If the configuration payload you choose from the Configuration Wizard contains a non-IronWare OS or Network OS product as a target, the payload will not be deployed to the non-IronWare OS or Network OS product.

13. From the **Target** list, select the product (the target source) to which the payload will be deployed:

- **Event Sender**: Deploy the payload to the product that sent the event. If the event was sent by a non-IronWare OS or Network OS product, the event action will not be deployed to that product.
- **Derived from**: Deploy the payload to the product that matches the IP address as specified in the attribute of the selected source. If the matching product is a non-IronWare OS or Network OS product, the event action will not be deployed to that product.
- **Specified in the Config**: Deploy the payload to the product that is specified in the payload. If the configuration you choose contains a non-IronWare OS or Network OS product as a target, the configuration will not be deployed to the non-IronWare OS or Network OS product.

14. If you selected **Derived from** as the target in step 13, select the attribute from the **Source** list.
15. From the **Transformation** column, specify what you want Event Processor to do with the value in the attribute:
    - **None —** Event Processor only reports the occurrence of the product.
    - **Find Device —** Find the product with the IP address in the attribute and deploy the payload to that product.
    - **Find Intruder MAC** — Find the product with the IP address in the attribute that matches the intruder MAC address and deploy the CLI configuration to that product.
    - **Find Port** — Find the port on a product with the IP address in the attribute and deploy the CLI configuration to that port.

    The **Transformation** column uses the product IP addresses and MAC addresses listed in the Address Finder. If the Address Finder list is empty, the product or port will not be found.
16. Click **Next** to display the **Action Group - E-mail Settings** pane of the **Add Event Action** dialog box if you selected **Alert by E-mail**. If you did not select **Alert by E-mail**, you will advance to the **Summary** pane.

Special events handling

The following special error conditions are examples of events that are categorized as Special Events Handling events, a separate category that appears in the **Name** list of the **Event Actions** dialog box. All pre-selected events are SNMP traps.

- Invalid T1 zone configuration event
- 48-blade inserted into a non-Virtual Fabric chassis
- Port fencing Fabric Watch trap, when a port is fenced
- Blade Processor FPGA version is incompatible with the Fabric OS firmware version

Though these error conditions are automatically considered “special events handling” events, you can add or edit any event action and mark the action as a special event for special events handling using the **Actions** pane of the **Edit Event Action** dialog box.

See step 8 of “Editing event actions” on page 1173 for information on enabling special events handling for an event using the **Actions** pane of the **Edit Event Action** dialog box.

Acknowledging special events

When the Management application receives and processes events selected as special events, the following status bar icon displays:

FIGURE 488 Status bar with highlighted special events icon

To configure special event acknowledgements, complete the following steps.

1. Click the special events icon to launch the **Special Events** dialog box, shown in Figure 489.

   The Special Events dialog box, shown in Figure 489, lists the most recent 1000 events that have been identified as special events.

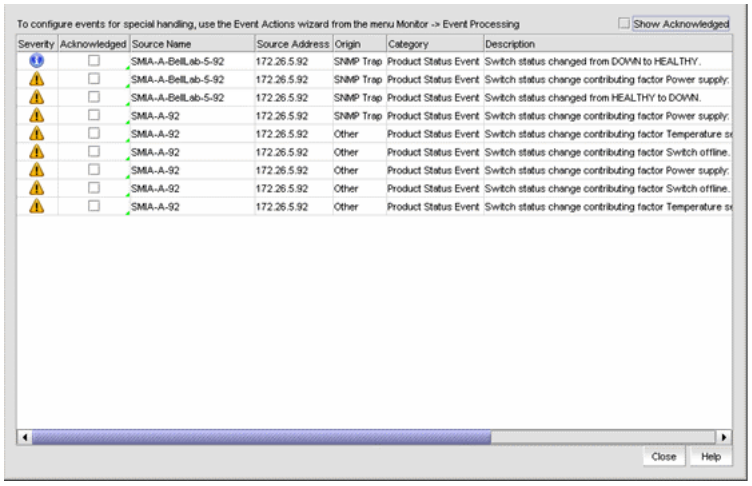


FIGURE 489 Special Events dialog box

2. Select the **Acknowledged** check box that corresponds to the special event you want to acknowledge.

   If an event is marked as acknowledged either in the **Special Events** dialog box or the Master Log, the event is acknowledged in both places.

3. To view all acknowledged special events, select the **Show Acknowledged** check box in the upper right corner of the dialog box. This check box is unselected by default.

   The acknowledged special events display, sorted by the last event server time.

Configuring event action e-mail settings

The **Action Group - E-Mail Settings** pane of the **Add Event Action** dialog box, shown in Figure 490, allows you to select e-mail recipients from a list, add new e-mail recipients, and compose e-mail messages.

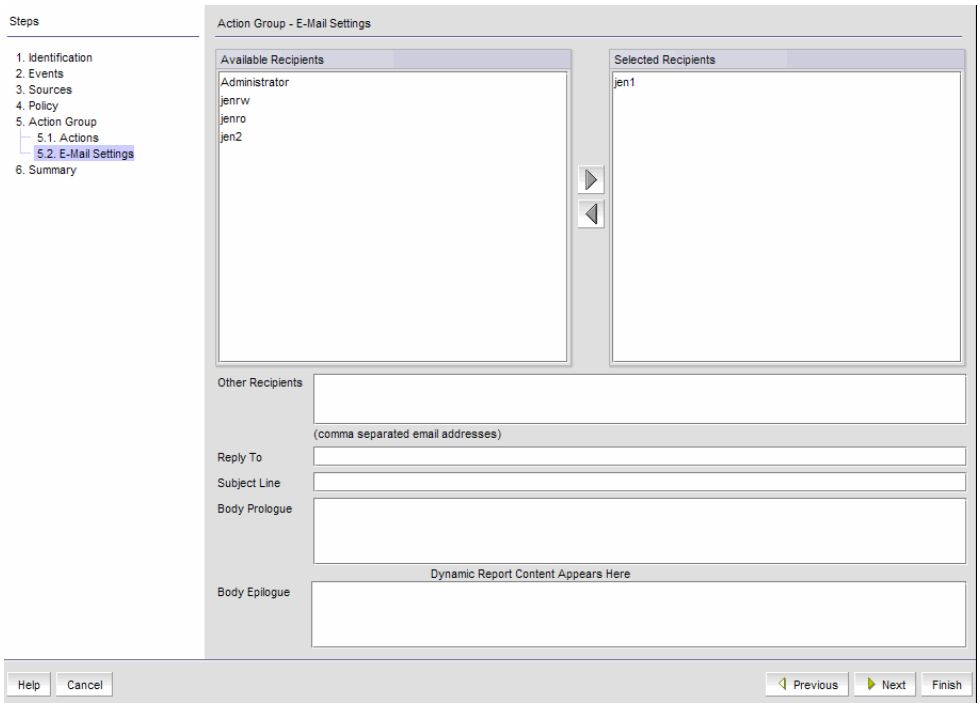


FIGURE 490 Action Group - E-Mail Settings pane of the Add Event Action dialog box

To configure the e-mail settings for the event action, complete the following steps.

1. Select the Management application user to whom the e-mail message will be sent from the **Available Recipients** list, and click the right arrow button to move the recipient to the **Selected Recipients** list.

   NOTE
   Make sure the user you select has an e-mail address defined in a user account.

2. (Optional) Add additional e-mail recipient addresses in the **Other Recipients** field. Separate multiple e-mail addresses with a semicolon. At least one e-mail address must be specified by either selecting an available recipient from the list (step 1) or entering an e-mail recipient.

3. If you want the e-mail message for the alert to display a description on the subject line, enter the text in the **Subject Line** field.

   NOTE
   You can create a prefix that is included in the subject line of every e-mail alert that the Management application sends. The prefix is defined in the configuration.properties file. The prefix plus the text entered in this field cannot exceed 255 characters.

4. If you want a prologue to be inserted at the beginning of the e-mail message, enter up to 255 characters in the **Body Prologue** field. The event action message follows the prologue.

5. If you want an epilogue to be placed at the end of the e-mail message, enter up to 255 characters in the **Body Epilogue** field.

NOTE
The prologue, the event action message, and the epilogue form the body of the e-mail alert.

6. Click **Finish**.

   The **Summary** pane of the **Edit Event Action** dialog box displays an overview of the e-mail configuration you are creating.

7. Review your entries and take one of the following actions:
   - Click **Finish** to approve the configuration.
   - Click **Previous** to return to the **Action Group - E-Mail Settings** pane of the **Add Event Action** dialog box.
   - Click **Cancel** to cancel the operation.

Creating a new event action definition by copying an existing definition

You can create a new event action definition by copying one that is in the **Event Actions** list.

To create a new event action definition by copying an existing definition, complete the following steps.

1. Select **Monitor > Event Processing > Event Actions**.

   The **Event Actions** dialog box displays.

2. Select the definition that you want to copy from the **Event Actions** list.
3. Click the **Duplicate** button to display the **Duplicate Event Actions** dialog box.

   The name of the event action is the name of the selected action with the word “copy” appended. For example, Action1 becomes Action1 copy.

4. Enter a new name for the definition.
5. Change the description of the definition, if needed. You can perform this action in any of the panes of the **Add Event Action** dialog box.
6. Click **Finish** to save the new definition.

Modifying an event action definition

CAUTION
Use caution when you modify an event action. Saving changes to an event action definition resets the runtime information for the events in the definition.

To modify an existing event action definition, complete the following steps.

1. Select **Monitor > Event Processing > Event Actions**.

   The **Event Actions** dialog box displays.

2. Select the definition that you want to edit from the **Event Actions** list.

3. Click **Edit** to display the **Edit Event Action** dialog box.
4. Make the changes you want to make to the definition. You can perform this action in any of the panes of the **Add Event Action** dialog box.
5. Click **Finish** to save your definition.

Deleting an event action definition

To delete an event action definition, complete the following steps.

1. Select **Monitor > Event Processing > Event Actions**.

   The **Event Actions** dialog box displays.
2. Select the definition that you want to delete from the **Event Actions** list.
3. Click **Delete**.

   A message displays asking you to confirm the deletion request.
4. Click **Yes** to delete the definition, or **No** to cancel the request.

Configuring event actions for Snort messages

To configure an event action for Snort messages, complete the following steps.

1. From the **Identification** pane of the **Add Event Action** dialog box, click **Next** to advance to the **Events** pane. See "Creating an event action definition" on page 1166 for complete instructions on event actions.

   The **Events** pane of the **Add Event Action** dialog box displays, shown in Figure 491. Snort® Message is the default in the **Show** list.

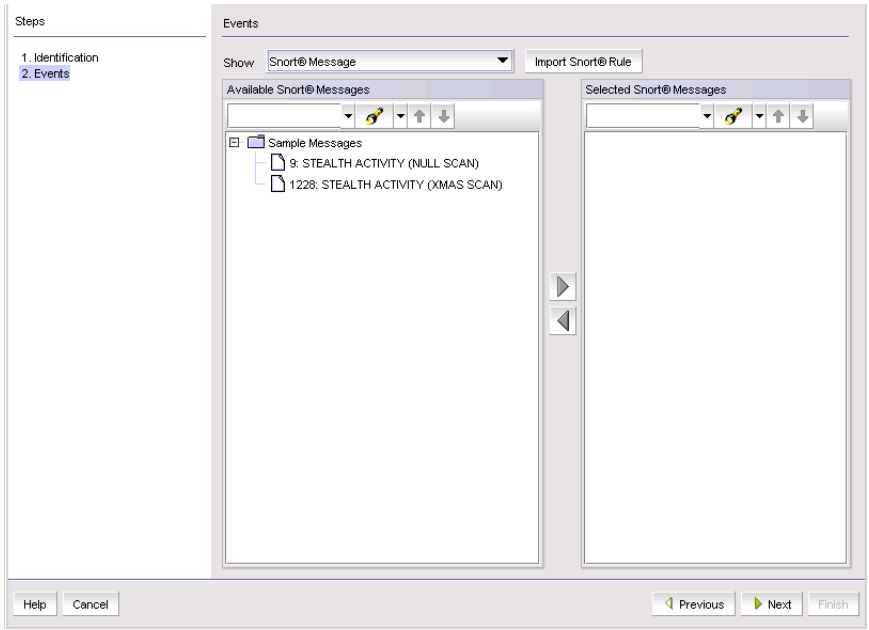


FIGURE 491 Events pane of the Add Event Action dialog box

2. Click the **Import Snort® Rule** button.

   The **Import Snort® Rule File** dialog box displays, shown in Figure 492.

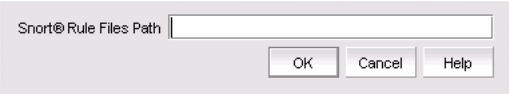


FIGURE 492 Import Snort® Rule File dialog box

3. Enter the complete path of the Snort rule file located on the Syslog server.
4. Click **OK** to import the Snort rules.
5. While still in the **Add Event Action** dialog box, continue to click **Next** until you advance to the **Action Group - Actions** pane.
6. Select the **Deploy CLI Configuration** check box and click **Configure** if you want to deploy a configuration from CLI Configuration Manager to products if the policy criteria have been met. You can only deploy a CLI configuration for IP products.

   NOTE
   If the CLI configuration you chose from CLI Configuration Manager contains a non-IronWare OSNetwork OS product as a target, the configuration will not be deployed to the non-IronWare OSNetwork OS product.

7. Select one of the following existing CLI configuration parameter sources from the **Parameter** list:
   - **Source IP** — The source IP address of the attack.
   - **Source Port** — The source port of the attack.
   - **Destination IP** — The destination IP address of the attack.
   - **Destination Port** — The destination port of the attack.
8. Continue to advance through the **Add Event Action** dialog box. The **Summary** pane of the **Edit Event Action** dialog box displays an overview of the e-mail configuration you are creating.
9. Review your entries and take one of the following actions:
   - Click **Finish** to approve the configuration.
   - Click **Previous** to return to the **Action Group - E-Mail Settings** pane of the dialog box.
   - Click **Cancel** to cancel the operation.

Pseudo events

A pseudo event is a combination of different SNMP traps that you decide would constitute a single event. For example, there are two separate SNMP traps for link up and link down occurrences. You might decide that these two occurrences should be just one event.

Displaying pseudo event definitions

To display the properties of a pseudo event definition, complete the following steps.

1. Select **Monitor > Event Processing > Pseudo Events**.

   The **Pseudo Events** dialog box, shown in Figure 493, displays.

FIGURE 493 Pseudo Events dialog box

2. To view additional information for a definition, select a definition from the list. Additional information displays in the **Details of Selected Pseudo Event** list at the bottom of the dialog box.

Creating pseudo event definitions

To create a pseudo event definition, complete the following steps.

1. Select **Monitor > Event Processing > Pseudo Events**.

   The **Pseudo Events** dialog box, shown in Figure 493, displays.

2. Click **Add**.
3. The **Identification** pane of the **Add Pseudo Event** dialog box displays.
4. Type a unique name for the pseudo event. Duplicate names are not allowed.
5. Select the **Enabled** check box to enable the pseudo event or clear the check box to disable the pseudo event.
6. Click **Next**.

   The **Policy** pane of the **Add Pseudo Event** dialog box, shown in Figure 494, displays.

Setting pseudo event policies

The **Policy** pane of the **Add Pseudo Event** dialog box, shown in Figure 494, allows you to create escalation, resolve, and flapping policies for the pseudo event, and then specify the time duration for each of these policies in minutes or seconds.

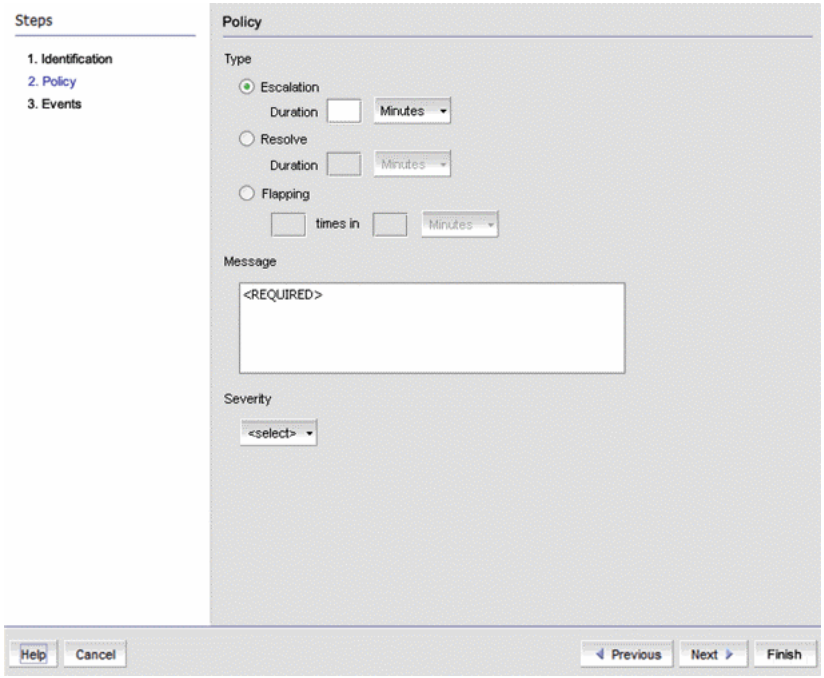


FIGURE 494 Policy pane of the Add Pseudo Event dialog box

To create policies for a pseudo event definition, complete the following steps.

1. Click the **Escalation** button to create an escalation policy, and then enter the duration of time that the Management application waits before performing the specified action. Specify the escalation time in minutes or seconds.

   When an event occurs, an escalation policy waits for a duration of time to see if the event remains in that state. If it does, then the specified action in the definition is performed.

   Refer to "Adding a pseudo event on the escalation policy" on page 1187 for complete instructions.

2. Click the **Resolve** button to create a resolve policy, and then enter the duration of time the Event Processor waits before generating the pseudo event. Specify the resolve time in minutes or seconds.

   When a down event occurs, a resolving policy waits for a specified duration to see if the event remains in that state by checking if an up event occurs. If an up event occurs, a resolving pseudo event is generated by the Event Processor.

   Refer to "Creating an event action with a pseudo event on the resolving policy" on page 1190 for complete instructions.

3. Click the **Flapping** button to create a flapping policy, and then enter the number of occurrences and the duration of time before the Management application performs the action specified in an event action. Specify the number of flapping times in minutes or seconds.

The flapping policy checks to see if the event consistently transitions between two opposite states during a specified length of time. If it does, then the specified action in the definition is performed.

Refer to "Creating an event action with a pseudo event on the flapping policy" on page 1191 for complete instructions.

4. Enter a description in the **Message** field. This description is displayed in the event log for this pseudo event. The event log displays the exact text you enter in this field; therefore, this message should describe the events in the event action policy.
5. Select a severity from **Severity** list. You must assign a severity to the pseudo event.
6. Click **Next**.

   The **Events** pane of the **Add Pseudo Event** dialog box, shown in Figure 495, displays.

Refer to the following topics for specific procedures using this dialog box.

- "Creating pseudo event definitions" on page 1182
- "Editing a pseudo event definition" on page 1186

Filtering pseudo event traps

The **Events** pane contains a **Selected Down Trap** list and a **Selected Up Trap** list. The **Selected Down Trap** list defines the traps for the down state of a product or an interface. The **Selected Up Trap** list defines the traps for the up state of the product or an interface.

NOTE
By default in a SAN+IP configuration, all traps known to the Management application are included in the **Available Traps** list, under the folders for the MIB to which they belong.

To filter pseudo event traps, complete the following steps.

1. Select **Monitor > Event Processing > Pseudo Events**.

   The **Pseudo Events** dialog box, shown in Figure 493, displays.
2. Click **Add**.

   The **Events** pane of the **Add Pseudo Event** dialog box, shown in Figure 495, displays.

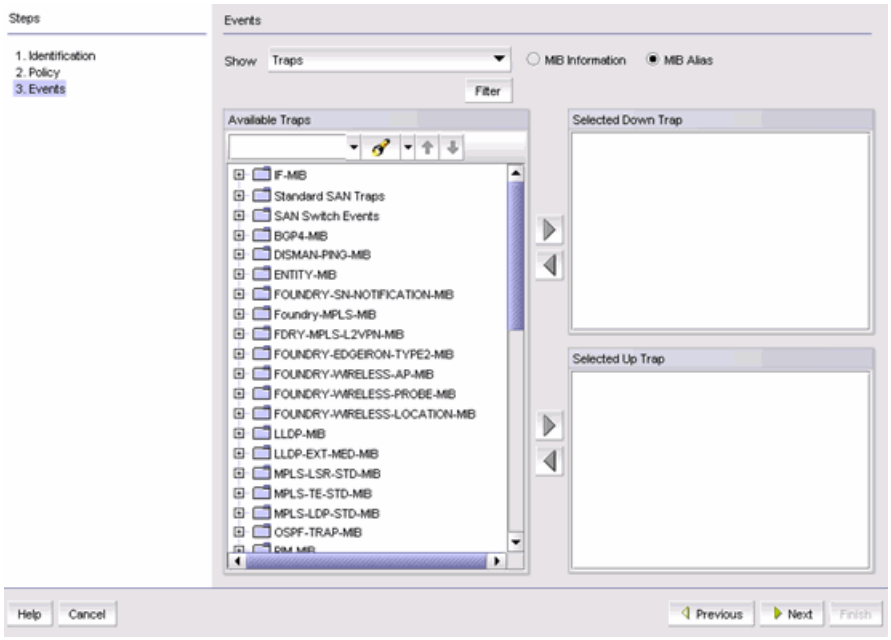


FIGURE 495 Events pane of the Add Pseudo Event dialog box

3. From the **Available Traps** list, select the trap for the down state of a product or interface.

   By default, all traps known to the Management application are included in the **Available Traps** list, which is a list of all traps that are available based on the MIB and filter criteria.

4. Select a trap for the **Selected Down Trap** list and a trap for the **Selected Up Trap** list.

   You cannot select the same trap for up and down conditions. Move the traps from the **Available Traps** list to the **Selected Down Trap** and **Selected Up Trap** lists using the right arrow button.

5. You can change the text associated with the selected trap by doing either of the following:

   - Click one of the following buttons:
     - **MIB Information**, if you want the default SNMP name for the traps to be displayed.
     - **MIB Alias**, if you want the aliases for the traps to be displayed.
   - Use the Trap Filter tool to limit the trap severity. To use this tool, click the **Filter** button to display the **Trap Filters** dialog box.

6. After limiting the list of available traps, expand the MIB folder to which the trap you want belongs under the **Available Traps** list, or right-click to select that trap. Click the right arrow button to move it to the **Selected Traps** list.

7. Select a trap for the up state of the condition.

   NOTE
   You must select a down and an up trap. You cannot select the same trap for the up and down conditions.

8. Click **Next** to advance to the **Summary** pane.

9. Click **Finish** to save your definition. The new pseudo event appears on the **Pseudo Event** list on the **Pseudo Event** dialog box.

Creating a pseudo event definition by copying an existing definition

You can create a pseudo event definition by copying an existing definition.

To create a pseudo event definition by copying an existing definition, complete the following steps.

1. Select **Monitor > Event Processing > Pseudo Events**.
2. Select the pseudo event definition that you want to copy from the **Pseudo Events** list.
3. Click the **Duplicate** button.

   The **Pseudo Events** dialog box, shown in Figure 493, displays.

   The name of the event action is the name of the selected action with the word “copy” appended. For example, “Event1” becomes “Event1 copy”.
4. Enter a new name for the pseudo event definition.
5. Make the changes you want to make to the definition. Refer to “Creating pseudo event definitions” on page 1182 for details.
6. Click **Finish** to save your definition.

Editing a pseudo event definition

Use caution when you modify pseudo event definitions. Saving changes to a pseudo event definition resets the run-time information for that pseudo event.

To edit a pseudo event definition, complete the following steps.

1. Select **Monitor > Event Processing > Pseudo Events**.

   The **Pseudo Events** dialog box, shown in Figure 493, displays.
2. Select the pseudo event definition that you want to edit from the **Pseudo Events** list.
3. Click the **Edit** button to display the **Edit Pseudo Event** dialog box.
4. Make the changes you want to make to the definition. Refer to “Creating pseudo event definitions” on page 1182 for details.
5. Click **Finish** to save your definition.

Deleting a pseudo event definition

Use caution when you delete pseudo event definitions. Deleting a pseudo event definition discards the run-time information for that pseudo event.

To delete a pseudo event definition, complete the following steps.

1. Select **Monitor > Event Processing > Pseudo Events**.

   The **Pseudo Events** dialog box, shown in Figure 493, displays.
2. Select the pseudo event definition that you want to delete from the **Pseudo Events** list.
3. Click **Delete**.

   A message displays, prompting you to confirm the deletion request.

4. Click **Yes** to delete the selected definition.

   The definition is removed from the **Pseudo Events** list.

Adding a pseudo event on the escalation policy

Use the escalation policy to be notified if a critical event occurs on a product, port, or system. When the event occurs, the escalation policy waits for a duration of time to see if the event remains in that state. If it does, then the specified action in the definition is performed.

The following two-part procedure uses both the **Identification** pane of the **Add Pseudo Events** dialog box and the **Add Event Actions** dialog box to create an event action with the escalation policy.

To add a pseudo event definition to the escalation policy, complete the following steps.

1. Select **Monitor > Event Processing > Pseudo Events**.

   The **Pseudo Events** dialog box, shown in Figure 493, displays.

2. Click **Add**.

   The **Identification** pane of the **Add Pseudo Event** dialog box displays.

3. Enter a name for the pseudo event.

4. Select the **Enabled** check box to enable the event, and click **Next**.

   The **Policy** pane of the **Add Pseudo Event** dialog box displays.

5. Click the **Escalation** button, and then enter the duration of time the Event Processor will wait before generating the pseudo event. Specify the escalation time in minutes or seconds.

6. Click **Next**.

   The **Events** pane of the **Add Pseudo Event** dialog box displays.

7. Select a critical event, such as LinkDown, and click the right arrow button to move it to the **Selected Down Trap** list.

8. Select a remediation event, such as LinkUp, and click the right arrow button to move it to the **Selected Up Trap** list.

9. Click **Next** to advance to the **Summary** pane.

10. Click **Finish** to complete the pseudo event configuration.

    Now, you must create a new event action definition using the **Add Event Actions** dialog box. Refer to the following sections for instructions on performing this task.

    - "Creating an event action definition" on page 1166
    - "Creating a new event action definition by copying an existing definition" on page 1179
    - "Creating an event action with a pseudo event on the escalation policy" on page 1188
    - "Creating an event action with a pseudo event on the resolving policy" on page 1190
    - "Creating an event action with a pseudo event on the flapping policy" on page 1191

Creating an event action with a pseudo event on the escalation policy

To create an event action with a pseudo event on the escalation policy, complete the following steps.

1. Select **Monitor > Event Processing > Event Actions**.

   The **Event Actions** dialog box displays.

2. Click **Add** to display the **Identification** pane of the **Add Event Action** dialog box.
3. Enter a name and description for the event action and select the **Enabled** check box to enable the event.
4. Click **Next** to display the **Events** pane.

   By default, the **Events** pane of the **Add Event Action** dialog box displays.

5. Select the **Pseudo Events** event type from the **Show** list.

   The available pseudo events display.

6. Select the pseudo event you created and click **Next**.

   The **Sources** pane of the **Add Event Action** dialog box displays.

7. Select the source that you will use to monitor this event from the **Selected Sources** list.
8. Click **Next** to advance to the **Policy** pane of the **Add Event Action** dialog box.

   The **Policy** pane of the **Add Event Action** dialog box displays.

9. Click the **Take actions for the selected events when they occur** button if you want to take action for the selected events when they occur.
10. Click **Next** to advance to the **Action Group-Actions** pane of the **Add Event Action** dialog box.

    The **Action Group-Actions** pane of the **Add Event Action** dialog box displays.

11. Select the **Alert by E-mail** check box. An e-mail notification will be sent to the designated e-mail recipient if the policy criteria have been met.
12. Click **Next** to display the **Action Group - E-mail Settings** pane of the **Add Event Action** dialog box.

    The **Action Group - E-mail Settings** pane of the **Add Event Action** dialog box allows you to select e-mail recipients from a list, add new e-mail recipients, and compose e-mail messages.

13. Select the Management application user to whom the e-mail message will be sent from the **Available Recipients** list, and click the right arrow button to move the recipient to the **Selected Recipients** list.

    NOTE
    Make sure the user you select has an e-mail address defined in a user account.

14. Add additional e-mail recipient addresses in the **Other Recipients** field. Separate multiple e-mail addresses with a semicolon.
15. If you want the e-mail message for the alert to display a description on the subject line, enter the text in the **Subject Line** field.
16. If you want a prologue to be inserted at the beginning of the e-mail message, enter up to 255 characters in the **Body Prologue** field. The event action message follows the prologue.

17. If you want an epilogue to be placed at the end of the e-mail message, enter up to 255 characters in the **Body Epilogue** field.

    NOTE
    The prologue, the event action message, and the epilogue form the body of the e-mail alert.

18. Click **Next** to advance to the **Summary** pane.
19. Click **Finish**.

    The **Summary** pane of the **Add Event Action** dialog box displays an overview of the e-mail configuration you are creating.

For more information about adding an event action, refer to "Event action definitions" on page 1166.

Adding a pseudo event on the resolving policy

When a down event occurs, a resolving policy waits for a specified duration to see if the event remains in that state by checking if an up event occurs. If an up event occurs, a resolving pseudo event is generated by the Event Processor.

The following two-part procedure uses both the **Add Pseudo Events** dialog box and the **Add Event Actions** dialog box to create an event action with the resolving policy.

To add a pseudo event definition to the resolving policy, complete the following steps.

1. Select **Monitor > Event Processing > Pseudo Events**.

   The **Pseudo Events** dialog box displays.

2. Click **Add**.

   The **Identification** pane of the **Add Pseudo Event** dialog box displays.

3. Enter a name for the pseudo event, and select the **Enabled** check box to enable the event.
4. Click **Next**.

   The **Policy** pane of the **Add Pseudo Event** dialog box displays.

5. Click the **Resolve** button, and then enter the duration of time the Event Processor will wait before generating the pseudo event. Specify the resolve time in minutes or seconds.
6. Click **Next**.

   The **Events** pane of the **Add Pseudo Event Events** dialog box displays.

7. Select a critical event, such as LinkDown, and click the right arrow button to move it to the **Selected Down Trap** list.
8. Select a remediation event, such as LinkUp, and click the right arrow button to move it to the **Selected Up Trap** list.
9. Click **Finish** to complete the pseudo event configuration.

   Now, you must create a new event action definition using the **Add Event Actions** dialog box.

Creating an event action with a pseudo event on the resolving policy

To create an event action with a pseudo event on the resolving policy, complete the following steps.

1. Select **Monitor > Event Processing > Event Actions**.

   The **Event Actions** dialog box displays.

2. Click **Add** to display the **Identification** pane of the **Add Event Action** dialog box.
3. Enter a name and description for the event action and select the **Enabled** check box to enable the event.
4. Click **Next** to display the **Events** pane.

   By default, the **Events** pane of the **Add Event Action** dialog box displays.

5. Select the **Pseudo Events** event type from the **Show** list.

   The available pseudo events display.

6. Select the pseudo event you created and click **Next**.

   The **Sources** pane of the **Add Event Action** dialog box displays.

7. Select the source that you will use to monitor this event from the **Selected Sources** list.
8. Click **Next** to advance to the **Policy** pane of the **Add Event Action** dialog box.

   The **Policy** pane of the **Add Event Action** dialog box displays.

9. Define the frequency of the event's occurrence that would trigger the action.
   - Click the **Take actions for the selected event when they occur** button if you want to take action for the selected events when they occur.
   - Click the **Take actions for the selected events based on below criteria** button if you want to take action for the selected events based on specified criteria.
10. Click **Next** to advance to the **Action Group-Actions** pane of the **Add Event Action** dialog box.

    The **Action Group-Actions** pane of the **Add Event Action** dialog box displays.

11. Select **Apply as a Logging Policy** to indicate whether or not you want the event occurrence to be logged in the Management application database:
    - Select **Log** to log the occurrence in the Management application database.
    - Select **Drop** to not log the occurrence in the Management application database.
12. Click **Next** to advance to the **Summary** pane.
13. Click **Finish**.

For more information about adding an event action, refer to "Event action definitions" on page 1166.

Adding a pseudo event on the flapping policy

The flapping policy checks to see if the event consistently transitions between two opposite states during a specified length of time. If it does, then the specified action in the definition is performed.

The following two-part procedure uses both the **Add Pseudo Events** dialog box and the **Add Event Actions** dialog box to create an event action with the flapping policy.

To add a pseudo event on the flapping policy, complete the following steps.

1. Select **Monitor > Event Processing > Pseudo Events**.

   The **Pseudo Events** dialog box displays.

2. Click **Add**.

   The **Identification** pane of the **Add Pseudo Event** dialog box displays.

3. Enter a name for the pseudo event, and select the **Enabled** check box to enable the event.

4. Click **Next**.

   The **Policy** pane of the **Add Pseudo Event** dialog box displays.

5. Click the **Flapping** button, and then enter the duration of time the Event Processor will wait before generating the pseudo event. Specify the number of flapping times in minutes or seconds.

6. Click **Next**.

   The **Events** pane of the **Add Pseudo Event** dialog box displays.

7. Select a critical event, such as LinkDown, and click the right arrow button to move it to the **Selected Down Trap** list.

8. Select a remediation event, such as LinkUp, and click the right arrow button to move it to the **Selected Up Trap** list.

9. Click **Next** to advance to the **Summary** pane.

10. Click **Finish** to complete the pseudo event configuration.

    Now, you must create a new event action definition using the **Add Event Actions** dialog box.

Creating an event action with a pseudo event on the flapping policy

To create an event action with a pseudo event on the flapping policy, complete the following steps.

1. Select **Monitor > Event Processing > Event Actions**.

   The **Event Actions** dialog box displays.

2. Click **Add** to display the **Identification** pane of the **Add Event Action** dialog box.

3. Enter a name and description for the event action and select the **Enabled** check box to enable the event.

4. Click **Next** to display the **Events** pane.

   By default, the **Events** pane of the **Add Event Action** dialog box displays.

5. Select the **Pseudo Events** event type from the **Show** list.

The available pseudo events display.

6. Select the pseudo event you created and click **Next**.

   The **Sources** pane of the **Add Event Action** dialog box displays.

7. Select the source that you will use to monitor this event from the **Selected Sources** list.

8. Click **Next** to advance to the **Policy** pane of the **Add Event Action** dialog box.

   The **Policy** pane of the **Add Event Action** dialog box displays.

9. Click the **Take actions for the selected events when they occur** button if you want to take action for the selected events when they occur.

10. Click **Next** to advance to the **Action Group-Actions** pane of the **Add Event Action** dialog box.

    The **Action Group-Actions** pane of the **Add Event Action** dialog box displays.

11. Select the **Deploy CLI Configuration** check box and click the **Configure** button if you want to deploy a configuration from CLI Configuration Manager to products if the policy criteria have been met.

    NOTE
    If the CLI configuration you chose from CLI Configuration Manager contains a non-IronWare OSNetwork OS product as a target, the configuration will not be deployed to the non-IronWare OSNetwork OS product.

12. You can either select an existing CLI configuration or create a new one and select that configuration. After selecting a CLI configuration, the name of the CLI configuration is displayed in the **Selected Configuration** field.

    - **Has Parameters** - Displays **Yes** if the CLI configuration has parameters that require values to be entered before it can be deployed, and displays **No** if no parameter needs to be defined.
    - The **Parameters** list lists the parameters that need to be defined in the configuration.
      - The **Parameter** column displays the parameter and its variables in the CLI configuration.
      - The **Source** column lists the appropriate SNMP attributes for the parameters. Each attribute contains a specific parameter value, such as an IP address. Select the attribute you want from the list.
      - The **Transformation** column uses the product IP addresses and MAC addresses listed in the Address Finder. If the Address Finder list is empty, the product or port will not be found. From this column, specify what you want Event Processor to do with the value in the attribute:
        - **Find Device**: Find the product with the IP address in the attribute and deploy the CLI configuration to that product.
        - **Find Port**: Find the port on a product with the IP address in the attribute and deploy the CLI configuration to that port.
        - **Find Intruder MAC**: Find the product with the IP address in the attribute that matches the intruder MAC address and deploy the CLI configuration to that product.
        - **None**: The Event Processor only reports occurrence of the products.

13. Select the **Deploy Product Configuration** check box if you want to deploy a payload to the products if the policy criteria have been met.
14. Select the **Apply as a Logging Policy** check box to indicate whether or not you want the event occurrence to be logged in the Management application database:
    - Select **Log** to log the occurrence in the Management application database.
    - Select **Drop** to not log the occurrence in the Management application database.
15. Click **Next** to advance to the **Summary** pane.
16. Click **Finish**.

For more information about adding an event action, refer to "Event action definitions" on page 1166.

Event custom reports

The **Event Custom Reports** dialog box allows you to manage customized event filter definitions and schedule when the definitions are run.

To access the dialog box, select **Reports > Event Custom Reports**.

The **Event Custom Reports** dialog box, shown in Figure 496, displays.

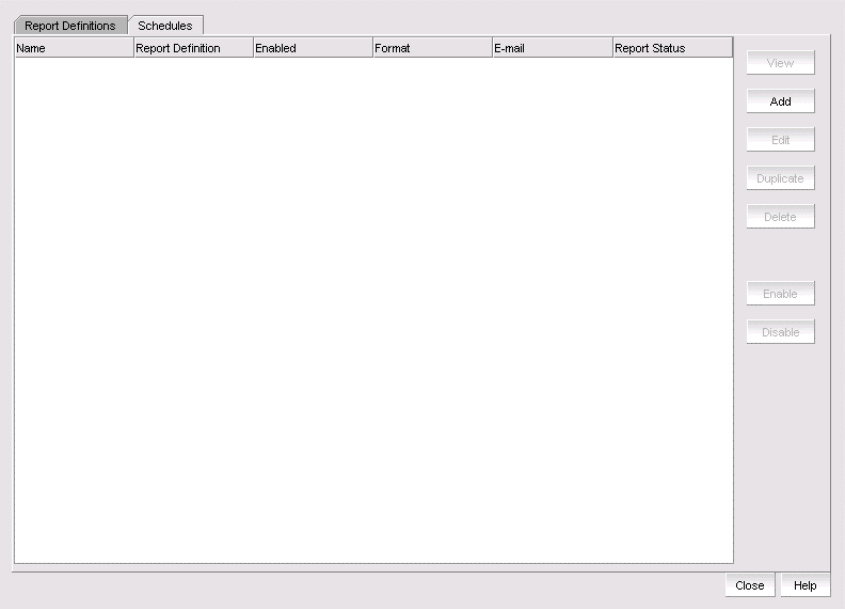


FIGURE 496 **Event Custom Reports dialog box - Report Definitions tab**

The **Event Custom Reports** dialog box has two tabs:

- The **Report Definitions** tab lists all the previously created report definition objects. This tab enables you to add a new definition or modify, delete, or duplicate existing report definitions.
- The **Schedules** tab lists all the previously created schedules on the report definition. This tab enables you to add a new schedule or modify, delete, or duplicate existing schedules. Users cannot view, edit, or share a schedule that was created by another user.

Defining report settings

You can configure report settings so that you see only a restricted set of information in a report.

NOTE
You can change the number of displayed event custom report records by following the procedure in "Configuring custom report preferences" on page 161. By default, 1000 records display, even if the event count is greater than 1000.

NOTE
You must first enter a name and title on the **Identification** tab before you can run the result settings.

To configure report settings, complete the following steps.

1. Select **Reports > Event Custom Reports**.

   The **Event Custom Reports** dialog box displays.

2. Click the **Add** button.

3. The **Add/Edit Report Definition** dialog box - **Product** tab, shown in Figure 497, displays.

4. Click the **Result Settings** tab.

   The **Add/Edit Report Definition** dialog box - **Result Settings tab** displays.

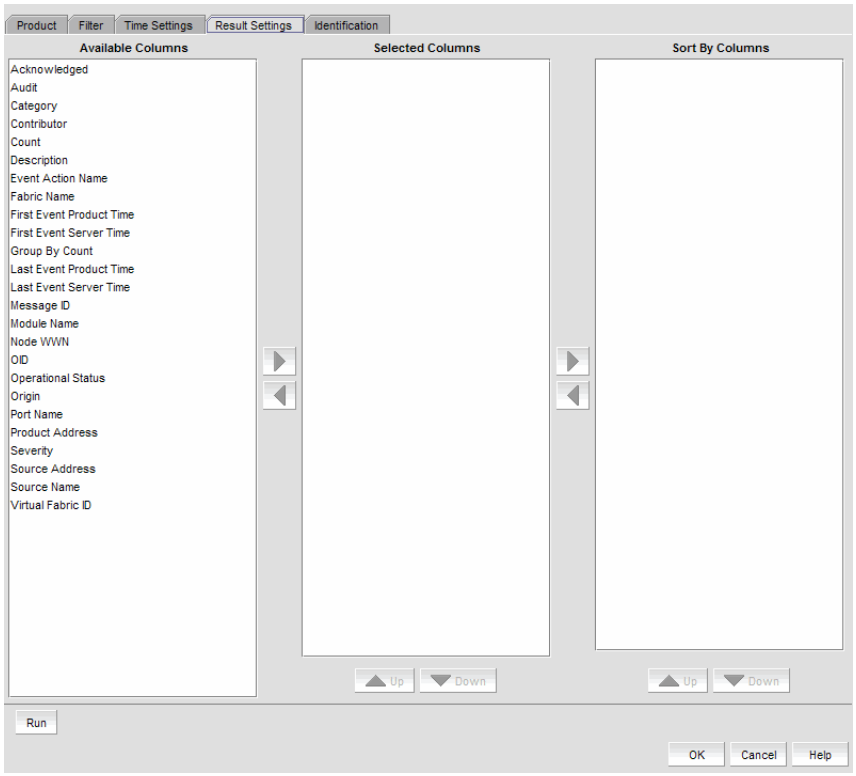


FIGURE 497 Add/Edit Report Definition dialog box - Result Settings tab

NOTE
The **Available Column** list lists the attributes you can include in the report. Each attribute represents a column on the report.

5. Select the attribute you want, then click the right arrow to move your selection to the **Selected Columns** list. To remove an attribute from the **Selected Columns** list, select the attribute that you want to remove, then click the left arrow button.
   - If you selected the **Count** column, the Management application adds the **First Seen** and **Last Seen** columns to a report.
   - For products that support stacking, the **Port** column shows the port.
6. Data for all attributes is sorted in ascending order and is sorted in the sequence that the attributes appear in the **Sort By Columns** list. In the **Selected Columns** list, select which attribute will be used to sort the generated report. Then click the right arrow button to move your selection to the **Sort by Columns** list. To remove an entry from the **Sort by Columns** list, select the entry, then click the left arrow button.
7. Click **OK** to save the definition, **Run** to launch the report, or click the **Identification** tab to display the parameters that you use to identify the definition.

Defining the report identity

The **Identification** tab in the **Event Custom Reports** dialog box allows you to enter the identity information of the report information.

To define the report identity, complete the following steps.

1. Select **Reports > Event Custom Reports**.

   The **Event Custom Reports** dialog box displays.
2. Click the **Add** button.
3. The **Add/Edit Report Definition** dialog box - **Product** tab displays.
4. Click the **Identification** tab.

   The **Add/Edit Report Definition** dialog box - **Identification** tab, shown in Figure 498, displays.

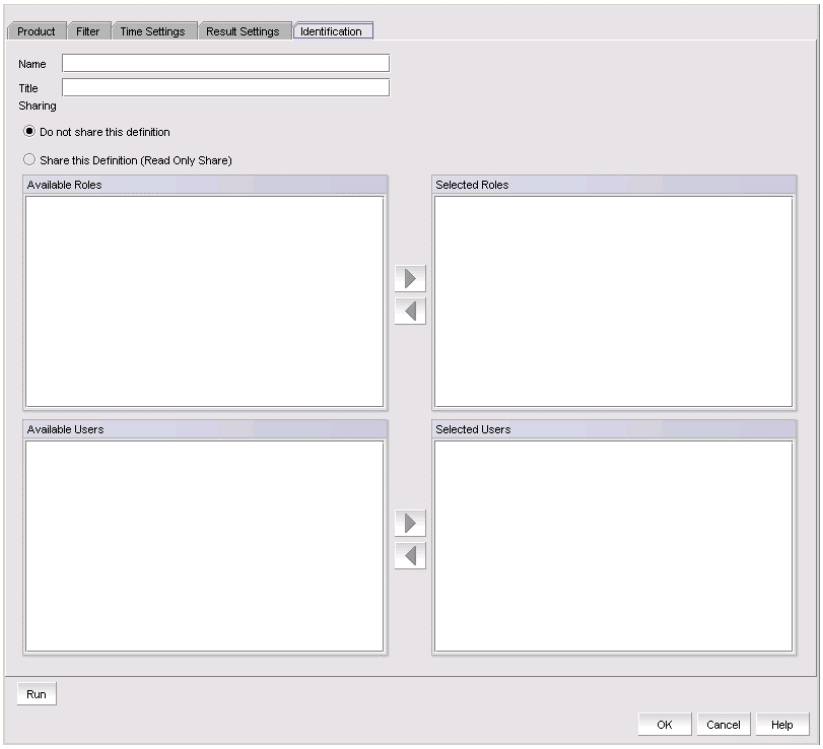


FIGURE 498 Add/Edit Report Definition dialog box - Identification tab

5. In the **Name** field, enter a name for the definition.

   This name appears under the **Name** column on the **Report Definitions** tab of the **Event Custom Reports** dialog box. This name must be unique for each report group. This is a required parameter.

6. In the **Title** field, enter a title for the definition, which will be used as the title of a generated report. This is a required parameter.

7. Click the **Do not share this definition** button if you do not want to share this definition with other Management application users.

   If you select this button, no Management application users will see this definition on the **Report Definitions** tab of the **Event Custom Reports** dialog box when they log in.

8. Click the **Share this definition (Read only)** button if you want other Management application users to have Read Only permission for this definition.

   If you selected the **Share this definition (Read only)** button, a list of Management application roles appears in the **Available Roles** list.

9. Select the roles that will have view and run access to this definition, then press the right arrow button to move the role in the **Selected Roles** list.

NOTE
All Management application users who have the selected roles will be able to view, copy, and run the definition.

10. Select the roles that will have view and run access to this definition, then press the right arrow button to move the role in the **Selected Roles** list.

    All Management application users who have the selected roles will be able to view, copy, and run the definition.

    NOTE
    You can share the available users definition with specific Management application users. If you click the **Share this definition (Read only)** button, a list of Management application user accounts appears in the **Available Users** list.

11. Select the user account that will be able to view and run this definition, then press the right arrow button to move that user account in the **Selected Users** list.
12. Click **OK** to save the definition, or click **Run** to launch the report.

Filtering a report definition

You can filter a report definition. To do so, you must first enter a name and title on the **Identification** tab and select at least one column in the **Results Setting** tab to run or save a filter. You can select from the available list of SAN products, IP products, or hosts by selecting the appropriate tab.

NOTE
The swDeviceStatusTrap (OID 1.3.6.1.4.1.1588.2.1.1.0.15) trap is sent from the switch whenever there is a device login or logout. This trap is part of the SW-MIB and is listed under the SW-MIB of the **SNMP Trap Recipients** dialog box, the **Event Actions** dialog box, and the **SNMP Trap Forwarding** dialog box. For a complete list of event categories, refer to "Event Categories" on page 1277.

To filter a report definition, complete the following steps.

1. Select **Reports > Event Custom Reports**.

   The **Event Custom Reports** dialog box displays.

2. Click the **Add** button.
3. The **Add/Edit Report Definition** dialog box - **Product** tab, shown in Figure 499, displays.

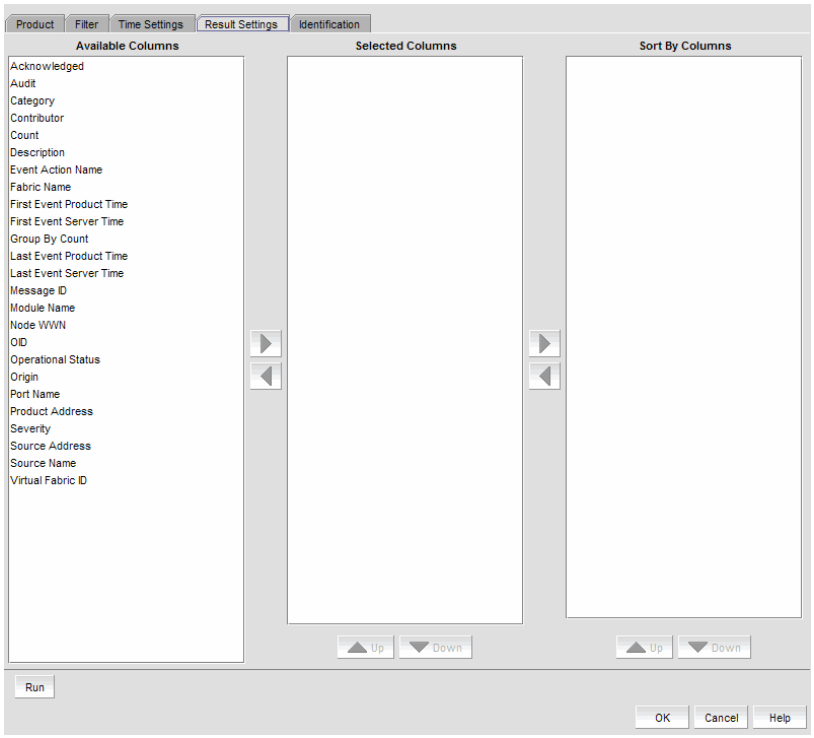


FIGURE 499 Add/Edit Report Definition dialog box - Product tab

4. Click the **Filter** tab.

   The **Add/Edit Report Definition** dialog box - **Filter** tab, shown in Figure 500, displays.

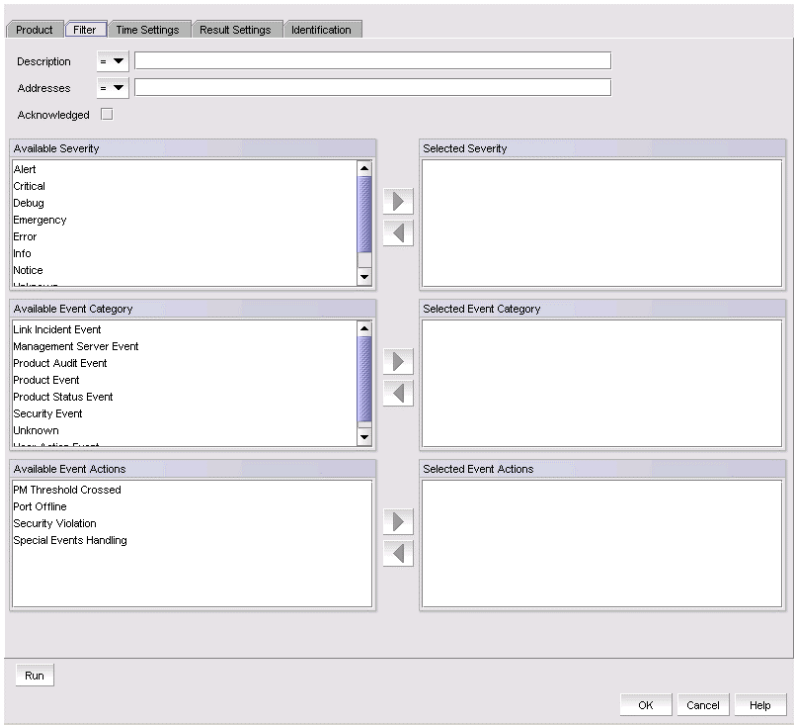


FIGURE 500 Add/Edit Report Definition dialog box - Filter tab

5. To limit the search results to traps, syslog, and pseudo event messages with a specific text string, enter the text string in the **Description** field.

   You can use an asterisk (*) to indicate a wildcard, as in the following examples:

   - *cdef: Matches a message ending with cdef
   - abc*: Matches a message beginning with abc
   - *abc*: Matches a message that contains abc

   For example, if you want to find the events that have the text “Auth” in the message, enter “*Auth*”.

   NOTE
   You can view all port history events for a switch by creating an event custom report and entering a description of **Port Login/Logout History** for that particular switch. The Port Login/Logout history trap will be listed under the **Available traps** list of the **Add Trap Filter** dialog box and the **Add Event Action** dialog box — **Events** pane.

   For information about event categories, refer to “Event Categories” on page 1277.

6. To limit the search results to traps, syslog, and pseudo event messages from a specific IP address, enter the IP address or the AP MAC address in the **Address** field. You can enter multiple addresses. Separate each address with a comma.
7. Select the **Acknowledge** check box if you want messages that have been acknowledged to be included in the report.
8. Select the severity from the **Available Severity** list, and click the right arrow button to move your selection to the **Selected Severity** list. Events with the selected severity are included in the report.
9. Select the event type you want to include in the report from the **Available Event Category** list. Click the right arrow button to move your selection to the **Selected Event Category** list.
10. Select the event action you want to include in the report from the **Available Event Actions** list. Click the right arrow button to move your selection to the **Selected Event Actions** list.
11. Click **OK** to save the definition, **Run** to launch the report, or click the **Time Settings** tab on the **Add/Edit Report Definition** dialog box if you want to filter the events by date and time.

Filtering report events by date and time

The **Event Custom Reports** dialog box — **Time Settings** tab allows you to specify the time range of the events to be reported.

To filter report events by date and time, complete the following steps.

1. Select **Reports > Event Custom Reports**.

   The **Event Custom Reports** dialog box displays.

2. Click the **Add** button.

   The **Add/Edit Report Definition** dialog box - **Product** tab displays.

3. Click the **Time Settings** tab.

   The Add/Edit Report Definition dialog box - Time Settings tab, shown in Figure 501, displays.

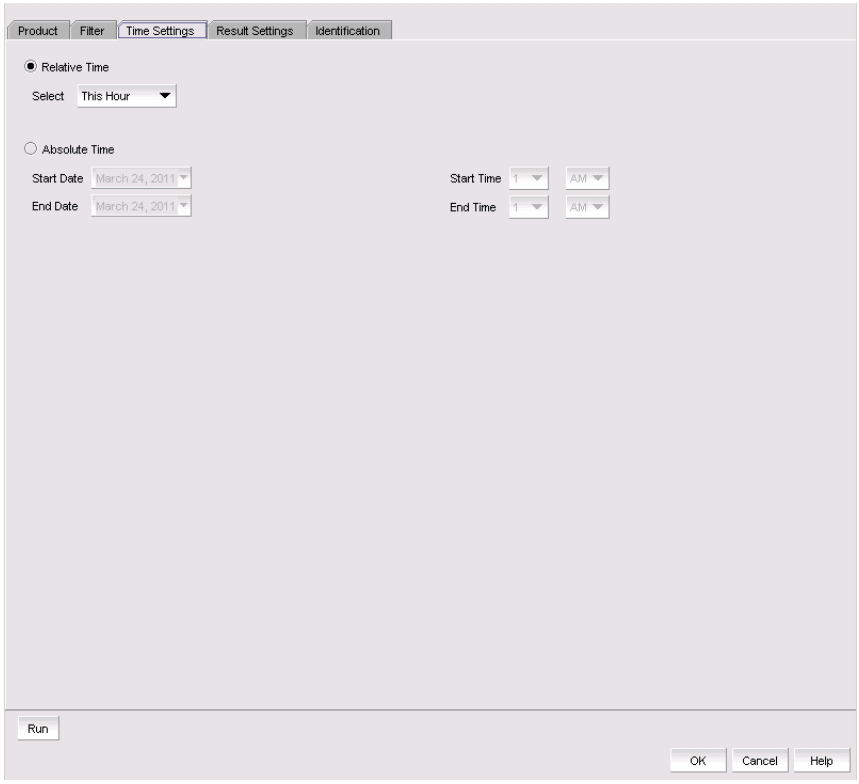


FIGURE 501 Add/Edit Report Definition dialog box - Time Settings tab

4. Choose between relative time (the default) and absolute time.
   - Click **Relative Time** if you want to filter traffic based on when the report is generated, and then select a relative time from the **Range** list. Relative time is calculated based on the date and time the report is generated.
   - Click **Absolute Time** if you want to filter traffic sent at a specific date and time.
     a. Select the specific start date from the **Start Date** list.
     b. Select the specific hour time for the start time from the **Start Time** list, and select AM or PM.
     c. Select the specific end date from the **End Date** list.
     d. Select the specific hour for the end time from the **End Time** list, and select AM or PM.
5. Click **OK** to save the definition, or click **Run** to launch the report.

Creating a new report definition by copying an existing definition

The simplest way to create a new report definition is by copying an existing definition.

To create a new report definition is by copying an existing definition, complete the following steps.

1. Select the definition you want to copy from the **Report Definitions** tab of the **Event Custom Reports** dialog box.
2. Click **Duplicate**.

   The name of the definition is the name of the selected definition with the word "copy" appended. For example, "SelectedPortName" becomes "SelectedPortName copy".
3. Click the **Identification** tab to enter a new name and description for the new definition.
4. Make changes to the report as required.
5. Perform one of the following tasks when you are finished modifying the definition:
   - Click **OK** to save the report.
   - Click **Cancel** to discard your changes and exit from the **Report Definitions** tab of the **Event Custom Reports** dialog box.
   - Click **Reset** to discard your changes without exiting from the **Report Definitions** tab of the **Event Custom Reports** dialog box.
   - Click **Run** to launch the report.

The new definition is added to the **Report Definitions** tab of the **Event Custom Reports** dialog box.

Editing a report definition

For your definitions, you can modify a definition and save the changes you have made. For a shared definition from another user, you can modify the definition, then run that definition to obtain the desired report; however, you will not be able to save your changes.

To edit a report definition, complete the following steps.

1. Click the **Report Definitions** tab of the **Event Custom Reports** dialog box and select the definition you want to modify.
2. Click **Edit**.
3. When the **Add/Edit Report Definition** dialog box displays, modify the definition. (Refer to "Filtering a report definition" on page 1197.)
4. When you have finished, perform one of the following tasks:
   - If you own this definition, the **OK** button is available. Click **OK** to save your changes.
   - Click **Run** to generate the report.
   - Click **Cancel** to discard your changes and exit the **Report Definitions** tab of the **Event Custom Reports** dialog box.

Deleting a report definition

You can delete a report definition, but only if it belongs to you.

To delete a report definition, complete the following steps.

1. To access the dialog box, select **Reports > Event Custom Reports**.

   The **Event Custom Reports** dialog box displays.

2. Click the **Report Definitions** tab of the **Event Custom Reports** dialog box and select the definition you want to delete.

3. Click the **Delete** button.

   A message displays, prompting you to confirm the deletion.

4. Click **Yes** to delete the definition or **No** to cancel your request.

Event custom report schedules

Click the **Schedules** tab, shown in Figure 502, to display its contents. The **Schedules** list shows the definitions that have been scheduled to automatically run at a specified date and time.

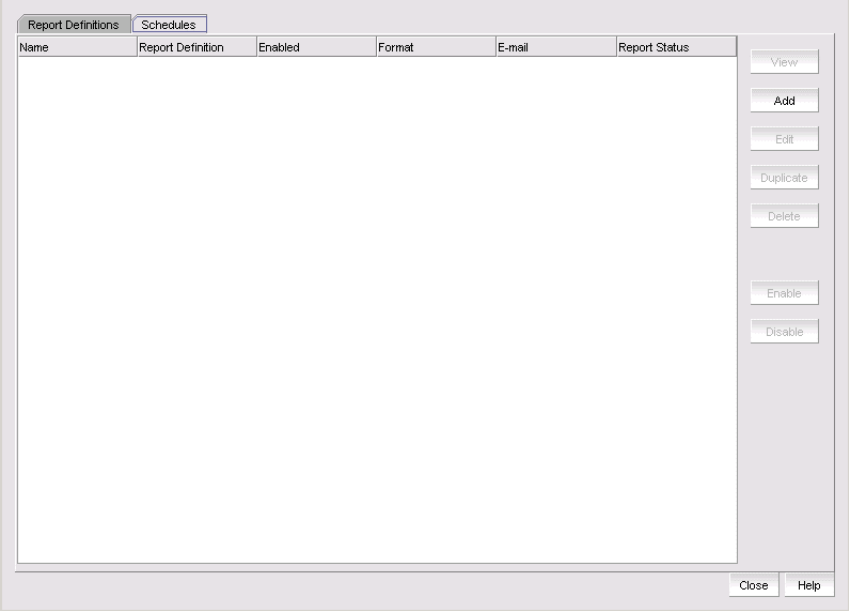


FIGURE 502 Schedules tab of the Event Custom Reports dialog box

From the **Schedules** tab of the **Event Custom Reports** dialog box, you can perform the following tasks:

- **View —** Displays the report data of the scheduled report definition. The **View** button is not enabled for a report that is listed as Not Available.
- **Add** — Launches the **Add Schedule** dialog box.
- **Edit** — Launches the **Edit Schedule** dialog box with the selected schedule information pre-populated.

- **Duplicate** — Creates a copy of the selected report schedule.
- **Delete —** Deletes the selected schedule from the **Schedules** list.
- **Enable** — Enables the selected schedule.
- **Disable** — Disables the selected schedule.

Adding or editing an event report schedule

The **Add Schedule** dialog box, shown in Figure 503, allows you to select an existing report definition and configure the parameters, such as the schedule's format, frequency, recipients, and message content, for when the report is run and to whom the report is sent.

To add or edit an event report schedule, complete the following steps.

1. Select **Reports > Event Custom Reports**.

   The **Event Custom Reports** dialog box displays.

2. Click the **Schedules** tab.
3. Click the **Add** button.

   The **Add Schedule** dialog box displays.

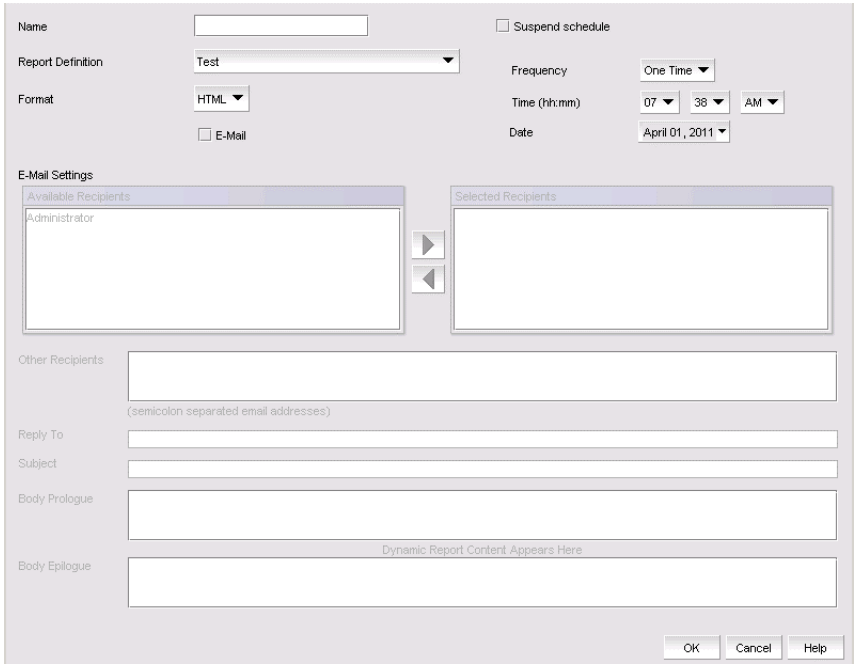


FIGURE 503 Add Schedule dialog box

4. Enter the name of the new schedule in the **Name** field. You must enter a unique name for the schedule. The name can be up to 64 characters in length and it is case-sensitive.
5. Select the **Suspend schedule** check box if you want to disable the schedule. For example, you may want to temporarily prevent a report from being generated until further notice. You can clear the check mark to resume the automatic generation of the report.
6. Select the report definition you want to schedule from the **Report Definition** list. If a report is deleted, the corresponding schedule will be deleted.

7. Select one of the following periods from the **Frequency** list:
    - **One Time**
    - **Hourly** — If you selected **Hourly** as the schedule type, **Minutes past the hour** appears. Select the minutes after the hour when the report will be generated.
    - **Daily** — If you selected **Daily** as the schedule type, **Time (hh:mm)** appears.
    - **Weekly** — If you selected **Weekly** as the schedule type, **Day of the week** appears. Select the day of the week when the report will be generated.
    - **Monthly** — If you selected **Monthly** as the schedule type, **Day of the month** appears. Select the day of the month when the report will be generated.
    - **Yearly** — If you selected **Yearly** as the schedule type, **Day of the year** appears. Select the day of the year when the report will be generated.
8. Select a report format from the **Format** list: HTML or CSV.
9. Select the time when the report will be generated. Indicate the hour, minute, and whether it is AM or PM. This parameter appears if you selected any schedule type except **Hourly**.
10. Select the **E-mail** check box if you want the report to be sent to e-mail recipients. The server limits the displayed or sent report to 1000 records.
11. Change the value of the customReports.MaxRecordsToDisplay parameter in the configuration.properties file to the number of records you want displayed or sent.
12. Indicate the date when the report is generated. Open the calendar and select the date. This parameter appears if you selected **One Time** or **Yearly** as the schedule type.
13. Enter an e-mail address to which the e-mail recipient can send a response. The e-mail address is a mandatory field.
14. From the **Available Recipients** list, select the user to whom the report will be sent. Click the right arrow button to move that user name to the **Selected Recipients** list. Click the left arrow button to remove the name from the **Selected Recipients** list and return it to the **Available Recipients** list.

    NOTE
    Make sure an e-mail address is configured in the user's account for the selected user.

15. Enter other e-mail addresses to which the report should be sent in the **Other Recipients** field, separating multiple addresses with a semicolon. At least one e-mail address from the **Application Recipients** or **Other Recipients** must be entered.
16. In the **Reply To** field, enter an e-mail address to which the e-mail recipient can send a response. This is a mandatory field.
17. In the **Subject Line** field, enter the text that you want to appear in the subject line of the e-mail message. You can leave this field empty.
18. If you want introductory text to be included at the beginning of the e-mail message, enter the text in the **Body Prologue** field. The maximum number of characters supported by the **Body Prologue** field is 256.
19. If you want specific text to be included at the end of the e-mail message, enter that text in the **Body Epilogue** field. The maximum number of characters supported by the **Body Epilogue** field is 256.

Event logs

You can view all events that take place through the Master Log at the bottom of the main window. You can also view a specific log by selecting an option from the **Logs** submenu of the **Monitor** menu. The logs are described in the following list:

- **Audit Log —** Displays all Application Events raised by the application modules and all Audit Syslog messages from the switches and Brocade HBAs.
- **Product Event Log —** Displays all Product Event type events from all discovered switches and Brocade HBAs.
- **Security Log —** Displays all security events for the discovered switches.
- **Syslog Log —** Displays syslog messages from switches and HBAs.

The Management application also has an event notification feature. By configuring event notification, you can specify when the application should alert you of an event. For details, refer to "Configuring e-mail notification" on page 1142.

For information about the Master Log interface, fields, and icons, refer to "Master Log" on page 287.

Viewing event logs

You can view log data through the Master Log on the main window. If you want to see only certain types of events; for example only security events, open a specific log through the **Logs** dialog box.

NOTE
You can also launch the Fabric logs and the Product Status logs from the status bar.

To view an event log, complete the following steps.

1. Select **Monitor > Logs >** <*Log_Type*>.

   The <*Log_Type*> **Logs** dialog box displays the type of log you selected.

2. Review the information in the log.
3. Click **Close**.

Copying part of a log entry

You can copy data from logs to other applications. Use this method to analyze or store the data using another tool.

To copy part of an event log, complete the following steps.

1. Select **Monitor > Logs >** <*Log_Type*>.

   The <*Log_Type*> **Logs** dialog box displays the type of log you selected.

2. Select the rows you want to copy:
   - To select contiguous rows, select the first row you want to copy, press **Shift**, and click the contiguous row or rows you want to copy.
   - To select non-contiguous rows, select the first row you want to copy, press **CTRL**, and click the additional row or rows you want to copy.

3. Right-click one of the selected rows and select **Copy Rows**.
4. Open the application to which you want to paste the data.
5. Click where you want to paste the data.
6. Press **CTRL+V** (or select **Edit > Paste** from the other application).

   All data and column headings are pasted.
7. Click **Close** to close the dialog box.

Copying an entire log entry

You can copy data from logs to other applications. Use this method to analyze or store the data using another tool.

To copy an event log, complete the following steps.

1. Select **Monitor > Logs >** <*Log_Type*>.

   The <*Log_Type*> **Logs** dialog box displays the type of log you selected.
2. Right-click a row and select **Copy Table**.
3. Open the application to which you want to paste the data.
4. Click where you want to paste the data.
5. Press **CTRL+V** (or select **Edit > Paste** from the other application).

   All data and column headings are pasted.
6. Click **Close** to close the dialog box.

Exporting the entire log

You can export the log data to a tab-delimited text file.

To export an event log, complete the following steps.

1. Select **Monitor > Logs >** <*Log_Type*>.

   The <*Log_Type*> **Log** dialog box displays the type of log you selected.
2. Right-click a row and select **Export Table**.

   The **Save table to a tab delimited file** dialog box displays.
3. Browse to the location where you want to export the data.
4. Enter a name for the file in the **File Name** field.
5. Click **Save**.

   All data and column headings are exported to the text file.
6. Click **Close** to close the dialog box.

E-mailing all event details from the Master Log

NOTE
You must configure e-mail notification before you can e-mail event details from the Master Log. To configure e-mail notification, refer to "Configuring e-mail notification" on page 1142.

To e-mail all event details from the Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
2. Select **E-mail > All.**

   The **E-mail** dialog box displays.
3. Enter the e-mail address of the person to receive the e-mail notifications in the **To** field.
4. Enter your e-mail address in the **From** field.
5. Click **OK**.

E-mailing selected event details from the Master Log

NOTE
You must configure e-mail notification before you can e-mail event details from the Master Log. To configure e-mail notification, refer to "Configuring e-mail notification" on page 1142.

To e-mail selected event details from the Master Log, complete the following steps.

1. Right-click the selected events in the Master Log.
2. Select the events that you want to e-mail.
3. Select **E-mail > Selection.**

   The **E-mail** dialog box displays.
4. Enter the e-mail address of the person to receive the e-mail notification in the **To** field.
5. Enter your e-mail address in the **Reply From** field.
6. Click **OK**.

Displaying event properties from the Master Log

You can view detailed information for an event.

NOTE
Network OS events display in both the SAN and IP tab of the Master Log.

To display event details from the Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
2. Select **Properties**.

   The **Event Properties** dialog box, shown in Table 98, displays.
3. Review the information.

TABLE 98 Event Properties

Event Field	Description
Probable Cause	The most likely reason the event occurred.
Description	A description of the event.
Count	Number of times this event occurred on the host.
Origin	The event's origin, for example, SNMP trap.
Message ID	The message associated with the event.
Port Name	The port name associated with the event.
First Event Server Time	The time the event occurred.
Fabric Name	The VCS fabric name.
Product Address	The IP address of the product on which the event occurred.
Audit	Information regarding the audit.
Category	One of the following event categories, which are detailed in "Event Categories" on page 1277: • Product Event • Link Incident Event • Product Audit Event • Product Status Event • Security Event • User Action Event • Management Server Event
Last Event Product Time	The day, date, and time the last event occurred on the product.
Last Event Server Time	The day, date, and time the last event occurred on the server.
Severity	The event severity.
Source Name	The source of the event.
Virtual Fabric ID	The virtual fabric identifier.
Contributor	The contributor to this event.
Recommended Action	The recommended action to take to remedy the event.
First Event Product Time	The day, date, and time the first event occurred on the product.
Operational Status	The product's operational status.
Module Name	The module associated with the event.
Source Address	The IP address of the source.
Acknowledged	Indicates whether the event has been acknowledged.

4. Click **Close** to close the **Event Properties** dialog box.

Copying part of the Master Log

You can copy data from logs to other applications. Use this method to analyze or store the data using another tool.

To copy part of the Master Log, complete the following steps.

1. Select the rows you want to copy in the Master Log:
   - To select contiguous rows, select the first row you want to copy, press **Shift**, and click the contiguous row or rows you want to copy.
   - To select non-contiguous rows, select the first row you want to copy, press **CTRL**, and click the additional row or rows you want to copy.
2. Right-click one of the selected rows and select **Table > Copy Rows**.
3. Open the application to which you want to paste the data.
4. Click where you want to paste the data.
5. Press **CTRL+V** (or select **Edit > Paste** from the other application). All data and column headings are pasted.

Copying the entire Master Log

You can copy the entire Master Log to other applications. Use this method to analyze or store the data using another tool.

To copy the entire Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
2. Select **Table > Copy Table**.
3. Open the application to which you want to paste the data.
4. Click where you want to paste the data.
5. Press **CTRL+V** (or select **Edit > Paste** from the other application). All data and column headings are pasted.

Exporting the Master Log

You can export the Master Log to a tab-delimited text file. Use this method to analyze or store the data using another tool.

To export the Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
2. Select **Table > Export Table**.

   The **Save table to a tab delimited file** dialog box displays.
3. Browse to the location where you want to export the data.
4. Enter a name for the file in the **File Name** field.
5. Click **Save**. All data and column headings are exported to the text file.
6. Click **Close** to close the dialog box.

Filtering events in the Master Log

You can filter the events that display in the Master Log on the main window. By default, all event types display in the **Selected Events** list.

When you select a filter from the **Filter** drop-down menu, the Master Log refreshes to display the events associated with that filter. This filter setting is kept when you exit the client.

For more information about the Master Log, refer to "Master Log" on page 287.

To filter events in the Master Log, complete the following steps.

1. Select the filter you want from the **Filter** drop-down menu at the top of the Master Log panel.

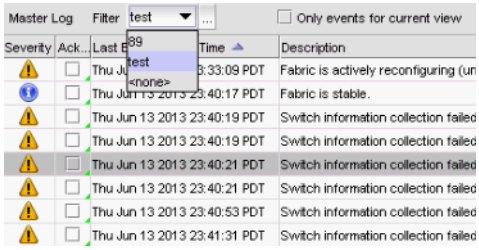


FIGURE 504 Master Log Filter menu

2. If you do not see the filter you want, click the **...** button immediately to the left of the menu.

   The **Define Filters** dialog box displays.

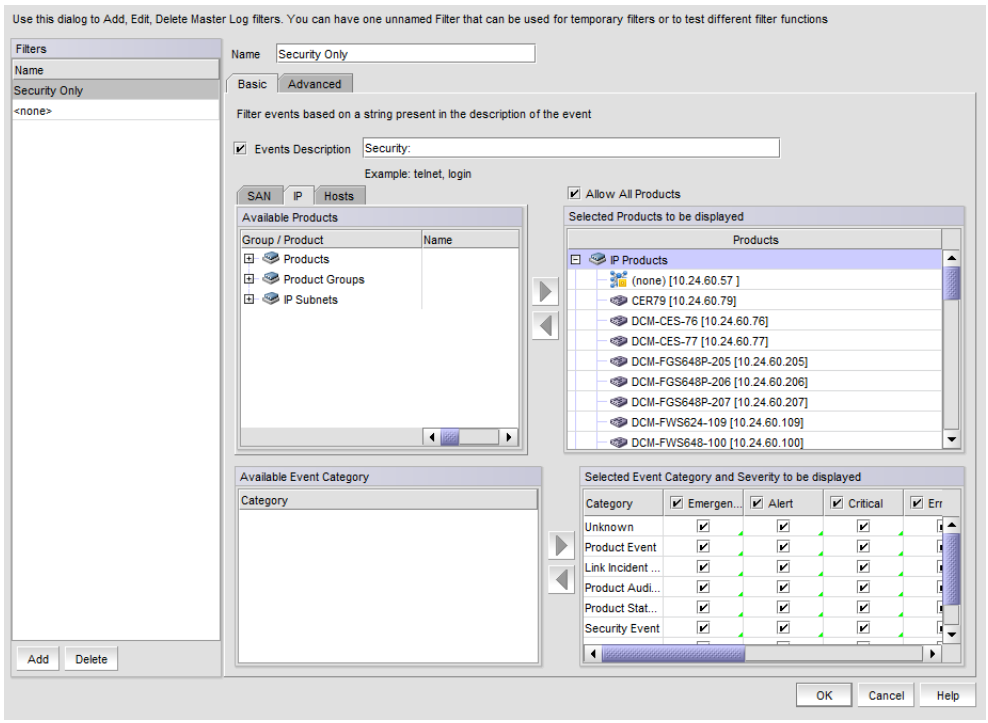


FIGURE 505 Define Filter dialog box - Basic tab, IP tab selected

3. Use the following to include or exclude products.

- To include an event type in the filter, select the event from the **Available Products** list and click the right arrow.
- To exclude an event type from the filter, select the event from the **Selected Products to be displayed** list and click the left arrow.
- To include all products, select the **Allow All Products** check box.

4. Select from the following to include or exclude event types.
   - To include an event type in the filter, select the event category from the **Available Event Category** list and click the right arrow.
   - To exclude an event type from the filter, select the event from the **Selected Event Category and Severity to be displayed** list and click the left arrow.
5. From the **Selected Event Category and Severity to be displayed** list, select one of the following severity levels to assigned to the selected event action:
   - Emergency
   - Alert
   - Critical
   - Errors
   - Warning
   - Notice
   - Info
   - Debug
   - Unknown

   Clear the severity level check boxes to turn off the filter for the selected events.
6. (Optional) To filter events based on a string (such as telnet or login) that appears in the event description, select the **Events Description** check box and enter the string that the filter is to use in the associated text box.
7. Enter a name for the filter in the **Name** field. The Filter name length is limited to 128 alphanumeric characters. You cannot use other characters in this text box.
8. If you want to create multiple filters, click **Add** after you define the filter. This adds the defined filter to the Filters list, but does not close the dialog.
9. When you have created all the filters you want, click **OK**.

   The Define Filters dialog closes and you are returned to the main window.

The 'unnamed' filter

If a filter is migrated from a previous release, it is saved with the name **unnamed**. If a filter was not present in the release you are migrating from, then there will be no **unnamed** filter. If the **unnamed** filter was the default filter for you in the previous release, it will be set as the default filter for you in the current release.

The 'none' filter

The filter named **none** is the default configuration filter. You cannot to edit or delete this filter. Selecting this filter lets you view Master Log events with no filtering applied. This is the default filter selected when no other filter is applied by the user or when there is no migrated filter.

Editing a Filter

To edit a filter, select the filter you want to edit in the Filters panel and make the desired changes to the filter configuration. Any changes you make will be reflected in the Filters panel when navigating to another filter, but changes are not made permanent until you click OK.

Duplicating a Filter

To duplicate a filter, select the filter you want to duplicate in Filters panel and click Add. The content of the selected filter will be loaded, but with the name field left blank. Enter a name for the new filter and click OK.

Deleting a Filter

To delete a filter, select the filter and click Delete. Deleting a filter removes the filter name from the Filters panel of the Define Filters dialog box. A filter is not permanently deleted until you click OK.

Notes on filters

- Changing the filter in one client session does not alter the filter selection on other clients. However, if the currently selected filter is updated, once the filter is saved, the master log is reloaded to reflect the changes to that filter. This affects all your client sessions.
- If the currently selected filter is deleted, the master log is reloaded, and changes the selected filter to **none** for all your client sessions.
- Copying user preferences includes all user-created filters.

Chapter

38

Packet Capture (Pcap)

In this chapter

Configuring packet captures

Organizations can configure switches as sensors to capture packets through the embedded sFlow capability and send them back to the Management application, which acts as an sFlow collector. The Management application then converts the sFlow data to Pcap format, which is understood by a variety of open source products. The open source products can then provide valuable tools to detect and defend against network attacks.

NOTE
Snort® is the only Pcap-aware tool supported by the Management application. For more information, refer to "Snort message forwarding" on page 1166.

To configure packet captures (PCAP)-related properties, complete the following steps:

1. Select **Configure > Packet Capture (Pcap).**

   The **Configure Pcap** dialog box, shown in Figure 506, displays.

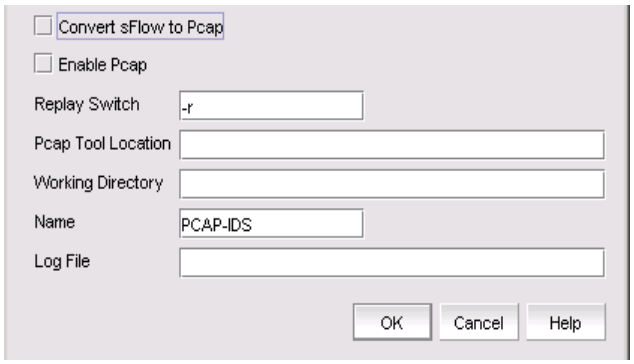


FIGURE 506 Configure Pcap dialog box

2. Click the **Convert sFlow to Pcap** check box to convert sFlow data to PCAP-formatted packets.
3. Click the **Enable Pcap** check box to instruct the Management application to analyze the PCAP-formatted packets.
4. Enter a value required by your PCAP-aware tool in the **Replay Switch** text box. This parameter is used to send data to the PCAP-aware tool. The default value is -r.
5. Enter the full path of the command that will be invoked to launch the PCAP-aware tool into the **Pcap Tool Location** text box.

For example, if SNORT is installed under the C:\\SNORT\ directory, enter the following commands to launch SNORT:

```
C:\\SNORT\bin\SNORT.exe -c
C:\\SNORT\etc\SNORT.conf -Xeds -K none
```

6. Specify the working directory for the PCAP-aware tool in the **Working Directory** text box.

   If this field is blank, the default directory is set to the *Install_Home*\bin directory.

7. Type the name of the PCAP-aware tool in the **Name** text box.

   This name is displayed in the Management application's event log to identify a message showing PCAP activity. If this field is blank, the default name "PcapAppl1" is used.

8. Enter the name of the file that will be used to log the output of the sFlow to PCAP conversion in the **Log File** text box.

   If this field is blank, the process output is logged to the default "PcapApp1.log file in the working directory.

9. Click **OK**.

Chapter

Technical Support

39

In this chapter

Server and client support save

You can use Technical Support to collect SupportSave data for the Management server and clients.

Server Support save data includes:-

- Engineering logs
- Events
- Configuration files
- Operating system-specific information
- Environment information
- Vital CPU, memory, network resources
- Agent and driver logs
- Install logs
- Core files
- Database (partial or full)
- Web Tools data

Client Support save data includes:-

- Client Log Files
- Client data model log

Capturing Server and Client support save data

To capture both server and client support save files, complete the following steps.

1. Select **Monitor > Technical Support > SupportSave**.

   The **SupportSave** dialog box displays.

2. Select the **Server SupportSave** check box to run supportsave on the server.
3. Enter a file name for the server support save file in the **File Name** field.

   The default file name is DCM-SS-*Time_Stamp*.

4. Select the **Include Database** check box to include the database in the support save and choose one of the following options.
   - Select the **Partial** (Excludes historical performance data and events) option to exclude historical performance data and events from the database capture.
   - Select the **Full** option to capture the entire database.

   Clear the **Include Database** check box to exclude the database in the support save.
5. Select the **Client SupportSave** check box to run supportsave on the client.
6. Enter a file name for the client support save file in the **File Name** field.

   The default file name is DCM-Client-SS-*Time_Stamp*.
7. Click **OK** on the **SupportSave** dialog box.
8. Click **OK** on the message.

   A progress message displays with a list of the steps to be performed:
   - Capturing client support save
   - Capturing logs and server data
   - Capturing partial/full database
   - Capturing data from the products

   You cannot close the progress message and you cannot perform any other actions until the SupportSave is complete.

   The application generates separate master logs to show the status of the Server and Client Support save collection.

   You cannot change the destination directory for Server and Client support save. Here are the default directories:
   - Server Support save location: *Install_Home*/support
   - Client Support save locations:
     - (Local client) *User_Home/Management_Application_Name/*localhost/support
     - (Remote client) *User_Home/Management_Application_Name/*Server IP/support

NOTE
Server support save initiated from the remote client is only available from a client installed on the server. However, you can copy the server support save from the **View Repository** dialog box (using the **Save** button) to the remote client location.

Capturing Server support save data

To capture server support save files, complete the following steps.

1. Select **Monitor > Technical Support > SupportSave**.

   The **SupportSave** dialog box displays.
2. Select the **Server SupportSave** check box to run supportsave on the server.
3. Make sure the **Client SupportSave** check box is clear.

4. Enter a file name for the server support save file in the **File Name** field.

   The default file name is DCM-SS-*Time_Stamp*.

5. Select the **Include Database** check box to include the database in the support save and choose one of the following options.

   - Select the **Partial** (Excludes historical performance data and events) option to exclude historical performance data and events from the database capture.
   - Select the **Full** option to capture the entire database.

   NOTE
   Selecting the **Full** option may increase the time needed for the SupportSave to complete.

   Clear the **Include Database** check box to exclude the database in the support save.

6. Click **OK** on the **SupportSave** dialog box.
7. Click **OK** on the message.

   A progress message displays with a list of the steps to be performed:

   - Capturing logs and server data
   - Capturing partial/full database
   - Capturing data from the products

   You cannot close the progress message and you cannot perform any other actions until the SupportSave is complete.

   The application generates separate master logs to show the status of the Server Support save collection.

Capturing Client support save data

To capture client support save files, complete the following steps.

1. Select **Monitor > Technical Support > SupportSave**.

   The **SupportSave** dialog box displays.

2. Select the **Client SupportSave** check box to run supportsave on the client.
3. Make sure the **Server SupportSave** check box is clear.
4. Enter a file name for the client support save file in the **File Name** field.

   The default file name is DCM-Client-SS-*Time_Stamp*.

5. Click **OK** on the **SupportSave** dialog box.
6. Click **OK** on the message.

   A progress message displays with a the step to be performed: Capturing client support save.

   You cannot close the progress message and you cannot perform any other actions until the SupportSave is complete.

   The application generates separate master logs to show the status of the Client Support save collection.

Client support save using a command line interface

Use the following procedures to capture client support save files through the command line interface (CLI).

Capturing client support save using the CLI (Windows)

To capture client support save files through the CLI, complete the following steps.

1. Go to the following location:
   - (Local client) *User_Home/Management_Application_Name/*localhost
   - (Remote client) *User_Home/Management_Application_Name/*Server IP
2. Run the clientsupportsave.bat file.
3. Define a capture location by typing `clientsupportsave` <*path*> in the CLI. If the path has spaces, enclose it in double quotes.

   By default, the capture location is one of the following:
   - (Local client) *User_Home/Management_Application_Name/*localhost
   - (Remote client) *User_Home/Management_Application_Name/*Server IP
4. Use an archive tool to create a ZIP file of the support save.

Capture client support save using the CLI (Linux)

To capture client support save files through the CLI, complete the following steps.

1. Go to /root */Management_Application_Name_Folder/*Server IP.
2. Run the clientsupportsave.sh file.
3. Define a capture location by typing `sh clientsupportsave` <*path*> in the CLI. If the path has spaces, enclose it in double quotes.

   By default, the capture location is /root */Management_Application_Name_Folder/*Server IP/support.
4. Use an archive tool to create a ZIP file of the support save.

Device technical support

You can use Technical Support to collect SupportSave data (such as, RASLOG, TRACE and so on) and switch events from Fabric OS, IronWare, and Network OS devices.

To gather technical support information for the Management application server, refer to "Capturing technical support information" on page 392.

Scheduling technical support information collection

You can capture technical support and event information for up to 50 devices. Technical SupportSave uses the built-in FTP, SCP, or SFTP server configured on the Management server to save data. To make sure the built-in FTP, SCP, or SFTP server is configured correctly, refer to"Configuring an external FTP, SCP, or SFTP server" on page 175.

NOTE
Network OS switches must be running Network OS 2.1.X or later to collect technical support data.

NOTE
The Host must be a managed Brocade HBA.

NOTE
Scheduling technical support data collection is not supported on ESXi Servers.

NOTE
You must have the SupportSave privilege to perform this task. For more information about privileges, refer to "User Privileges" on page 1283.

To capture technical support and event information, complete the following steps.

1. Select **Monitor > Technical Support > Product/Host SupportSave**.

   The **Technical SupportSave** dialog box displays.

2. Click the **Schedule** tab.

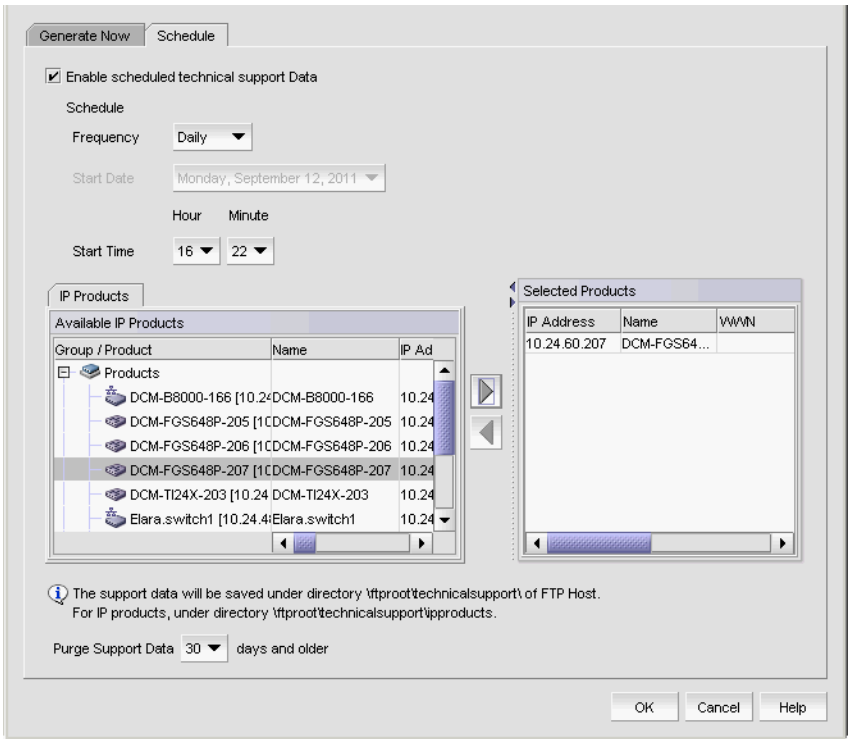


FIGURE 507 Technical SupportSave dialog box, Schedule tab

3. Select the **Enable scheduled Technical Support Data** check box.
4. Select how often you want the scheduled collection to occur from the **Frequency** list.
5. Select the start date for the scheduled collection from the **Start Date** list.

   This list is only available when you select Weekly or Monthly from the **Frequency** list.
6. Select the time you want the scheduled collection to begin from the **Start Time Hour** and **Minute** lists.
7. Click the **IP Products** tab, if necessary, and complete the following steps.

   The **Available IP Products** table displays the following information:

   - **Group/Product** — All discovered devices and ports as both text and icons.
   - **Name** — The name of the available product.
   - **IP Address** — The switch port's IP address.
   - **Product Type** — The type of product.
   - **Serial #** — The serial number of the device.
   - **Status** — The operational status of the switch, for example, unknown or marginal.
   - **Vendor** — The hardware vendor's name.
   - **Model** — The name and model number of the hardware.
   - **Port Count** — The total number of ports.
   - **Firmware** — The firmware version.
   - **Build Label** — The build version.
   - **Location** — The customer site location.

- **Contact** — The primary contact at the customer site.
- **Description** — A description of the customer site.
- **Role** — A description of the customer site.

a. Right-click in the **Available IP Products** table and select **Expand All**.

b. Select the products you want to collect data for in the **Available IP Products** table and click the right arrow to move them to the **Selected Products and Hosts** table.

NOTE
For a VCS fabric, SupportSave data is collected for the nodes in the fabric when you create the schedule. Nodes removed from the fabric at a later date will still be included. Nodes added to the fabric at a later date will be ignored.

Technical SupportSave data for IronWare and Fabric OS DCB products is saved to the following directory: *Install_Home*\data\ftproot\technicalsupport\ipproducts

Technical SupportSave uses the following naming convention for the IronWare device support save files: IPProd-*Device_Display_Name-IP_Address-Time_Stamp*.

Technical SupportSave uses the following naming convention for the Fabric OS DCB device support save files from the IP tab: IPProd-DCB-*Time_Stamp*.

If you select more than one IronWare device for collection, the IronWare device support save files are saved as individual zip files. However, if you select more than one Fabric OS DCB device for collection, the DCB device support save files are bundled together in a zip file.

Technical SupportSave data for Network OS products in either standalone or VCS mode are saved to the following directory:
Install_Home\data\ftproot\technicalsupport\ipproducts\NOS

Technical SupportSave uses the following naming convention for the VCS-enabled Network OS device support save files:
IPProd-*Fabric_Name-Seed_Switch_IP-Time_Stamp*\IPProd-*Fabric_Name-Product_Name-Product_IP-Time_Stamp*

A consolidated fabric zip file is created only in the when the Management application is configure with an internal FTP server.

Technical SupportSave uses the following naming conventions for the standalone Network OS device support save files:
IPProd-*Device_Display_Name-IP_Address-Time_Stamp*.

If you select more than one standalone Network OS device for SupportSave collection, the device support save files are saved as individual zip files.

If you select VCS-enabled or Standalone Network OS devices for support save collection using External FTP or SCP servers, the directory structure is the same as above; however, the files are not zipped in the External FTP or SCP location.

8. Click the **Hosts** tab and complete the following steps.

The Available Hosts table displays the following information:

- **Name** — The name of the available host.
- **IP Address** — The host port's IP address.
- **Network Address** — The network address of the host.

- **Fabrics** — The fabric of the host.

a. Right-click in the **Available Hosts** table and select **Expand All**.

b. Select the products you want to collect data for in the **Available Hosts** table and click the right arrow to move them to the **Selected Products and Hosts** table.

The **Selected Products and Hosts** table displays the following information:

- **IP Address** — The IP address of the selected product or host. For VCS-enabled product's, the IP address of the selected node.
- **Name** — The name of the selected product or host. For VCS-enabled product's, the *Principal_Switch_Name-Product_Name* of the selected node.
- **WWN** — The world wide name of the selected product or host. For VCS-enabled product's, the world wide name of the selected node.
- **Firmware Type** — The type of firmware: IOS (IronWare)or NOS (Network OS).
- **Firmware version** — The firmware version of the selected product or host. For VCS-enabled product's, the firmware version of the selected node.
- **Support Save Credentials** — Whether the product or host has supportSave credentials or not.

Technical SupportSave data for IP products is saved to the following directory: *FTP_Host*\ftproot\technicalsupport\ipproducts

9. Select how often you want to purge the support data from the **Purge Support Data** list.
10. Click **OK** on the **Technical SupportSave** dialog box.
11. Click **OK** on the confirmation message.

Data collection may take 20-30 minutes for each selected switch. This estimate may increase depending on the number of switches selected. Check the Master Log for status information.

NOTE
Unreachable switches increase the time needed to collect supportSave data.

Starting immediate technical support information collection

Technical SupportSave uses the built-in FTP, SCP, or SFTP server configured on the Management server to save data. To make sure the built-in FTP, SCP, or SFTP server is configured correctly, refer to"Configuring an external FTP, SCP, or SFTP server" on page 175.

NOTE
Fabric OS switches must be running Fabric OS 5.2.X or later to collect technical support data.

NOTE
Network OS switches must be running Network OS 2.1.X or later to collect technical support data.

NOTE
The HBA must be a managed Brocade HBA.

NOTE
You must have the SupportSave privilege to perform this task. For more information about privileges, refer to "User Privileges" on page 1283.

To capture technical support and event information for specified devices, complete the following steps.

1. Select **Monitor > Technical Support > Product/Host SupportSave**.

   The **Technical SupportSave** dialog box displays.

2. Click the **Generate Now** tab, if necessary.

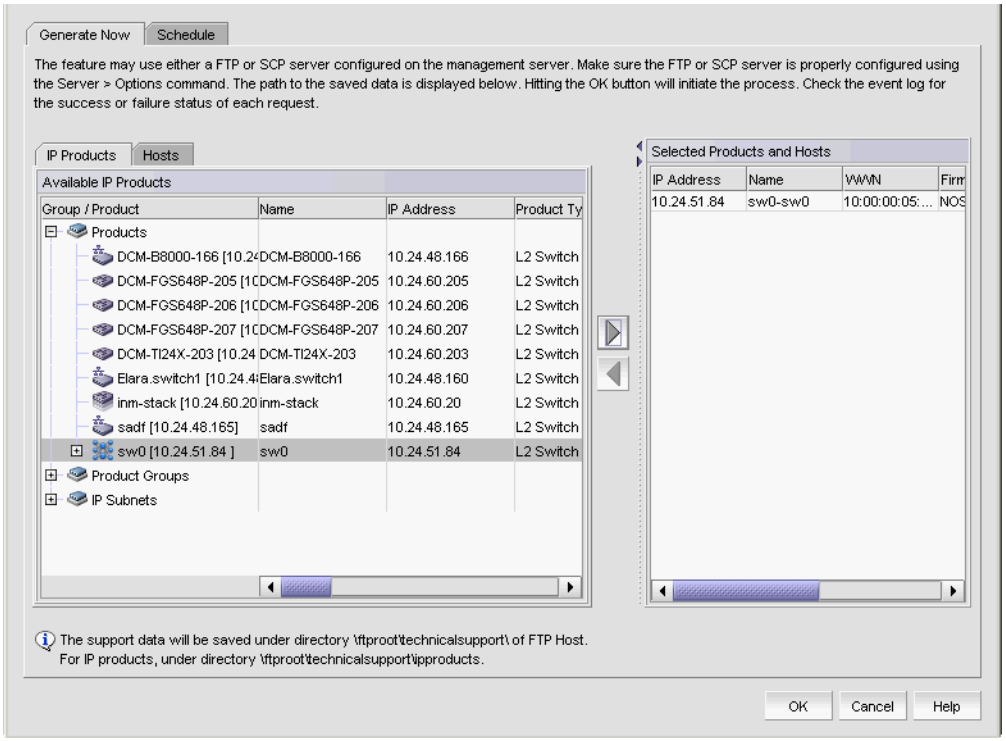


FIGURE 508 Technical SupportSave dialog box, Generate Now tab

3. Click the **IP Products** tab, if necessary, and complete the following steps.

   a. Right-click in the **Available IP Products** table and select **Expand All**.

   b. Select the products you want to collect data for in the **Available IP Products** table and click the right arrow to move them to the **Selected Products and Hosts** table.

      Technical SupportSave data for IronWare and Fabric OS DCB products is saved to the following directory: *Install_Home*\data\ftproot\technicalsupport\ipproducts

      Technical SupportSave uses the following naming convention for the IronWare device support save files: IPProd-*Device_Display_Name-IP_Address-Time_Stamp*.

      Technical SupportSave uses the following naming convention for the Fabric OS DCB device support save files from the IP tab: IPProd-DCB-*Time_Stamp*.

      If you select more than one IronWare device for collection, the IronWare device support save files are saved as individual zip files. However, if you select more than one Fabric OS DCB device for collection, the DCB device support save files are bundled together in a zip file.

Technical SupportSave data for Network OS products in either standalone or VCS mode are saved to the following directory:
Install_Home\data\ftproot\technicalsupport\ipproducts\NOS

Technical SupportSave uses the following naming convention for the VCS-enabled Network OS device support save files:
IPProd-*Fabric_Name-Seed_Switch_IP-Time_Stamp*\IPProd-*Fabric_Name-Product_Name-Product_IP-Time_Stamp*

A consolidated fabric zip file is created only in the when the Management application is configure with an internal FTP server.

Technical SupportSave uses the following naming conventions for the standalone Network OS device support save files:
IPProd-*Device_Display_Name-IP_Address-Time_Stamp*.

If you select more than one standalone Network OS device for SupportSave collection, the device support save files are saved as individual zip files.

If you select VCS-enabled or Standalone Network OS devices for support save collection using External FTP or SCP servers, the directory structure is the same as above; however, the files are not zipped in the External FTP or SCP location.

4. Click the **Hosts** tab, if necessary, and complete the following steps.
   a. Right-click in the **Available Hosts** table and select **Expand All**.
   b. Select the hosts you want to collect data for in the **Available Hosts**table and click the right arrow to move them to the **Selected Products and Hosts** table.

      Technical SupportSave data for IP products is saved to the following directory:
      FTP_Host\ftproot\technicalsupport\ipproducts
5. Click **OK** on the **Technical SupportSave** dialog box.

   Data collection may take 20-30 minutes for each selected switch. This estimate my increase depending on the number of switches selected.

   The **Technical SupportSave Status** dialog box displays with the following details.

Field	Description
Name	The name of the product. For VCS-enabled product's, the *Principla_Switch_Name-Product_Name* of the selected node.
IP Address	The product's IP address. For VCS-enabled product's, the IP address of the selected node.
Firmware Type	The type of product.
Progress	The status of the supportsave. On products running Fabric OS 7.0 or later, this field shows the percentage complete and is updated every minute. For IronWareand Host products, as well as Fabric OS products running 6.4 or earlier, this field cannot display the percentatge (only displays whether it is 'in Progress' or' Completed').
Status	The status of the support save, for example, Ceases or Failure.

6. Click **Close** on the **Technical SupportSave Status** dialog box.

Viewing the technical support repository

You can only view technical support save files that are captured in the default location. Table 99 details the default locations for the technical support save files.

TABLE 99 Technical support save defaults

Type	Default location	Default naming convention
Client SupportSave	*User_Home*/ServerIP/Managed Product Name/support	DCM-Client-SS-*Time_Stamp*
Server SupportSave	*Install_Home*\support	DCM-SS-*Time_Stamp*
Host (discovered from the IP tab)	*Install_Home*\data\ftproot\technicalsupport\host	IPProd-DCB-*Time_Stamp*
IronWare Product	*Install_Home*\data\ftproot\technicalsupport\ipproducts	IPProd-*Device_Display_Name-IP_Address-Time_Stamp*
Auto Trace Dump	*Install_Home*\data\ftproot\tracedump\	
Standalone Network OS devices	*Install_Home*\data\ftproot\technicalsupport\ipproducts\NOS	IPProd-*Device_Display_Name-IP_Address*-Time_Stamp
VCS-enabled Network OS devices	*Install_Home*\data\ftproot\technicalsupport\ipproducts\NOS	IPProd-*Fabric_Name-Seed_Switch_IP-Time_Stamp*\IPProd-*Fabric_Name-Product_Name-Product_IP-Time_Stamp*

To view the technical support repository, complete the following steps.

1. Select **Monitor > Technical Support > View Repository**.

   The **Technical Support Repository** dialog box displays.

2. Review the techncial support repository details:

Field/Component	Description
Available SupportSave table	Select the support data file you want to view. Displays the following information: **File Name** — The name of the SupportSave file. **Size (MB)** — The name of the SupportSave file. **Last Modified** — The date the SupportSave file was generated. **Firmware Type** — The type of file (Client, Server, FOS (Fabric OS), IOS (IronWare), NOS (Network OS),). Blank for Host support save files.
E-mail button	Click to e-mail the support data file. For the procedure, refer to "E-mailing technical support information" on page 1227.
FTP button	Click to copy the support data file to an external FTP server. For the procedure, refer to "Copying technical support information to an external FTP server" on page 1227.
Save button	Click to save a copy of the support data. For the procedure, refer to "Saving technical support information to another location" on page 1226.
Delete button	Click to delete the support data file. For the procedure, refer to "Deleting technical support files from the repository" on page 1228.

3. Click **OK** on the **Technical Support Repository** dialog box.

Saving technical support information to another location

To save technical support information to a location other than the default, complete the following steps.

1. Select **Monitor > Technical Support > View Repository**.

   The **Technical Support Repository** dialog box displays.

2. Select a device support save file and click **Save.**

   The **Save** dialog box displays.

3. Browse to the location where you want to save the support file.
4. Click **Save** on the **Save** dialog box.
5. Click **OK** on the message.
6. Click **OK** on the **Technical Support Repository** dialog box.

E-mailing technical support information

NOTE
You cannot e-mail technical support information collected from the remote client.

To e-mail technical support information, complete the following steps.

1. Select **Monitor > Technical Support > View Repository**.

   The **Technical Support Repository** dialog box displays.

2. Select the file you want to e-mail in the table.
3. Click **E-mail** to e-mail the event and supportsave files (zip).

   NOTE
   The **E-mail** button is unavailable from the remote client.

   You must configure the Management application e-mail server before you can define the e-mail action. For more information, refer to .

   The **E-mail** dialog box displays.

4. Enter the e-mail address of the person to receive the e-mail in the **To** field.
5. Enter your e-mail address in the **From** field.
6. Click **OK**.

   The e-mail is sent and the **Technical Support Repository** dialog box closes automatically.

Copying technical support information to an external FTP server

NOTE
You cannot copy technical support information to an external FTP server collected from the remote client.

To copy the SupportSave data located in the built-in FTP server to an external FTP server, complete the following steps.

1. Select **Monitor > Technical Support > View Repository**.

   The **Technical Support Repository** dialog box displays.

2. Select the file you want to copy in the table.
3. Click **FTP** to send the switch event and supportsave files (zip) by FTP.

   NOTE
   The **FTP** button is unavailable from the remote client.

   The **FTP Credentials** dialog box displays.

4. Enter the network address or domain name of the external FTP server in the **Network Address** field.
5. Enter your user name and password.

6. Enter the destination directory where you want to copy the data on the external FTP server in the **Destination Directory** field.

   The destination directory should be the sub directory of the external FTP server's root directory. For example, if you enter "repository" as the destination directory, then the support save file is copied to the "/repository" directory of the external FTP server.

7. Click **OK**.

   The data is copied and the **Technical Support Repository** dialog box closes automatically.

Deleting technical support files from the repository

To delete a technical support file from the repository, complete the following steps.

1. Select **Monitor > Technical Support > View Repository**.

   The **Technical Support Repository** dialog box displays.

2. Select the file you want to delete in the table.
3. Click **Delete**.
4. Click **OK** on the **Technical Support Repository** dialog box.

5.

Chapter

40

Reports

In this chapter

Reports overview

Reports are available from the **Reports** menu. You must have the Reports privilege to access the reports. For more information about privileges, refer to "“User Privileges” on page 1283.

Browser requirements

IP reports display in a web browser. Reports are supported in the following browsers:

- Windows Internet Explorer 9 or 10 on Windows
- Firefox 19 on Windows or Linux
- Google Chrome

Viewing IP reports

Reports are available from the **Reports** menu. You must have the Reports privilege to access the reports. For more information about privileges, refer to “User Privileges” on page 1283.

- Click the **Reports** button on the menu bar to display the report options.
- Click a report option to display the report that you want.

NOTE
ATM ports are not displayed in the reports. The ATM module may appear in the reports, but the modules will be listed as having no ports.

Exporting and saving IP reports to a file

You can save a report to a CSV (comma seperated values) or HTML file. Each report has an **Export** list at the top right corner of the page.

1. Select one of the following from the **Export** list:
   - Select **Export as HTML**.
   - Select **Export as CSV**.
2. Browse to the location where you want to save the file and click **Save**.

Exporting IP reports to e-mail recipients

You can e-mail a report in a CSV or HTML file format. To export reports to an e-mail recipient, you must configure e-mail event notification (refer to "Configuring e-mail notification" on page 1142).

If you want to export the report to an e-mail recipient, complete the following steps.

1. Select one of the following from the **E-mail** list:
   - Select **E-mail as HTML**.
   - Select **E-mail as CSV**.

   The **Report via E-mail** dialog box displays (Figure 509).

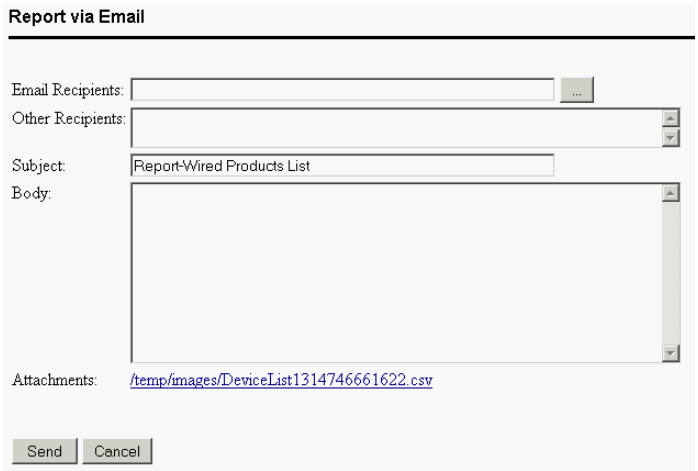


FIGURE 509 Report via E-Mail dialog box

2. Click the ellipsis button next to the **E-mail Recipients** field.

The **Users** dialog box displays.

3. Select the preconfigured e-mail user account from the list and click **OK**.
4. Enter additional e-mail addresses in the **Other Recipients** field.
5. Enter text in the **Subject** field to change the subject of the e-mail.
6. Enter text in the **Body** field to send a message with the report.
7. Click **Send** to send the report.

NOTE
Mozilla Firefox Browser does not support the window close script.
Click the browser close button (X) to cancel.

IP report contents

Each report contains the following information:

- The name of the report displays at the top of the report.
- Data is presented in a tabular format.
- The **Export** and **E-mail** buttons in the top right corner of the report allows you to save the report to a file or e-mail the report. You can use an application that supports comma-separated values (CSV) or HTML to view the saved file.

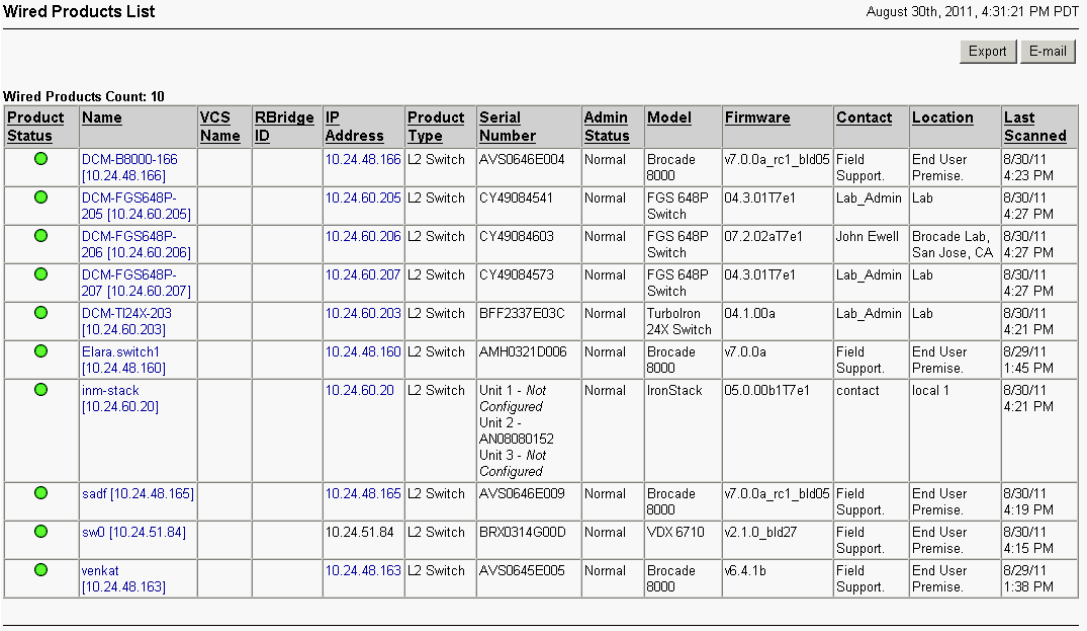
IP Wired Products report

The Wired Products report displays general and detailed configuration information about wired products that are under the management server.

The information on the report comes from the software image version that is in the management application for that product. To ensure that the latest configuration information is in the management application, run the discovery process or resynchronize the product.

To view the **Wired Products List**, select **Reports > Wired Products** from the main menu.

The **Wired Products List** displays (Figure 510).



Wired Products List — August 30th, 2011, 4:31:21 PM PDT

Export | E-mail

Wired Products Count: 10

Product Status	Name	VCS Name	RBridge ID	IP Address	Product Type	Serial Number	Admin Status	Model	Firmware	Contact	Location	Last Scanned
	DCM-B8000-166 [10.24.48.166]			10.24.48.166	L2 Switch	AVS0646E004	Normal	Brocade 8000	v7.0.0a_rc1_bld05	Field Support.	End User Premise.	8/30/11 4:23 PM
	DCM-FGS648P-205 [10.24.60.205]			10.24.60.205	L2 Switch	CY49084541	Normal	FGS 648P Switch	04.3.01T7e1	Lab_Admin	Lab	8/30/11 4:27 PM
	DCM-FGS648P-206 [10.24.60.206]			10.24.60.206	L2 Switch	CY49084603	Normal	FGS 648P Switch	07.2.02aT7e1	John Ewell	Brocade Lab, San Jose, CA	8/30/11 4:27 PM
	DCM-FGS648P-207 [10.24.60.207]			10.24.60.207	L2 Switch	CY49084573	Normal	FGS 648P Switch	04.3.01T7e1	Lab_Admin	Lab	8/30/11 4:27 PM
	DCM-TI24X-203 [10.24.60.203]			10.24.60.203	L2 Switch	BFF2337E03C	Normal	TurboIron 24X Switch	04.1.00a	Lab_Admin	Lab	8/30/11 4:21 PM
	Elara.switch1 [10.24.48.160]			10.24.48.160	L2 Switch	AMH0321D006	Normal	Brocade 8000	v7.0.0a	Field Support.	End User Premise.	8/29/11 1:45 PM
	inm-stack [10.24.60.20]			10.24.60.20	L2 Switch	Unit 1 - *Not Configured* Unit 2 - AN08080152 Unit 3 - *Not Configured*	Normal	IronStack	05.0.00b1T7e1	contact	local 1	8/30/11 4:21 PM
	sadf [10.24.48.165]			10.24.48.165	L2 Switch	AVS0646E009	Normal	Brocade 8000	v7.0.0a_rc1_bld05	Field Support.	End User Premise.	8/30/11 4:19 PM
	sw0 [10.24.51.84]			10.24.51.84	L2 Switch	BRX0314G00D	Normal	VDX 6710	v2.1.0_bld27	Field Support.	End User Premise.	8/30/11 4:15 PM
	venkat [10.24.48.163]			10.24.48.163	L2 Switch	AVS0645E005	Normal	Brocade 8000	v6.4.1b	Field Support.	End User Premise.	8/29/11 1:38 PM

FIGURE 510 Wired Product List

The Wired Products report contains the fields and components detailed in Table 100.

TABLE 100 Wired Products report fields and components

Field/Component	Description
Wired Products Count	The number of wired products in the report.
Product Status	Whether the product is reachable (green icon), marginal ( ), degraded link ( ), down ( ), unhealthy ( ), or not reachable ( ).
Name	The name of the product. Click the name of a product to launch the **Detailed Product Report**.
VCS Name	The name of the VCS product. Click the name of a product to launch the **Detailed Cluster Report**.
RBridge ID	The RBridge ID of the VCS product.
IP Address	The IP address of the product. Click the IP address of a product to launch the Web Element Manager. This is not supported on VDX devices.
Product Type	The type of product.
Serial Number	The serial number of the product.
Admin Status	The administrative status of the product. Possible status includes: • Normal — The product is in normal operating mode. • Troubleshooting — The product is in troubleshooting mode.
Model	The model of the product.
Firmware	The firmware level of the product.
Contact	The contact name for the product.
Location	The location of the product.
Last Scanned	The date and time, including time zone, the product was scanned last.

TABLE 100 Wired Products report fields and components (Continued)

Field/Component	Description
Export button	Click to export the report. For more information, refer to "Exporting and saving IP reports to a file" on page 1232.
E-mail button	Click to e-mail the report. For more information, refer to "Exporting IP reports to e-mail recipients" on page 1232.

Detailed Product Report

To view the details of a Wired Products report, click the name of a wired product in the Wired Products report. To launch the Detailed Product Report from the topology, right-click the product on the Network Objects, L2 Topology, Ethernet Fabrics, IP Topology, or VLAN Topology view and select **Detailed Report**.

NOTE
This report is not available for VCS clusters.

The Detailed Product Report displays (Table 101).

TABLE 101 Detailed Product Report fields and components

Field/Component	Description
System Information	System information includes the following: • **Alias Name** — An optional name that is entered using the **Properties** dialog box. It provides an alternate name for the product if you want to override the **Host Name** and **System Name** values. • **Host Name** — The name that the Management application obtains from the product during discovery. This may be the Domain Name System (DNS) name of the product, but may come from other naming services, depending on the configuration of the operating system on which the Management application is running. • **System Name** — The name the Management application retrieves from the "sysName" SNMP MIB variable during discovery. This name corresponds to the value specified by the **hostname** command in the product configuration file. The Management application displays the first name it finds for the product in the following order: Alias Name, Host Name, System Name. The Alias Name takes precedence over Host Name, which takes precedence over System Name, and so on. • **Contact** — A contact name for the product. • **Location** — The location of the product. • **Serial Number** — The serial number of the product. A serial number is not displayed for products that support stacking. Serial numbers for these products are displayed under the **Stacking Units** table. • **Description** — A description of the product.
Stacking Units	This section only displays if the product is configured as a stacked device. It includes the following: • **Unit** — The ID of the unit on the stack. • **Present** — Whether the stacked device is physically present. • **Role** — The role of the unit. • **Model** — The model number of the stacked device. • **Firmware** — The firmware level of the stacked device. • **Priority** — The priority bit of the stacked device. • **Description** — A description of the stacked device.

TABLE 101 Detailed Product Report fields and components (Continued)

Stacking Port - Realtime	The name of the stacked device with drill-down support. When you click on the name, the "IP Stacking Ports - Realtime report" launches (refer to "IP Stacking Ports - Realtime report" on page 1244).
Admin Status	Admin status information includes the following: • **Status** — Whether the product is in normal operating mode or troubleshooting mode. • **Status Last Updated** — When the last status update occurred. • **Memo** — A memo for the product. • **Memo Last Updated** — When the last memo update occurred.
Modules	Module information shows what modules are installed on the product. • **Unit/Slot Number** — For products that support stacking, you can view the unit number and slot number. **Slot Number** — For products that do not support stacking, you can view the slot number. • **Type** — For wireless products, the type shows the model name of the product. For wired products, the type of module installed in the slot. • **Serial Number** — The serial number of the module. For wired products, the serial number cell may be blank. • **Ports** — The number of ports on the product. The number of ports for ATM modules displays as zero. • **Present** — Whether the module is still installed on the product.
IP Addresses	The IP addresses of each interface, including the virtual routing interface on wired products. For Layer 2 switches, the management IP address displays in the IP Addresses table with "management" in the Interface column. • **Port** — The port number. • **IP Address** — The IP address. • **Subnet Mask** — The subnet mask number. • **VRF** — The virtual routing interface.
Ethernet Ports	Physical port information for each port on the product. The identifier, interface name, type, speed, physical address (displays as 0000.0000.0000 for module interfaces), name, VLAN tag mode (tagged, untagged, dual, or blank), and duplex mode of the physical interfaces on the product. • **Identifier** — The port identifier. • **Port Name** — The port name. • **Type** — The type of port. • **Speed (Mbps)** — The speed of the port. • **MAC Address** — The MAC address of the port. • **Name** — The name of the port. • **Tag Mode** — The tag mode of the port. • **Duplex Mode** — The duplex mode of the port. • MCT Client Name — The client name of the MCT switch. • Role — The role of the port, such as ICL or MCT.

TABLE 101 Detailed Product Report fields and components (Continued)

Cluster (MCT switches only)	Cluster information for a Multi-Chassis Trunk (MCT) switch. Information includes: • **Cluster ID** — The MCT cluster ID. • **Cluster Name** — The MCT cluster name. • **Cluster State** — Whether the MCT cluster is deployed or undeployed. • **Client Isolation Mode** — Whether isolation mode is loose or strict. • **Active Member VLAN Range** — The active member VLAN for data. • **Configured Member VLAN Range** — The configured member VLAN for data. • **Keep Alive VLAN** — An alternate VLAN for Cluster Communication Protocol (CCP) when the Inter-Chassis Link (ICL) is down. • **Session VLAN** — The VLAN used by the cluster for control operations. • **ICL Name** — The ICL name.
Cluster Peer (MCT switches only)	Cluster peer information for a Multi-Chassis Trunk (MCT) switch. Information includes: • **Peer Product** — The name and IP address of the MCT peer product. • **Peer IP Address** — The VE interface IP address of the MCT peer. • **Peer RBridge ID** — The RBridge ID of the MCT peer. • **ICL Name** — The name of the ICL used to reach the MCT peer. • **Keep Alive Interval** — The interval time for CCP over the keep-alive VLAN. • **Hold Time** — The hold-time before making the CCP down state when ICL goes down. • **Fast Failover** — Whether fast failover is enabled or disabled. • **Active VLAN Range** — The active member VLAN for data. • **Peer State** — Whether the peer state is CCP up or CCP down. • **Peer State Up Time** — How long the peer has been up. • **Peer State Down Reason** — The reason the peer is down.
Physical Ports - Realtime	The name of the device with drill-down support. When you click on the name, the "IP Physical Ports - Realtime report" launches (refer to "IP Physical Ports - Realtime report" on page 1244).
GRE Tunnels	Information on any GRE tunnel on the product. Information includes the following: • **Identifier** — The GRE tunnel identifier. • **Name** — The name of the GRE tunnel.
Controller Cluster	Cluster information for a wireless controller. Information includes: • **Cluster Name —** The cluster name. • **Cluster Mode —** The cluster mode. Options include Active and Standby. • **Cluster members** — The IP address of the controllers in cluster mode.
Virtual Interfaces	Information on any virtual interface on the product.
Loopback Interfaces	Information on any loopback interface on the product.
Chassis Inventory	Information for fans, power supplies, sensors, and other chassis components on third-party products. Information is displayed for a third-party product if the product supports the ENTITY MIB. • **Type** — The chassis model. • **Name** — The name of the chassis. • **Description** — A description of the product. • **Serial Number** — The serial number of the product.
Software Licenses	The name of the software licenses assigned to the product. • **Package Name** — The name of the license. • **License Id** — The license on the product. • **License Type** — The type of license (trial or normal). • **Expiry Date** — Whether the license is expired or unlimited. • **Precedence** — The precedence of the license. • **Status** — The status of the license (expired or active).

TABLE 101 Detailed Product Report fields and components (Continued)

AP List Count	Access Point information for wireless controllers. The table title includes the number of access points attached to the selected device. Information includes:
	• **Product Status** — Whether the AP is online (green icon), offline (red icon), or pending adoption (gray icon).
	• **Name** — The device name used to identify AP.
	• **Connected Switch** — IP address of the controller or switch connected to the AP. Also displays the port number if the AP is directly connected.
	• **Controller** — IP address of the controller which manages the AP. Also displays the port number if the AP is directly connected.
	• **Cluster Name** — The controller cluster name. Click to view the controller cluster details.
	• **Controller —** Cluster information for a wireless controller. Information includes:
	  • **Cluster Name —** The cluster name.
	  • **Cluster Mode —** The cluster mode of the AP. Options include Active and Standby.
	  • **Cluster members** — The IP address of the controllers in cluster mode.
	• **MAC Address** — The AP device MAC address.
	• **Model** — The model of the AP.
	• **Profile Name** — The AP profile name.
	• **RF Domain Name** — The RF domain name set for the AP.
	• **Serial Number** — The serial number of the AP.
	• **Firmware** — The firmware level of the AP.
	• **Client count** — The number of wireless clients or stations connected or associated to the AP.
	• **Last scanned** — The last time the APs were scanned.

Detailed Cluster Report

NOTE
This report is only available for VCS clusters.

To launch the Detailed Cluster Report from the topology, right-click the VCS cluster on the Network Objects, L2 Topology, Ethernet Fabrics, IP Topology, or VLAN Topology view and select **Detailed Report**.

The Detailed Cluster Report displays (Table 102).

TABLE 102 Detailed Cluster Report fields and components

Field/Component	Description

TABLE 102 Detailed Cluster Report fields and components (Continued)

System Information	System information includes the following: • **Alias Name** — An optional name that is entered using the **Properties** dialog box. It provides an alternate name for the product if you want to override the **Host Name** and **System Name** values. • **Host Name** — The name that the Management application obtains from the product during discovery. This may be the Domain Name System (DNS) name of the product, but may come from other naming services, depending on the configuration of the operating system on which the Management application is running. • **System Name** — The name the Management application retrieves from the "sysName" SNMP MIB variable during discovery. This name corresponds to the value specified by the **hostname** command in the product configuration file. The Management application displays the first name it finds for the product in the following order: Alias Name, Host Name, System Name. The Alias Name takes precedence over Host Name, which takes precedence over System Name, and so on. • **Config Mode** — The configuration mode. • **Node Count** — The number of nodes in the fabric. • **Status** — The status of the product. • **Contact** — A contact name for the product. • **Location** — The location of the product. • **Description** — A description of the product
Nodes	Node information includes the following: • **Name** — The name of the node. Click the name of a product to launch the Detailed Product Report. • **IP Address** — The IP address of the product. • **Product Type** — The type of product. • **Serial Number** — The serial number of the product. • **RBridge ID** — The RBridge ID number of the product. • **Status** — The status of the product. • **Model** — The model of the product. • **Firmware** — The firmware level of the product. • **Fabric Ports** — The number of fabric ports on the product. • **Edge Ports** — The number of edge ports on the product.
Admin Status	Admin status information includes the following: • **Name** — The name of the product. Click the name of a product to launch the Detailed Product Report. • **Status** — Whether the product is in normal operating mode or troubleshooting mode. • **Status Last Updated** — When the last status update occurred. • **Memo** — A memo for the product. • **Memo Last Updated** — When the last memo update occurred.
Modules	Module information shows what modules are installed on the product. • **Unit/Slot Number** — For products that support stacking, you can view the unit number and slot number. **Slot** — For products that do not support stacking, you can view the slot number. • **Type** — For wireless products, the type shows the model name of the product. For wired products, the type of module installed in the slot. • **Serial Number** — The serial number of the module. For wired products, the serial number cell may be blank. • **Ports** — The number of ports on the product. The number of ports for ATM modules displays as zero. • **Present** — Whether the module is still installed on the product.

TABLE 102 Detailed Cluster Report fields and components (Continued)

IP Addresses	The IP addresses of each interface, including the virtual routing interface on wired products. For Layer 2 switches, the management IP address displays in the IP Addresses table with "management" in the Interface column. • **Port** — The port number. • **IP Address** — The IP address. • **Subnet Mask** — The subnet mask number. • **VRF** — The virtual routing interface.
Ethernet Ports	This table contains the following information for each Ethernet interface on the product: • **Identifier** — The port identifier. • **Port Name** — The port name. • **Name** — The name of the port. • **MAC Address** — The MAC address of the port. • **Type** — The type of port. • **Speed (Mbps)** — The speed of the port. • **Duplex Mode** — The duplex mode of the port. • **Tag Mode** — The tag mode of the port. • **Role** — The role (edge or fabric) of the port. • **Profile Mode** — Whether profile mode is enabled or disabled. • **Active Profile** — The active profile of the port. • **Attached MAC** — The MAC address of a device attached to the port.
FC Ports	This table contains the following information for each FC interface on the product: • **Identifier** — The port identifier. • **Port Name** — The port name. • **Port WWN** — The world wide name of the port. • **Area ID/Port Index** — The area identifier and port index of the port. • **Type** — The type of port. • **Port Speed (Gb/s)** — The speed of the port. • **Trunked** — Whether the port is trunked. • **Trunk Index** — The trunk index of the port.
Physical Ports - Realtime	The name of the device with drill-down support. When you click on the name, the "IP Physical Ports - Realtime report" launches (refer to "IP Physical Ports - Realtime report" on page 1244).
Physical Media - Realtime	The name of the device with drill-down support. When you click on the name, the "IP Physical Media - Realtime report" launches (refer to "IP Physical Media - Realtime report" on page 1245).
Software Licenses	The name of the software licenses assigned to the product. • **Name** — The name of the node. • **Licensed Feature** — The licensed feature on the node. • **License Key** — The license key for the feature (displays as asterisks).

IP Module report

The Module List report presents the modules installed in discovered IronWare or third-party products and in which products they are installed.

The Module List report has the parameters described in Table 103.

TABLE 103 Module List report fields and components

Field/Component	Description
Description	The type of module installed.
Serial Number	The serial number of the module.
Product	The host name of the product where the module is installed. This name can be set from the CLI. Click the name of the product to display the Detailed Product Report.
VCS Name	The name of the VCS fabric.
[Unit/]Slot No	The slot on the product where the module is installed. If the product supports stacking, the slot is shown in the [*unit#*/]*slot#* format.

You can sort the report by clicking on a column header. For example, if you want to sort the table by serial number, click the Serial Number column header.

IP Port VLANs report

A list of port VLANs configured on IronWare or third-party products is available in the Port VLANs report. Lists of protocol VLANs are available in the port VLAN structure. For IronWare and Network OS products, these reports reflect the VLAN information available in VLAN Manager.

To access the Port VLANs report, select **Reports > VLANs**.

To display information about a VLAN, click its ID. The Port VLANs report has the parameters described in Table 104.

TABLE 104 Port VLANs report fields and components

Field/Component	Description
Port VLAN Information	This section contains the Layer 3 VLANs list, which displays links to protocol VLANs associated with the port VLAN.
Ports in Port VLAN #:	This section shows the following information: • **Product** — The name of the products that have ports belonging to the VLAN. For VCS fabric members, displays the VCS IP address with the name of the products that have ports belonging to the VLAN. • **Interface** — The port number or slot number that belongs to the VLAN. • **Interface Name** — The name of the interface. • **Tag Mode** — Whether the port is tagged, untagged, dual, or blank. • **PVLAN Type** — The PVLAN type.

You can sort the report by clicking on a column header. For example, if you want to sort the table by tag mode, click the Tag Mode column header.

IP Layer 3 VLAN report

The Layer 3 VLAN report contains links to lists of protocol VLANs associated with a port VLAN. To view the list of protocol VLANs, click a link under the Layer 3 VLANs section of the Port VLANs report. The Layer 3 VLAN report displays.

If the report is empty, then there are no protocol VLANs that have been configured for the port VLAN. The Layer 3 VLAN report has the parameters described in Table 105.

TABLE 105 Layer 3 VLAN report fields and components

Field/Component	Description
Protocol VLANs in Port VLAN	This section lists the details of protocol VLANs configured under the port VLAN.
IP Subnet VLANs in Port VLAN #	Several sections on the report display the subnet VLANs that have been configured under the port VLAN.

If any protocol or subnet VLANs have been configured under the protocol VLAN, you can click the **Details** link for that VLAN to find out more information for that VLAN.

IP Subnet report

The IP Subnet report displays the list of IP subnets discovered on the network. To appear on this list, the subnet must contain at least one discovered product.
To view the IP Subnet report, select **Reports > IP Subnet Reports**. The IP Subnet report has the parameters described in Table 106.

TABLE 106 IP Subnet report fields and components

Field/Component	Description
IP Address	The list of IP subnets discovered on the network. These address are listed in numerical order.
Subnet Mask	The mask of the subnet.
Products	A link to a list of products in the subnet.

To determine which products belong to a subnet, click the **Products** link for that subnet. For example, clicking products for the IP subnet 112.112.112.0 displays the Product List by IP Subnet report. The Product List by IP Subnet report has the parameters described in Table 107.

TABLE 107 Product List by IP Subnet report fields and components

Field/Component	Description
Name	The name of the products that belong to the subnet. Click to launch the Detailed Product Report.
IP address	The IP address of the product. Click to launch the Web Element Manager. Web Element Manager is not supported on VDX devices.
Image Version	The version of the software image running on the product.
Product Type	The product type.
Contact	The name of the person to call about the product.
Location	The location of the product.
Last Scanned	The date and time, including time zone, the product was last scanned for the latest software image by discovery.

You can sort the report by clicking on a column header.

NOTE
You cannot access EdgeIron products from this report.

IP Address report

The IP Address report displays all discovered IP addresses of wired products on the network.

To view the IP Address report, select **Reports > IP Address Report**. The IP Address report has the parameters described in Table 108.

TABLE 108 IP Address report fields and components

Field/Component	Description
IP Address	The IP address of the product, access point, or interface. These addresses are in numerical order. Click to launch the Web Element Manager. Web Element Manager is not supported on VDX devices.
Subnet Mask	The subnet mask associated with the IP address.
Product	The host name of the product on which the IP address is configured. The name of the product has a hyperlink that displays detailed product information.
VCS Name	The name of the VCS fabric. Click to display the detailed fabric report.
Identifier	The port number or slot number and port number on which the IP address is configured.
Port Name	The port name.
MAC Address	The MAC address of the product, access point, or interface.

You can sort the report by clicking on a column header. For example, if you want to sort the table by subnet mask, click the Subnet Mask column header.

MAC Address report

The MAC Address report shows the MAC addresses of wired products that have been discovered on the network.

Display the report by selecting **Reports > MAC Addresses**. The MAC Address report has the parameters described in Table 109.

TABLE 109 MAC Address report fields and components

Field/Component	Description
MAC Address	The MAC address of the interface.
Product	The name of the product to which the MAC address belongs. The name of the product has a hyperlink that displays detailed product information.
VCS Name	The name of the VCS fabric. Click to display the detailed fabric report.
Port	The port number or slot number and port number to which the MAC address belongs.
Attached Device (MAC)	(FCoE devices only) The device name and MAC address for connected devices.

You can sort the report by clicking on a column header. For example, if you want to sort the table by port number, click the Port column header.

IP Physical Ports - Realtime report

The Physical Ports - Realtime report shows the status of physical interfaces of products that have been discovered on the network.

To display the report, choose one of the following options;

- Right-click the device in the **IP Products** dialog box and select **Physical Ports Report**.
- Right-click the device on the Network Objects, L2 Topology, Ethernet Fabrics, IP Topology, or VLAN Topology view and select **Physical Ports Report**.
- From the Detailed Product Report, click the device name in the **Physical Ports - Realtime** table.
- From the Detailed Fabric Report, click the device name in the **Physical Ports - Realtime** table.

The Physical Ports - Realtime report has the parameters described in Table 110.

TABLE 110 Physical Ports - Realtime report fields and components

Field/Component	Description
Identifier	A unique identifier for each port on the device. The identifier includes the module, slot, and interface.
Administrative Status	The administrative status of the port.
Operational Status	The operational status of the port.
PoE Control	Displays the PoE status of the port.

You can sort the report by clicking on a column header. For example, if you want to sort the table by administrative status, click the Administrative Status column header.

IP Stacking Ports - Realtime report

The Stacking Ports - Realtime report shows the stacking port and neighbor port details.

To display the report, from the Detailed Product Report, click the device name in the **Stacking Ports - Realtime** table.

The Stacking Ports - Realtime report has the parameters described in Table 111.

TABLE 111 Stacking Ports - Realtime report fields and components

Field/Component	Description
Stacking Port Connections	Identifies the connected ports to the neighbor port and the unused ports of the stacked units.

IP Physical Media - Realtime report

The Physical Media - Realtime report shows the port optics (SFP) details of Network OS devices.

To display the report, complete the following steps.

1. Right-click the device on the topology and select **Detailed Report.**
2. Click the device name in the **Physical Media - Realtime** table.

   The Physical Media - Realtime report has the parameters described in Table 112.

TABLE 112 Physical Media - Realtime report fields and components

Field/Component	Description
Identifier	A unique identifier for each port on the device. The identifier includes the module, slot, and interface.
Tx Power	The transmit power.
Rx Power	The receive power.
Transceiver Temp(C)	The temperature of the transceiver
Voltage (mVolts)	The voltage of the SFP.
Transceiver Current (mAmps)	The transceiver current.
Speed (MB/s)	The speed in megabits per second.
Distance	The distance of the SFP.
Vendor	The vendor of the SFP.
Vendor OUI	The vendor's Organizationally Unique Identifier from a MAC address.
Vendor PN	The vendor's part number.
Vendor REV	The vendor's REV.
Serial #	The serial number of the SFP.
Date Code	The date code of the SFP.
Media Form Factor	The media form factor of the SFP.
Connector	The connector type.
Wave Length (nm)	The wave length of the SFP.
Encoding	The transceiver encoding method of the SFP.

You can sort the report by clicking on a column header. For example, if you want to sort the table by the identifier, click the column header.

IP Deployment reports

Deployment reports provide information about deployments performed from the Management application. These deployments include device configuration deployments, software image backups, Realm Manager deployments, and configuration backups. The reports are available in case administrators want to know whether a deployment succeeded or failed.

Deployment reports are not available for third-party devices.

Viewing a deployment report

1. Select **Reports > Deployment**.

   The **Configurations** report displays in the web browser with the following details:

   - **User** list — Select one of the following options:
     - All — Select to see deployments for all users.
     - System User — Select to see deployments for the system user only.
     - Current User — Select to see deployments for the current user only.
   - **Show auto registration events** check box — Select to show auto registration events.
   - **User** — Name of the user that performed the deployment.
   - **Configuration Name** — Name of the deployment.

2. Click the link in the **Configuration Name** column to display the details of the deployment.

   The **Configuration Deployment Report** displays in the web browser with the following details:

   - **Configuration Name** — Name of the deployment.
   - **Deployment Time** — Time when the deployment occurred.
   - **User** — Name of the user that performed the deployment.
   - **Status** — Status of the deployment.

   If you select a report where all devices in that deployment have been deleted, an "associated devices removed" message displays.

3. Click the link in the **Deployment Time** column to display the details of the deployment.

   The **Detailed Configuration Deployment Report** displays in the web browser with the following details:

   - **Configuration** — Name of the deployment.
   - **Product** — Product on which the deployment occurred.
   - **Status** — Status of the deployment.
   - **Error** — Any error messages.

4. To export a report to a file, refer to "Exporting and saving IP reports to a file" on page 1232.
5. To e-mail a report, refer to "Exporting IP reports to e-mail recipients" on page 1232.
6. To configure how often to purge deployment reports, refer to "Configuring deployment report preferences" on page 161

Reports Template Manager overview

The Report Template Manager enables you to run, import, export, or delete preconfigured and user-defined reports.

Preconfigured reports

The Management application provides four preconfigured reports:

- Products List — This report displays general and detailed configuration information about products discovered by the Management application. For more information, refer to "IP Wired Products report" on page 1233.
- Detailed Product Report — This report displays configuration information about a specific product. For more information, refer to "Detailed Product Report" on page 1235.
- Detailed Cluster Report — This report displays configuration information about a VCS cluster. For more information, refer to "Detailed Cluster Report" on page 1255.
- Ports Tx/Rx Ratio — This report displays the ratio between transmitted and received data on a port or group of ports for the specified parameters. For more information, refer to "Ports Tx/Rx Ratio report" on page 1257.
- Low Traffic Ports — This report displays the percentage of data transmitted and received on ports for the specified parameters. For more information, refer to "Low Traffic Ports report" on page 1259.

User-defined reports

You can create user-defined reports using BIRT (Business Intelligence and Reporting Tools) report designer version 4.2.1 or later, a third-party open source reporting tool.

Accessing the Report Template Manager

1. Select **Reports > Report Manager**.

   The **Report Template Manager** dialog box displays (Figure 511).

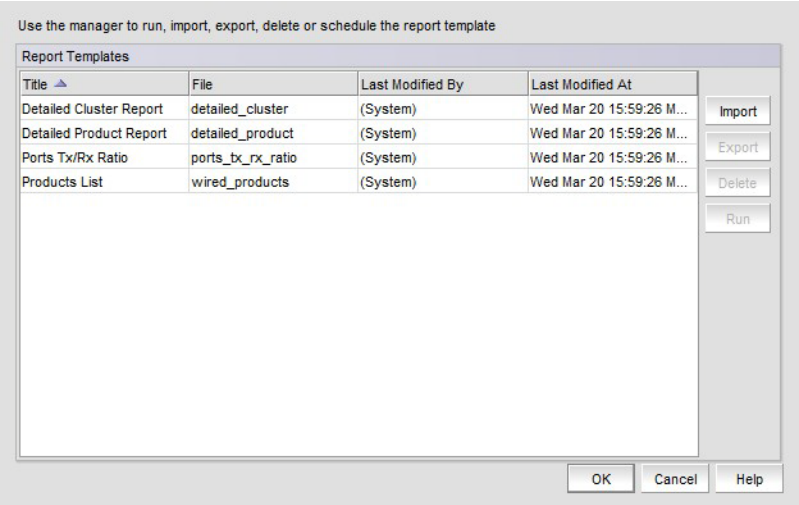


FIGURE 511 Report Template Manager dialog box

   The **Report Template Manager** dialog box includes the following fields and components:

   - **Report Templates** table — Lists all reports.
     - **Title** — The title of the report, which must be unique.
     - **File** — The file name of the report, which must be unique.
     - **Last Modified By** — The user (for example, System or Administrator) who modified the report last.
     - **Last Modified At** — The date and time the report was modified last.
   - **Import** button — Click to import a report template (refer to "Importing a report template" on page 1250).
   - **Export** button — Click to export a report template (refer to "Exporting a report template" on page 1250).
   - **Delete** button — Click to delete a report (refer to "Deleting reports" on page 1250).
   - **Run** button — Click to run a report (refer to "Viewing a report" on page 1249).

2. Click **OK** to close the **Report Template Manager** dialog box.

Viewing a report

1. Select **Reports > Report Manager**.

   The **Report Template Manager** dialog box displays.

2. Select the report you want to run in the **Report Templates** table.

3. Click **Run**.

   If one or more parameters are required for the report, the **Parameter** dialog box displays (Figure 512).

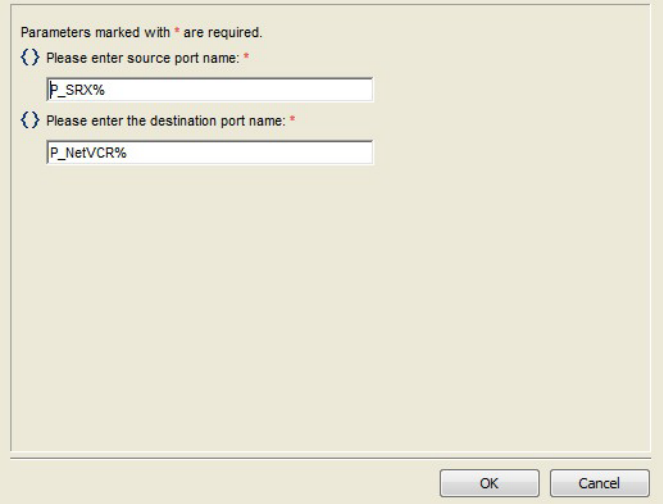


FIGURE 512 Parameter dialog box

4. Enter the parameters (such as IP address, source port name, or destination port name).

NOTE
The parameter fields cannot be empty.

   The source and destination port names can use the SQL wildcard character "%".

5. Click **OK**.

   The report displays. For more information about report content and functions, refer to "Report content and functions" on page 1251.

6. Click **OK** to close the **Report Template Manager** dialog box.

Importing a report template

You can use the BIRT report designer to create user-defined report templates that you can then import into Report Template Manager.

1. Select **Reports > Report Manager**.

   The **Report Template Manager** dialog box displays.

2. Click **Import**.

   The **Open** dialog box displays.

3. Browse to the location from which you want to import the report and click **Open**.

   If a report with the same file name already exists, click **Yes** on the overwrite message to overwrite the report.

   If the title for the imported report already exists or the report does not have a title, an **Edit Report Title** dialog box displays. Enter a new title for the report and click **OK**.

4. Click **OK** to close the **Report Template Manager** dialog box.

Exporting a report template

You can export a preconfigured or user-defined report template and use the BIRT report designer to modify the report that you can then reimport into Report Template Manager.

1. Select **Reports > Report Manager**.

   The **Report Template Manager** dialog box displays.

2. Click **Export**.

   The **Save** dialog box displays. If you want to change the name of the report, change the name of the file in the **File Name** field.

3. Browse to the location to which you want to export the report and click **Save**.

   If a report with the same file name already exists, click **Yes** on the overwrite message to overwrite the report.

   When the export is complete, click **OK** on the successful export message.

4. Click **OK** to close the **Report Template Manager** dialog box.

Deleting reports

You can delete preconfigured and user-defined reports. If you delete a preconfigured report, and then reimport it, the preconfigured report works as if it is a user-defined report.

1. Select **Reports > Report Manager**.

   The **Report Template Manager** dialog box displays.

2. Select one or more reports and click **Delete**.

   For preconfigured reports, click **Yes** on the continue message to delete the report.

   For user-defined reports, click **Yes** on the confirmation message to delete the report.

3. Click **OK** to close the **Report Template Manager** dialog box.

Report content and functions

Each report contains the following information:

- The name of the report displayed at the top of the report.
- The date and time the report was generated.
- The report data, presented in a tabular format.

Depending on the report type, you can perform the following functions:

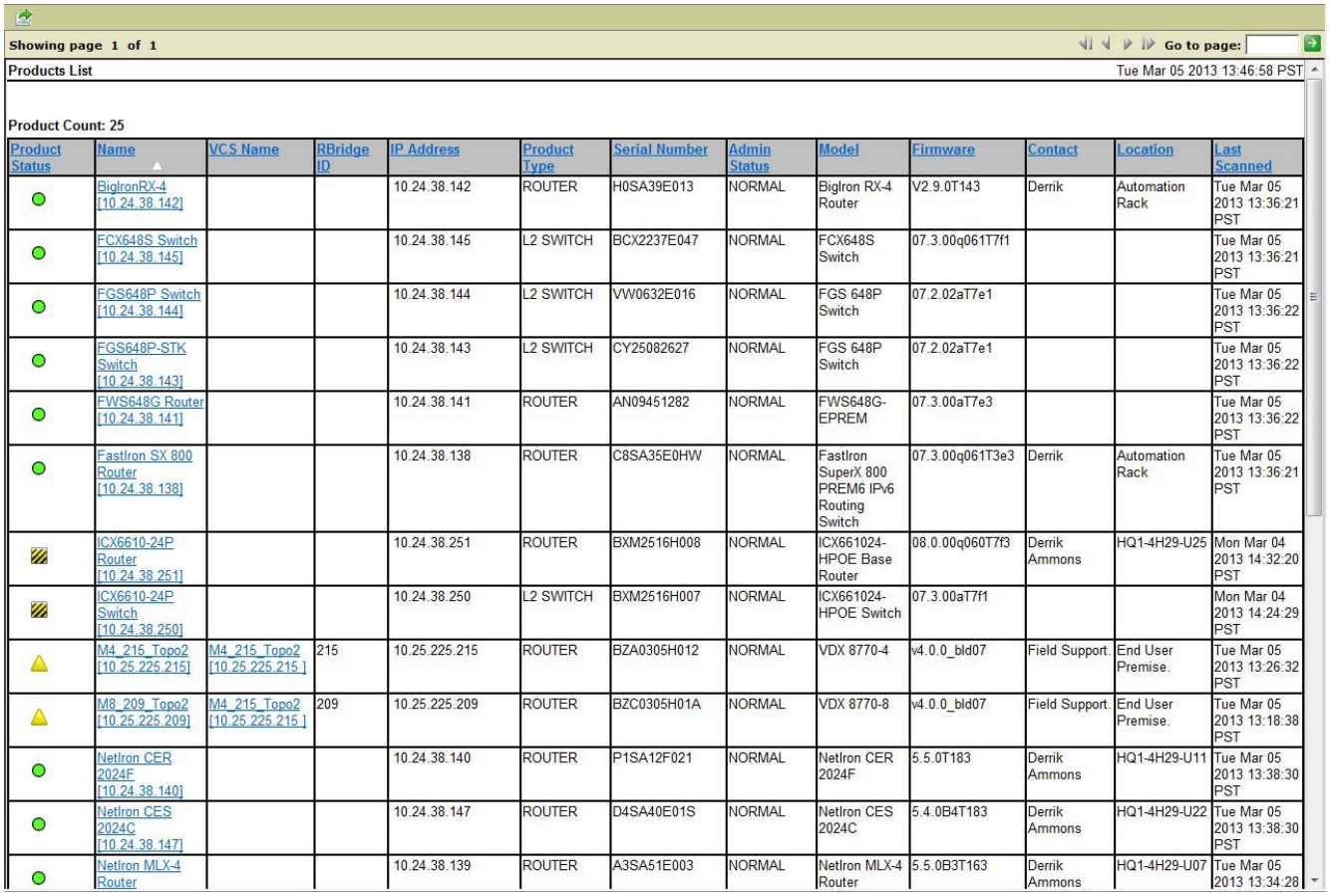
- Sort a table by clicking a column head. Click a column head again to reverse the sort order.
- Launch a more detailed report by clicking a link within the report.
- Export report data to a CSV, PDF, or Word file by clicking the **Export Data** icon in the Report toolbar (refer to "Exporting data from the report" on page 1260).
- Navigate through the report by using the following icons in the Report toolbar.

Icon	Description
	First page — Click to return to the first page in the report. Unavailable when you are on the first page of the report.
	Previous page — Click to return to the previous page in the report. Unavailable when you are on the first page of the report.
	Next page — Click to move to the next page in the report. Unavailable when you are on the last page of the report.
	Last page — Click to move to the last page in the report. Unavailable when you are on the last page of the report.
	Go to page — Enter a page number and click the arrow button to display a specific page in the report.

Products List report

The Products List report displays general and detailed configuration information about all discovered products (Figure 510).

The information on the report comes from the software image version that is in the Management application for that product. To ensure that the latest configuration information is in the Management application, run the discovery process or resynchronize the product.



Showing page 1 of 1 — Go to page:

Products List — Tue Mar 05 2013 13:46:58 PST

Product Count: 25

Product Status	Name	VCS Name	RBridge ID	IP Address	Product Type	Serial Number	Admin Status	Model	Firmware	Contact	Location	Last Scanned
	BigIronRX-4 [10.24.38.142]			10.24.38.142	ROUTER	H0SA39E013	NORMAL	BigIron RX-4 Router	V2.9.0T143	Derrik	Automation Rack	Tue Mar 05 2013 13:36:21 PST
	FCX648S Switch [10.24.38.145]			10.24.38.145	L2 SWITCH	BCX2237E047	NORMAL	FCX648S Switch	07.3.00q061T7f1			Tue Mar 05 2013 13:36:21 PST
	FGS648P Switch [10.24.38.144]			10.24.38.144	L2 SWITCH	VW0632E016	NORMAL	FGS 648P Switch	07.2.02aT7e1			Tue Mar 05 2013 13:36:22 PST
	FGS648P-STK Switch [10.24.38.143]			10.24.38.143	L2 SWITCH	CY25082627	NORMAL	FGS 648P Switch	07.2.02aT7e1			Tue Mar 05 2013 13:36:22 PST
	FWS648G Router [10.24.38.141]			10.24.38.141	ROUTER	AN09451282	NORMAL	FWS648G-EPREM	07.3.00aT7e3			Tue Mar 05 2013 13:36:22 PST
	FastIron SX 800 Router [10.24.38.138]			10.24.38.138	ROUTER	C8SA35E0HW	NORMAL	FastIron SuperX 800 PREM6 IPv6 Routing Switch	07.3.00q061T3e3	Derrik	Automation Rack	Tue Mar 05 2013 13:36:21 PST
	ICX6610-24P Router [10.24.38.251]			10.24.38.251	ROUTER	BXM2516H008	NORMAL	ICX661024-HPOE Base Router	08.0.00q060T7f3	Derrik Ammons	HQ1-4H29-U25	Mon Mar 04 2013 14:32:20 PST
	ICX6610-24P Switch [10.24.38.250]			10.24.38.250	L2 SWITCH	BXM2516H007	NORMAL	ICX661024-HPOE Switch	07.3.00aT7f1			Mon Mar 04 2013 14:24:29 PST
	M4_215_Topo2 [10.25.225.215]	M4_215_Topo2 [10.25.225.215]	215	10.25.225.215	ROUTER	BZA0305H012	NORMAL	VDX 8770-4	v4.0.0_bld07	Field Support.	End User Premise.	Tue Mar 05 2013 13:26:32 PST
	M8_209_Topo2 [10.25.225.209]	M4_215_Topo2 [10.25.225.215]	209	10.25.225.209	ROUTER	BZC0305H01A	NORMAL	VDX 8770-8	v4.0.0_bld07	Field Support.	End User Premise.	Tue Mar 05 2013 13:18:38 PST
	NetIron CER 2024F [10.24.38.140]			10.24.38.140	ROUTER	P1SA12F021	NORMAL	NetIron CER 2024F	5.5.0T183	Derrik Ammons	HQ1-4H29-U11	Tue Mar 05 2013 13:38:30 PST
	NetIron CES 2024C [10.24.38.147]			10.24.38.147	ROUTER	D4SA40E01S	NORMAL	NetIron CES 2024C	5.4.0B4T183	Derrik Ammons	HQ1-4H29-U22	Tue Mar 05 2013 13:38:30 PST
	NetIron MLX-4 Router			10.24.38.139	ROUTER	A3SA51E003	NORMAL	NetIron MLX-4 Router	5.5.0B3T163	Derrik Ammons	HQ1-4H29-U07	Tue Mar 05 2013 13:34:28

FIGURE 513 Products List report

Table 113 describes the fields and components of the Products List report.

TABLE 113 Products List report fields and components

Field/Component	Description
Product Count	The number of products in the report.
Product Status	Whether the product is reachable (green icon), marginal ( ), degraded link ( ), down ( ), unhealthy ( ), or not reachable ( ).
Name	The name of the product. Click the name of a product to launch the Detailed Product Report.
VCS Name	The name of the VCS product. Click the name of a product to launch the Detailed Cluster Report.
RBridge ID	The RBridge ID of the VCS product.

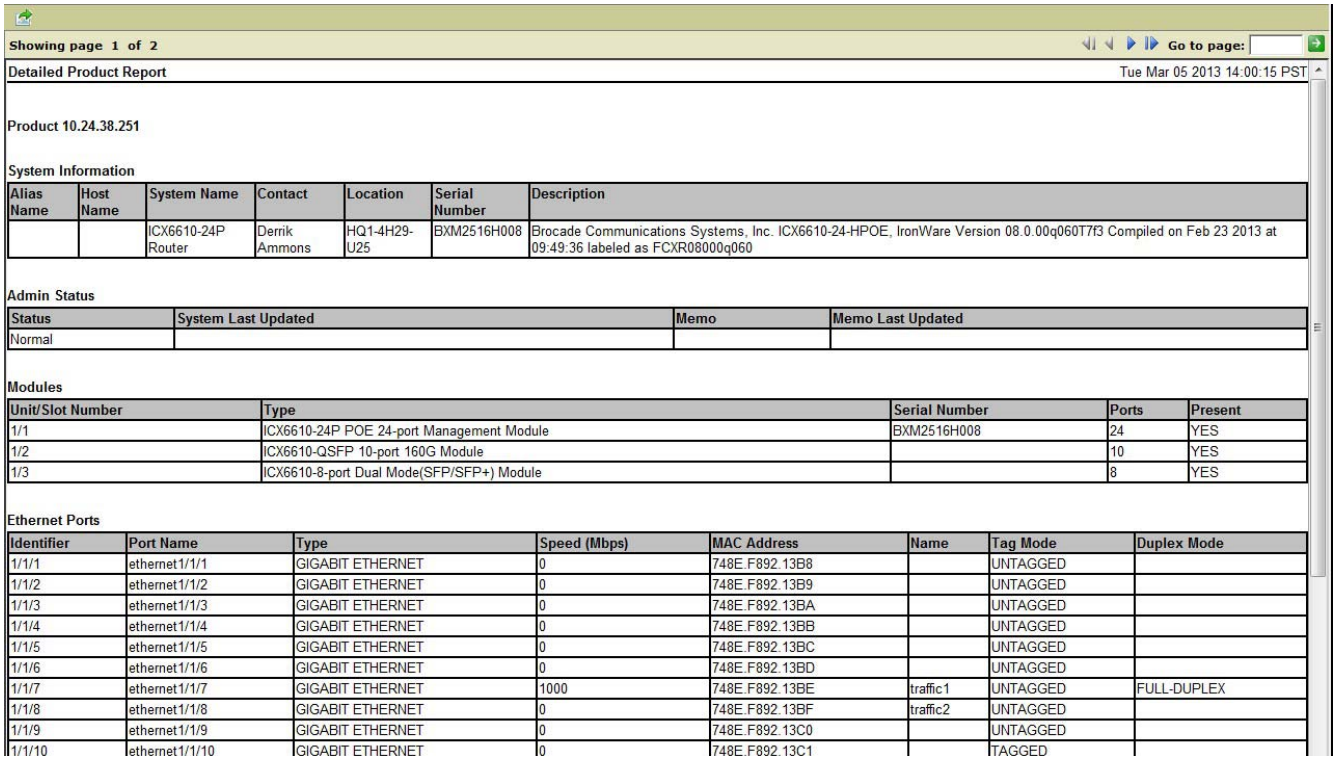
TABLE 113 Products List report fields and components (Continued)

Field/Component	Description
IP Address	The IP address of the product.
Product Type	The type of product.
Serial Number	The serial number of the product.
Admin Status	The administrative status of the product. Possible status includes: • Normal — The product is in normal operating mode. • Troubleshooting — The product is in troubleshooting mode.
Model	The model of the product.
Firmware	The firmware level of the product.
Contact	The contact name for the product.
Location	The location of the product.
Last Scanned	The date and time the product was last scanned.

Detailed Product Report

The Detailed Product Report displays general and detailed configuration information about products (Figure 514).

NOTE
This report is not available for VCS clusters. VCS cluster data is available in the Detailed Cluster Report (refer to "Detailed Cluster Report" on page 1255).



Showing page 1 of 2 Go to page:

Detailed Product Report Tue Mar 05 2013 14:00:15 PST

Product 10.24.38.251

System Information

Alias Name	Host Name	System Name	Contact	Location	Serial Number	Description
		ICX6610-24P Router	Derrik Ammons	HQ1-4H29-U25	BXM2516H008	Brocade Communications Systems, Inc. ICX6610-24-HPOE, IronWare Version 08.0.00q060T7f3 Compiled on Feb 23 2013 at 09:49:36 labeled as FCXR08000q060

Admin Status

Status	System Last Updated	Memo	Memo Last Updated
Normal			

Modules

Unit/Slot Number	Type	Serial Number	Ports	Present
1/1	ICX6610-24P POE 24-port Management Module	BXM2516H008	24	YES
1/2	ICX6610-QSFP 10-port 160G Module		10	YES
1/3	ICX6610-8-port Dual Mode(SFP/SFP+) Module		8	YES

Ethernet Ports

Identifier	Port Name	Type	Speed (Mbps)	MAC Address	Name	Tag Mode	Duplex Mode
1/1/1	ethernet1/1/1	GIGABIT ETHERNET	0	748E.F892.13B8		UNTAGGED	
1/1/2	ethernet1/1/2	GIGABIT ETHERNET	0	748E.F892.13B9		UNTAGGED	
1/1/3	ethernet1/1/3	GIGABIT ETHERNET	0	748E.F892.13BA		UNTAGGED	
1/1/4	ethernet1/1/4	GIGABIT ETHERNET	0	748E.F892.13BB		UNTAGGED	
1/1/5	ethernet1/1/5	GIGABIT ETHERNET	0	748E.F892.13BC		UNTAGGED	
1/1/6	ethernet1/1/6	GIGABIT ETHERNET	0	748E.F892.13BD		UNTAGGED	
1/1/7	ethernet1/1/7	GIGABIT ETHERNET	1000	748E.F892.13BE	traffic1	UNTAGGED	FULL-DUPLEX
1/1/8	ethernet1/1/8	GIGABIT ETHERNET	0	748E.F892.13BF	traffic2	UNTAGGED	
1/1/9	ethernet1/1/9	GIGABIT ETHERNET	0	748E.F892.13C0		UNTAGGED	
1/1/10	ethernet1/1/10	GIGABIT ETHERNET	0	748E.F892.13C1		TAGGED	

FIGURE 514 Detailed Product Report

Table 114 describes the fields and components of the Detailed Product Report.

TABLE 114 Detailed Product Report fields and components

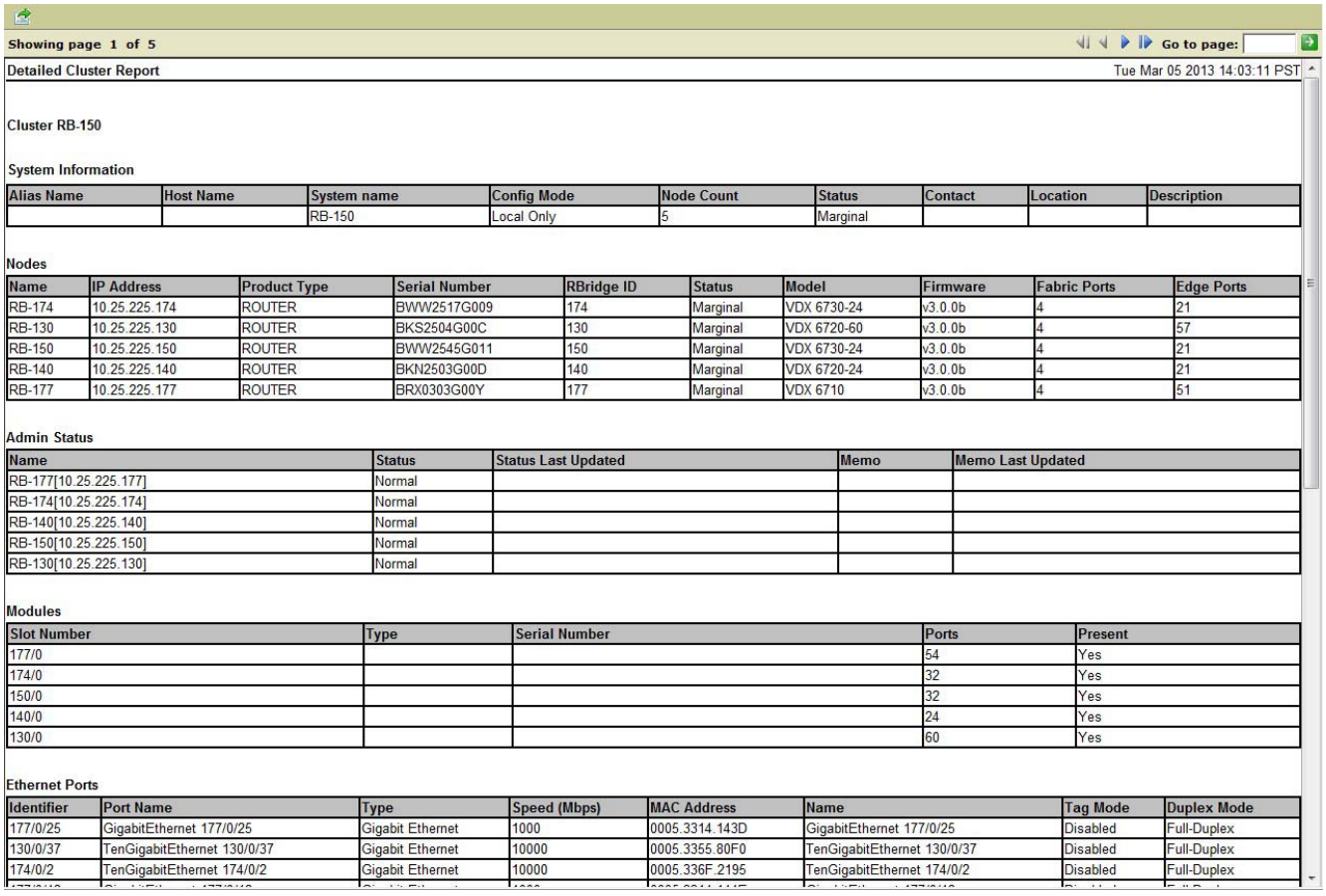
Field/Component	Description
Product	The IP address of the product.
System Information	System information includes the following: • **Alias Name —** An optional name that is entered using the **Properties** dialog box. It provides an alternate name for the product if you want to override the **Host Name** and **System Name** values. • **Host Name —** The name that the Management application obtains from the product during discovery. This may be the Domain Name System (DNS) name of the product, but may come from other naming services, depending on the configuration of the operating system on which the Management application is running. • **System Name** — The name the Management application retrieves from the "sysName" SNMP MIB variable during discovery. This name corresponds to the value specified by the **hostname** command in the product configuration file. The Management application displays the first name it finds for the product in the following order: Alias Name, Host Name, System Name. The Alias Name takes precedence over Host Name, which takes precedence over System Name, and so on. • **Contact —** A contact name for the product. • **Location —** The location of the product. • **Serial Number —** The serial number of the product. The serial number is not displayed for products that support stacking. • **Description —** A description of the product.
Admin Status	Administrative status information includes the following: • **Status —** Whether the product is in normal operating mode or troubleshooting mode. • **System Last Updated —** When the last system update occurred. • **Memo —** A memo for the product. • **Memo Last Updated —** When the last memo update occurred.
Modules	Module information shows what modules are installed on the product. • **Unit/Slot Number —** For products that support stacking, you can view the unit number and slot number. **Slot Number** — For products that do not support stacking, you can view the slot number. • **Type** — For wireless products, the model name of the product. For wired products, the type of module installed in the slot. • **Serial Number** — The serial number of the module. For wired products, the serial number cell may be blank. • **Ports** — The number of ports on the product. The number of ports for ATM modules displays as zero. • **Present** — Whether the module is installed on the product.
Ethernet Ports	This table contains the following information for each Ethernet interface on the product: • **Identifier** — The port identifier. • **Port Name** — The port name. • **Type** — The type of port. • **Speed (Mbps)** — The speed of the port. • **MAC Address** — The MAC address of the port. • **Name** — The name of the port. • **Tag Mode** — The tag mode of the port. • **Duplex Mode** — The duplex mode of the port.

TABLE 114 Detailed Product Report fields and components (Continued)

Physical Ports	Physical port information for each port on the product. • **Identifier** — The port identifier of the physical interfaces on the product. • **Port Name** — The port name of the physical interfaces on the product. • **Type** — The type of port of the physical interfaces on the product. • **Speed (Mbps)** — The speed of the physical interfaces on the product. • **MAC Address** — The MAC address of the physical interfaces on the product. Displays as 0000.0000.0000 for module interfaces. • **Name** — The name of the port on the product. • **Tag Mode** — The tag mode (tagged, untagged, dual, or blank) of the physical interfaces on the product. • **Duplex Mode** — The duplex mode of the physical interfaces on the product.

Detailed Cluster Report

The Detailed Cluster Report report displays general and detailed configuration information about fabrics (Figure 515).



Showing page 1 of 5 — Go to page:

Detailed Cluster Report — Tue Mar 05 2013 14:03:11 PST

Cluster RB-150

System Information

Alias Name	Host Name	System name	Config Mode	Node Count	Status	Contact	Location	Description
		RB-150	Local Only	5	Marginal			

Nodes

Name	IP Address	Product Type	Serial Number	RBridge ID	Status	Model	Firmware	Fabric Ports	Edge Ports
RB-174	10.25.225.174	ROUTER	BWW2517G009	174	Marginal	VDX 6730-24	v3.0.0b	4	21
RB-130	10.25.225.130	ROUTER	BKS2504G00C	130	Marginal	VDX 6720-60	v3.0.0b	4	57
RB-150	10.25.225.150	ROUTER	BWW2545G011	150	Marginal	VDX 6730-24	v3.0.0b	4	21
RB-140	10.25.225.140	ROUTER	BKN2503G00D	140	Marginal	VDX 6720-24	v3.0.0b	4	21
RB-177	10.25.225.177	ROUTER	BRX0303G00Y	177	Marginal	VDX 6710	v3.0.0b	4	51

Admin Status

Name	Status	Status Last Updated	Memo	Memo Last Updated
RB-177[10.25.225.177]	Normal			
RB-174[10.25.225.174]	Normal			
RB-140[10.25.225.140]	Normal			
RB-150[10.25.225.150]	Normal			
RB-130[10.25.225.130]	Normal			

Modules

Slot Number	Type	Serial Number	Ports	Present
177/0			54	Yes
174/0			32	Yes
150/0			32	Yes
140/0			24	Yes
130/0			60	Yes

Ethernet Ports

Identifier	Port Name	Type	Speed (Mbps)	MAC Address	Name	Tag Mode	Duplex Mode
177/0/25	GigabitEthernet 177/0/25	Gigabit Ethernet	1000	0005.3314.143D	GigabitEthernet 177/0/25	Disabled	Full-Duplex
130/0/37	TenGigabitEthernet 130/0/37	Gigabit Ethernet	10000	0005.3355.80F0	TenGigabitEthernet 130/0/37	Disabled	Full-Duplex
174/0/2	TenGigabitEthernet 174/0/2	Gigabit Ethernet	10000	0005.336F.2195	TenGigabitEthernet 174/0/2	Disabled	Full-Duplex

FIGURE 515 Detailed Cluster Report

Table 115 describes the fields and components of the Detailed Cluster Report.

TABLE 115 Detailed Cluster Report fields and components

Field/Component	Description
Cluster	The name of the cluster.
System Information	System information includes the following: • **Alias Name —** An optional name that is entered using the **Properties** dialog box. It provides an alternate name for the product if you want to override the **Host Name** and **System Name** values. • **Host Name —** The name that the Management application obtains from the product during discovery. This may be the Domain Name System (DNS) name of the product, but may come from other naming services, depending on the configuration of the operating system on which the Management application is running. • **System Name** — The name the Management application retrieves from the "sysName" SNMP MIB variable during discovery. This name corresponds to the value specified by the **hostname** command in the product configuration file. The Management application displays the first name it finds for the product in the following order: Alias Name, Host Name, System Name. The Alias Name takes precedence over Host Name, which takes precedence over System Name. • **Config Mode** — The configuration mode. • **Node Count** — The number of nodes in the fabric. • **Status** — The status of the fabric. • **Contact —** A contact name for the product. • **Location —** The location of the product. • **Serial Number —** The serial number of the product. The serial number is not displayed for products that support stacking. • **Description —** A description of the product.
Nodes	Node information includes the following: • **Name** — The name of the node. Click the name of a product to launch the **Detailed Product Report.** • **IP Address** — The IP address of the product. • **Product Type** — The type of product. • **Serial Number** — The serial number of the product. • **RBridge ID** — The RBridge ID number of the product. • **Status** — The status of the product. • **Model** — The model of the product. • **Firmware** — The firmware level of the product. • **Fabric Ports** — The number of fabric ports on the product. • **Edge Ports** — The number of edge ports on the product.
Admin Status	Administrative status information includes the following: • **Name** — The name and IP address of the product. • **Status —** Whether the product is in normal operating mode or troubleshooting mode. • **Status Last Updated —** When the last status update occurred. • **Memo —** A memo for the product. • **Memo Last Updated —** When the last memo update occurred.

TABLE 115 Detailed Cluster Report fields and components (Continued)

Modules	Module information shows what modules are installed on the product. • **Slot Number** — For products that do not support stacking, you can view the slot number. • **Type** — The type of module installed in the slot. • **Serial Number** — The serial number of the module. For wired products, the serial number cell may be blank. • **Ports** — The number of ports on the product. The number of ports for ATM modules displays as zero. • **Present** — Whether the module is installed on the product.
Ethernet Ports	This table contains the following information for each Ethernet interface on the product: • **Identifier** — The port identifier. • **Port Name** — The port name. • **Type** — The type of port. • **Speed (Mbps)** — The speed of the port. • **MAC Address** — The MAC address of the port. • **Name** — The name of the port. • **Tag Mode** — The tag mode of the port. • **Duplex Mode** — The duplex mode of the port.

Ports Tx/Rx Ratio report

The Ports Tx/Rx Ratio report (Figure 516) details the ratio between transmitted and received data on a port or group of ports for the specified parameters.

Showing page 1 of 31 Go to page:

Ports Tx/Rx ratio for port names like "%" and "%" Tue Mar 05 2013 14:22:20 PST

Summary

Location	Device Name	IP Address	Total Received (MB)	Total Tansmitted (MB)	Ratio (%)	Collection Time
HQ1-4H29-U22	NetIron CES 2024C	10.24.38.147	6.2769	8.0750	128.65	Tue Mar 05 2013 14:22:00 PST
HQ1-4H29-U11	NetIron CER 2024F	10.24.38.140	15.5632	20.9420	134.56	Tue Mar 05 2013 14:22:00 PST
End User Premise.	sw0	10.25.225.157	10,784.1514	673.6249	6.25	Tue Mar 05 2013 14:22:00 PST
End User Premise.	sw0	10.25.225.158	10,784.1514	668.3159	6.20	Tue Mar 05 2013 14:22:00 PST
End User Premise.	sw0	10.25.225.205	10,784.1514	133.8921	1.24	Tue Mar 05 2013 14:22:00 PST
End User Premise.	sw0	10.25.225.159	10,784.1514	1,337.5188	12.40	Tue Mar 05 2013 14:22:00 PST
End User Premise.	sw0	10.25.225.175	10,784.1514	8,245.9221	76.46	Tue Mar 05 2013 14:22:00 PST
End User Premise.	RB-179	10.25.225.179	3,440.4858	3,299.0518	95.89	Tue Mar 05 2013 14:22:00 PST
End User Premise.	RB-177	10.25.225.177	111.8130	115.7341	103.51	Tue Mar 05 2013 14:22:00 PST
End User Premise.	RB-174	10.25.225.174	110.0844	78.8497	71.63	Tue Mar 05 2013 14:22:00 PST
End User Premise.	RB-150	10.25.225.150	242.0697	187.1548	77.31	Tue Mar 05 2013 14:22:00 PST
End User Premise.	RB-140	10.25.225.140	86.1849	102.0974	118.46	Tue Mar 05 2013 14:22:00 PST
End User Premise.	RB-130	10.25.225.130	110.9880	220.6480	198.80	Tue Mar 05 2013 14:22:00 PST
End User Premise.	M8_209_Topo2	10.25.225.209	79.5244	58.9402	74.12	Tue Mar 05 2013 14:22:00 PST
End User Premise.	M4_215_Topo2	10.25.225.215	82.3601	91.2486	110.79	Tue Mar 05 2013 14:22:00 PST

Rx Details

Location	Device Name	Name	Port Name	Rx (MB)
HQ1-4H29-U22	NetIron CES 2024C	to_MLXe1/2	ethernet1/1	6.2769
HQ1-4H29-U11	NetIron CER 2024F	to_MLXe1/1	ethernet1/1	15.5632
HQ1-4H29-U07	NetIron MLX-4 Router	to_CESe1/1	ethernet1/2	8.0754
HQ1-4H29-U07	NetIron MLX-4 Router	to_CERe1/1	ethernet1/1	20.9439
HQ1-4H29-U07	NetIron MLX-4 Router	test2	ethernet1/12	2.6921
HQ1-4H29-U07	NetIron MLX-4 Router	test1	ethernet1/11	2.6921
HQ1-4H29-U07	NetIron MLX-4 Router	ixia2	ethernet1/17	0.0001
HQ1-4H29-U07	NetIron MLX-4 Router	ixia1	ethernet1/18	0.0000
End User Premise.	sw0	TenGigabitEthernet 205/1/9	TenGigabitEthernet 205/1/9	0.0000
End User Premise.	sw0	TenGigabitEthernet 205/1/8	TenGigabitEthernet 205/1/8	0.0000
End User Premise.	sw0	TenGigabitEthernet 205/1/7	TenGigabitEthernet 205/1/7	0.0000
End User Premise.	sw0	TenGigabitEthernet 205/1/6	TenGigabitEthernet 205/1/6	0.0000
End User Premise.	sw0	TenGigabitEthernet 205/1/5	TenGigabitEthernet 205/1/5	0.0000

FIGURE 516 Ports Tx/Rx Ratio report

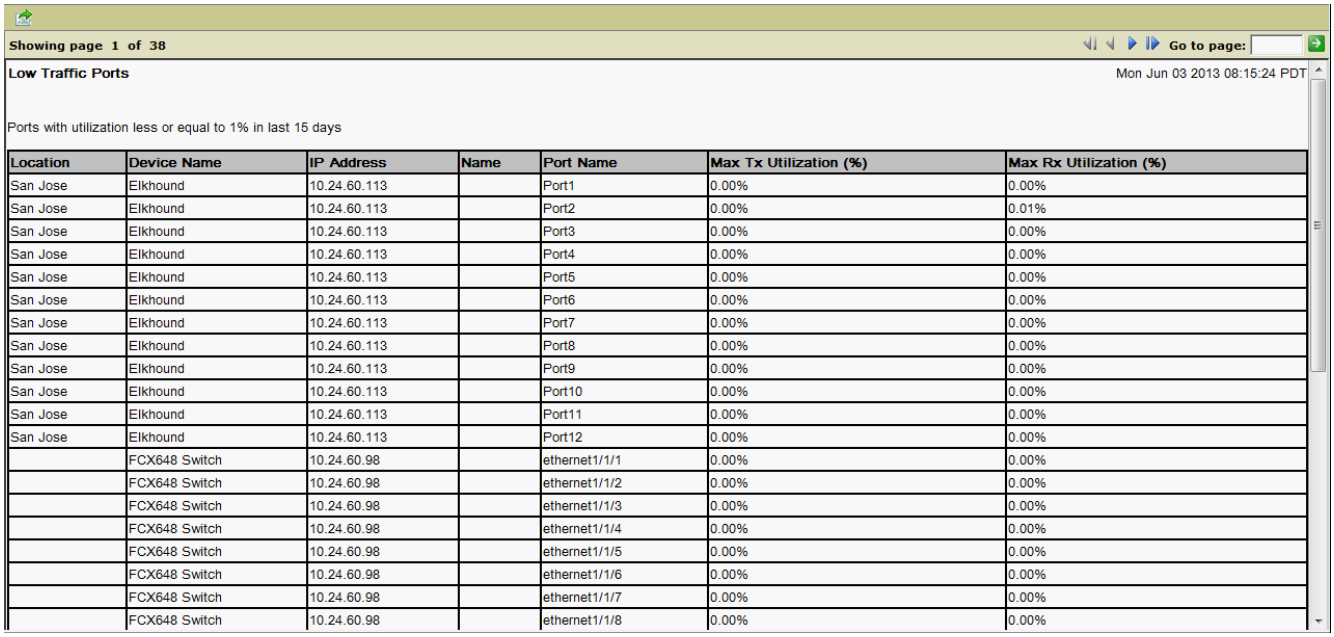
Table 116 describes the fields and components of the Ports Tx/Rx Ratio report.

TABLE 116 Ports Tx/Rx Ratio report fields and components

Field/Component	Description
Summary table	
Location	The location of the device.
Device Name	The name of the device. Click the device name link to launch the **Detailed Product Report**.
IP Address	The IP address of the device.
Total Received (MB)	The total data received (the sum of Rx in **Rx Details** table) in megabytes.
Total Transmitted (MB)	The total data transmitted (the sum of Tx in **Tx Details** table) in megabytes.
Ratio (%)	The ratio of the total received to the total transmitted (100*(Total Transmitted)/(Total Received)). Displays N/A if the total received is zero.
Collection Time	The time data was collected
Rx Details table	
Location	The location of the device.
Device Name	The name of the device.
Name	The name of the received data.
Port Name	The name of the port.
Rx (MB)	The total data received in megabytes.
Tx Details table	
Location	The location of the device.
Device Name	The name of the device.
Name	The name of the transmitted data.
Port Name	The name of the port.
Tx (MB)	The total data transmitted in megabytes.

Low Traffic Ports report

The Low Traffic Ports report details the port utilization that is less than or equal to the percentage and number of days you specify (Figure 517).



Showing page 1 of 38 Go to page:

Low Traffic Ports Mon Jun 03 2013 08:15:24 PDT

Ports with utilization less or equal to 1% in last 15 days

Location	Device Name	IP Address	Name	Port Name	Max Tx Utilization (%)	Max Rx Utilization (%)
San Jose	Elkhound	10.24.60.113		Port1	0.00%	0.00%
San Jose	Elkhound	10.24.60.113		Port2	0.00%	0.01%
San Jose	Elkhound	10.24.60.113		Port3	0.00%	0.00%
San Jose	Elkhound	10.24.60.113		Port4	0.00%	0.00%
San Jose	Elkhound	10.24.60.113		Port5	0.00%	0.00%
San Jose	Elkhound	10.24.60.113		Port6	0.00%	0.00%
San Jose	Elkhound	10.24.60.113		Port7	0.00%	0.00%
San Jose	Elkhound	10.24.60.113		Port8	0.00%	0.00%
San Jose	Elkhound	10.24.60.113		Port9	0.00%	0.00%
San Jose	Elkhound	10.24.60.113		Port10	0.00%	0.00%
San Jose	Elkhound	10.24.60.113		Port11	0.00%	0.00%
San Jose	Elkhound	10.24.60.113		Port12	0.00%	0.00%
	FCX648 Switch	10.24.60.98		ethernet1/1/1	0.00%	0.00%
	FCX648 Switch	10.24.60.98		ethernet1/1/2	0.00%	0.00%
	FCX648 Switch	10.24.60.98		ethernet1/1/3	0.00%	0.00%
	FCX648 Switch	10.24.60.98		ethernet1/1/4	0.00%	0.00%
	FCX648 Switch	10.24.60.98		ethernet1/1/5	0.00%	0.00%
	FCX648 Switch	10.24.60.98		ethernet1/1/6	0.00%	0.00%
	FCX648 Switch	10.24.60.98		ethernet1/1/7	0.00%	0.00%
	FCX648 Switch	10.24.60.98		ethernet1/1/8	0.00%	0.00%

FIGURE 517 Low Traffic Ports report

Table 117 describes the fields and components of the Low Traffic Ports report.

TABLE 117 Low Traffic Ports report fields and components

Field/Component	Description
Location	The location of the device.
Device Name	The name of the device.
IP Address	The IP address of the device.
Name	The user-defined name of the port.
Port Name	The port type and identifier, such as ethernet2/19.
Max Tx Utilization (%)	The percentage of data transmitted.
Max Rx Utilization (%)	The percentage of data received.

Exporting data from the report

You can export data from a report to CSV, PDF, or Word.

1. Run a report (refer to "Viewing a report" on page 1249).
2. From the report, click the **Export Report** icon on the Report toolbar.

   The **Export Report** dialog box displays.
3. Select an export format (PDF or Word) from the **Export Format** list.
4. Configure what content to export by selecting one of the following options:
   - Select **All pages** to export the entire report.
   - Select **Current page** to export the displayed page.
   - Select **Pages** and enter the page numbers or range you want to export.
5. Size the report data by selecting one of the following options:
   - Select **Auto** to display the report at the default size (Actual size).
   - Select **Actual size** (PDF only) to display the report at its actual size.
   - Select **Fit to whole page** (PDF only) to resize the report to display entirely in the view.
6. Click **OK** on the **Export Report** dialog box.
7. View the report immediately by clicking **Open** on the **File Download** dialog box.
8. Save the report by clicking **Save** on the **File Download** dialog box.
9. Browse to the location where you want to save the report and click **Save** on the **Save As** dialog box.

Appendix

Application menus

A

In this appendix

Dashboard main menus

The menu bar is located at the top of the main window. The following table outlines the many functions available on each menu.

Menu	Command	Command Options
Server Menu		
	Users — Select to configure users and user groups.	
	User Profile — Select to configure user profiles.	
	Active Sessions — Select to display the active Management application sessions.	
	Server Properties — Select to display the Server properties.	
	Options — Select to configure the Management application options.	
	Exit — Select to close the Management Client.	
View Menu		
	Show Main Tab — Select to choose which tab to display.	
		Dashboard — Select to show the dashboard.
		SAN — Select to show the SAN tab.
		IP — Select to show the IP tab.
	Show Panels — Select to choose which widgets to display.	
		All Panels — Select to show the Dashboard and Master Log.
		Dashboard — Select to only show the Dashboard.
		Master Log — Select to only show the Master Log.
Help Menu		
	Contents — Select to open the Online Help.	
	Find — Select to search the Online Help.	

Menu	Command	Command Options
	License — Select to view or change your License information.	
	About *Management_Application_Name* **—** Select to view the application information, such as the company information and release number.	

IP main menus

The menu bar is located at the top of the main window. The following table outlines the many functions available on each menu.

Menu	Command	Command Options
Server Menu		
	Users. Select to configure users and user groups.	
	User Profile. Select to configure user profiles.	
	Active Sessions. Select to display the active Management application sessions.	
	Server Properties. Select to display the Server properties.	
	Options. Select to configure the Management application options.	
	Exit. Select to close the Management Client.	
Edit Menu		
	Copy. Select to copy information and move it to another location.	
	Select All. Select to select all objects in the Connectivity Map and Product List.	
	Properties. Select to display the selected objects properties.	
View Menu		
	Show Main Tab. Select to choose which tab to display.	
		Dashboard. Select to show the dashboard.
		SAN. Select to show the SAN tab.
		IP. Select to show the IP tab.

Menu	Command	Command Options
	Show Panels. Select to choose which panels to display.	
		All Panels. Select to show all panels.
		Topology Map. Select to only show the topology map.
		Product List. Select to only show the Product List.
		Master Log. Select to only show the Master Log.
	Main Display. Select to choose which topology to display	
		Network Objects. Select to display Network Objects.
		L2 Topology. Select to display the L2 topology map.
		Ethernet Fabrics. Select to display the Ethernet Fabrics topology map.
		IP Topology. Select to display the IP topology map.
		VLAN Topology. Select to display the VLAN topology map.
		Host Topology. Select to display the Host topology map.
	Enable Flyover Display. Select to enable flyover display.	
	Show Ports. — Select to show utilized ports on the selected device.	
	Map Display Layout. Select to choose a map format.	
		Organic. Select to set the map format to organic.
		Orthogonal. Select to set the map format to orthogonal.
		Orthogonal (Merge Lines). Select to set the map format to orthogonal with merged lines.
		Hierarchical. Select to set the map format to hierarchical.
		Circular. Select to set the map format to circular.
		Free Form. Select to set the map format to free form.
	Product Label. Select to configure which product labels display.	
		Name + IP. Select to display the product name and IP address as the product label.
		Name. Select to display the product name as the product label.
		IP Address. Select to display the IP Address (IPv4 or IPv6 format) as the product label.
Discover Menu		
	IP Products. Select to set up IP product discovery.	
	Rediscover. Select to rediscover devices.	
	Host Adapters. Select to discover hosts.	
	VM Managers. Select to discover VM managers.	
	Add Product Group. Select to create a product management group.	

Menu	Command	Command Options
		Static. Select to create a product group based on device.
		Dynamic. Select to create a product group based on device attributes.
	Add Port Group. Select to create a port management group.	
	Edit Group. Select to edit a management group.	
	Duplicate Group. Select to duplicate a management group.	
	Delete Group. Select to delete a management group.	
Configure Menu		
	Element Manager. Select to configure a selected device.	
		Front Panel. (IronWare OS device) Select to display a graphic of the front panel for the selected device.
		Web. (IronWare OS device) Select to launch the web management interface for the selected device.
		Hardware. (Fabric OS devices) Select to launch the Element Manager or Web Tools application for the selected device.
		Ports. (Fabric OS devices) Select to launch Web Tools - Port Administration for the selected device.
		Admin. (Fabric OS devices) Select to launch Web Tools - Switch Administration for the selected device.
	Configuration. Select to manage the selected device.	
		Save. Select to save device configurations to the repository.
		Save Running to Startup. (Fabric OS devices) Select to save the DCB running configuration to the startup configuration on selected switches. Requires at least one discovered DCB switch.
		Restore. Select to restore device configurations from the repository.
		Configuration Repository. (Trial and Licensed version Only) Select to manage device configurations from the repository.
		Schedule Backup. (Trial and Licensed version Only) Select to schedule configuration backup.
		Replicate. (Trial and Licensed version Only) (Fabric OS devices) Select to replicate the switch Configuration or Security.
	Configuration Wizard. Select to launch the Configuration Wizard.	
	CLI Configuration. Select to launch the CLI Configuration Wizard.	
	Deployment. Select to manage deployment.	

Menu	Command	Command Options
	Application Delivery. Select to choose an application delivery method.	
		VIP Servers. Select to monitor and configure real and virtual servers.
		GSLB. Select to create global server load balancing (GSLB) policies.
		SSL Certificates. Select to manage SSL certificates.
	MPLS. Select to configure the multiprotocol label switches service (MPLS).	
		VLL. Select to configure virtual leased line (VLL) services.
		VPLS. Select to configure virtual private LAN services (VPLS).
		VCID Pool. Select to create a pool of virtual circuit identifiers (VCID).
		LSP. Select to configure label switched path (LSP).
	Firmware Management. Select to launch the Image Repository.	
	DCB. Select to manage a DCB switch, port, or link aggregation group (LAG).	
	FCoE. Select to manage an FCoE port.	
	Host. Select to manage a selected host.	
		Adapter Software. Select to launch HCM.
		Adapter Ports — Select to configure Host Adapter ports.
	Packet Capture (Pcap). Select to configure packet capture.	
	Policy Based Routing — Select to configure policy-based routing.	
	Security. Select to manage security.	
		L2 ACL. Select to configure Layer 2 Access Control Lists on products and ports.
		L3 ACL. Select to configure Layer 3 Access Control Lists on products and ports.
		MAC Filter. Select to configure Media Access Control filters on products and ports.
		ACL Accounting. Select to enable or disable ACL accounting and clear counters.
	VLANs. Select to launch the VLAN Manager.	
	Zoning. Select to configure zones.	
		Fabric. Select to configure fabric zones.
		LSAN Zoning (Device Sharing). (Trial and Licensed version Only) Select to configure LSAN zones.

Menu	Command	Command Options
		Set Change Limits. Select to set zone limits for zone activation.
		List Zone Members. (Trial and Licensed version Only) Select to display all members in a zone.
Monitor Menu		
	Performance. Select to monitor IP devices.	
		Dashboard — Select to launch the Performance Dashboard.
		Historical Data Collectors. Select to monitor historical data.
		Real-Time Graph/Tables. Select to monitor performance through a graph or table, which displays real-time data for transmit and receive data.
		Historical Graph/Tables. Select to monitor a performance through a graph or table, which displays historical data for transmit and receive data.
		Expressions. Select to create expressions using management information base (MIB) objects.
		Custom Reports. Select to create custom performance reports.
	Traffic Analysis. Select to monitor traffic.	
		Configure sFlow. Select to configure sFlow payloads.
		Monitor sFlow. Select to monitor sFlow.
		Traffic Accounting. Select to run a traffic report.
		Custom Reports. Select to create custom traffic reports.
	Policy Monitor — Select to manage best practice policies.	
	Power Center. Select to monitor power over Ethernet.	
	MPLS. Select to monitor MPLS.	
		VLL. Select to monitor virtual leased line (VLL) services.
		VPLS. Select to monitor virtual private LAN services (VPLS).
		LSP Topology. Select to monitor label switched path (LSP).
	MRP Topology. Select to view an MRP topology.	
	Events. Select to display all events triggered on the selected product.	
	Event Notification. Select to configure the Management application to send event notifications at specified time intervals.	
		E-mail. Select to configure the Management application to send event notifications through e-mail.

Menu	Command	Command Options
		Call Home. Select to configure the Management Server to automatically dial-in to or send an E-mail to a support center to report system problems.
	Event Processing. Select to configure event processing.	
		Pseudo Events. Select to configure pseudo events.
		Event Actions. Select to configure events actions.
	Logs. Select to display logs.	
		Audit. Select to display a history of user actions performed through the application (except login/logout).
		Product Event. Select to display errors related to SNMP traps and Client-Server communications.
		Product Status. Select to display operational status changes of managed products.
		Security. Select to display security information.
		Syslog. Select to display Syslog events related to the selected device or fabric.
	SNMP Setup. Select to configure SNMP traps.	
		Trap Forwarding. Select to configure trap forwarding.
		Product Trap Recipients. Select to register a host as a trap recipient.
		Event Reception. Select to configure the server to accept or drop traps and specify SNMP credentials and community strings, which are required to decode traps on receiving them.
		Informs — Select to configure informs.
	Syslog Configuration. Select to configure Syslog for the management server.	
		Syslog Forwarding. Select to configure Syslog forwarding.
		Product Syslog Recipients. Select to register a host as a syslog recipient.
	Technical Support. Select to configure technical support data.	
		SupportSave. Select to capture server and client support data.
		Product/Host SupportSave. Select to configure technical support data collection.
		View Repository. Select to view repository data.
Reports Menu		
	Event Custom Reports. Select to generate custom event reports.	
	Wired Products. Select to run a wired product report.	
	AP Products — Select to run an AP product report.	

Menu	Command	Command Options
	Modules. Select to run a report on modules.	
	VLANs. Select to run a VLAN information report.	
	IP Subnets. Select to run a report of IP subnets on the network.	
	IP Addresses. Select to run a report on IP addresses on the network.	
	MAC Addresses. Select to run a report of MAC addresses on the network.	
	Product CLI. Select to run a product CLI report.	
	Deployment. Select to run a deployment report.	
	Host Adapters — Select to run a Host product report.	
		Inventory Report — Select to run a Host inventory report.
		Faulty SFP Report — Select to run a faulty SFP report.
Tools Menu		
	Address Finder. Select to search for IP or MAC addresses on the network.	
	Setup. Select to set up the applications that display on the **Tools** menu.	
	Product Menu. Select to access the tools available on a device's shortcut menu.	
	Tools List (determined by user settings). Select to open a software application. You can configure the **Tools** menu to display different software applications. Recommended tools to include in this menu include an internet browser, the command prompt application, and Notepad.	
Help Menu		
	Contents. Select to open the Online Help.	
	Find. Select to search the Online Help.	
	License. Select to view or change your License information.	
	About *Management_Application_Name*. Select to view the application information, such as the company information and release number.	

IP shortcut menus

You can use the Management application interface main menu to configure, monitor, and troubleshoot your IP components. The instructions for using these features are documented in the associated chapters of this manual.

For each IP component, you can optionally right-click the component and a shortcut menu displays. The following group components do not have shortcut menus:

- IP Subnet
- VLAN
- L2 Cloud

The table below details the command options available for each component.

Component	Menu/Submenu Commands	Comments
IronWare device		
	Element Manager >	
	Front Panel	Displays the IronWare device's front panel.
	Web	Launches the device's Web Management Interface.
	Configuration >	
	Save	Launches the **Configuration** dialog box with selected device highlighted.
	Restore	Launches the **Configuration** dialog box with selected device highlighted.
	Configuration Repository	Launches the **Configuration** dialog box with selected device highlighted.
	Schedule Backup	Launches the **Schedule Backup** dialog box.
	Security >	
	L2 ACL	
	L3 ACL	
	MAC Filter	
	Rate Limit Policy	
	Performance >	
	Real-Time Graph / Table	Launches the **Real-Time Graphs / Tables** dialog box.
	Historical Graph / Table	Launches the **Historical Graphs / Tables** dialog box.
	Power Center	
	Events	Displays an Event Log for the device.
	CLI through Server	Launches the device's CLI Element Manager.
	User Defined Menu items	
	Setup Tools	
	Technical Support	
	Network Objects	Displays the Network Objects view with the selected device highlighted.
	L2 Topology	Displays the L2 Topology view with the selected device highlighted.
	Detailed Report	Generates and displays a Detailed Report for the selected device
	Physical Ports Report	Generates and displays a Physical Ports Report for the selected device
	L2 sFlow Report	Generates and displays a Layer 2 sFlow Report for the selected device
	L3 sFlow Report	Generates and displays a Layer 2 sFlow Report for the selected device
	STP Report	Generates an STP/RSTP report for the selected device. Only available on the VLAN Topology view with STP enabled.
	Properties	Displays the Properties dialog box for the selected device.

Component	Menu/Submenu Commands	Comments
	Table >	Only available from Product List.
	Copy “Cell_Value”	Copies the information in the selected cell.
	Copy Row	Copies all information in the selected row.
	Copy Table	Copies all information in the table.
	Export Row	Copies all information in the selected row.
	Export Table	Copies all information in the table.
	Print	Launches the Print dialog box.
	Search	Moves cursor/focus to the Search field on the Product List toolbar.
	Select All	Highlights all rows in the table.
	Size All Columns To Fit	Resizes all columns in the table to fit the contents.
	Expand All	Expands the Product List to display all rows.
	Collapse All	Collapse all rows in the Product List.
	Customize	Launches the Customize Columns dialog box.
DCB		
	Element Manager >	Launches Web Tools.
	Hardware	
	Ports	
	Admin	
	Configuration >	
	Save	
	Save Running to Startup	
	Restore	
	Configuration Repository	
	Schedule Backup	
	Replicate >	
	Configuration	
	Security	
	Enable / Disable >	
	Enable	
	Disable	
	Firmware Management	
	Swap Blades	Only available from chassis.
	DCB	
	FCoE	
	VLAN	
	Zoning	
	Allow / Prohibit Matrix	
	Security >	
	L2 ACL	
	Performance >	
	Real-Time Graph	
	Historical Graph	

Component	Menu/Submenu Commands	Comments
	Fabric Watch > Configure Port Fencing Frame Monitor Performance Thresholds	
	Technical Support > Product / Host SupportSave View Repository	
	Events	
	Port Connectivity	
	Port Optics (SFP)	
	Telnet	
	Telnet through Server	
	Network Objects	Displays the Network Objects view with the selected device highlighted.
	L2 Topology	Displays the L2 Topology view with the selected device highlighted.
	Table > Copy '*Device_Name* Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
VCS/VDX		
	Configuration > Save Restore Configuration Repository Schedule Backup	
	DCB	
	FCoE	
	Security > L2 ACL	
	VLANs	
	Zoning	
	Performance > Real-Time Graph Historical Graph	

Component	Menu/Submenu Commands	Comments
	Fabric Watch > Configure Port Fencing Frame Monitor Performance Thresholds	
	Technical Support > Product / Host SupportSave View Repository	
	Events	
	CLI through Server	
	Setup Tools	
	Network Objects	Displays the Network Objects view with the selected device highlighted.
	L2 Topology	Displays the L2 Topology view with the selected device highlighted.
	Ethernet Fabric	
	Detailed Report	Generates and displays a Detailed Report for the selected device
	Physical Ports Report	Generates and displays a Physical Ports Report for the selected device
	L2 sFlow Report	Generates and displays a Layer 2 sFlow Report for the selected device
	L3 sFlow Report	Generates and displays a Layer 2 sFlow Report for the selected device
	Properties	
	Table > Copy '*Device_Name* Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
Third-party device		
	Network Objects	Displays the Network Objects view with the selected device highlighted.
	L2 Topology	Displays the L2 Topology view with the selected device highlighted.
	Performance > Real-Time Graph / Table Historical Graph / Table	 Launches the **Real-Time Graphs / Tables** dialog box. Launches the **Historical Graphs / Tables** dialog box.
	Events	Displays an Event Log for the device.
	CLI through Server	Launches the device's CLI Element Manager.
	User Defined Menu items	
	Setup Tools	Launches the **Setup Tools** dialog box.
	Detailed Report	Generates and displays a Detailed Report for the selected device

Component	Menu/Submenu Commands	Comments
	Physical Ports Report	Generates and displays a Physical Ports Report for the selected device
	Properties	Displays the Properties dialog box for the selected device.
	Table >	Only available from Product List.
	Copy “Cell_Value”	Copies the information in the selected cell.
	Copy Row	Copies all information in the selected row.
	Copy Table	Copies all information in the table.
	Export Row	Copies all information in the selected row.
	Export Table	Copies all information in the table.
	Print	Launches the Print dialog box.
	Search	Moves cursor/focus to the Search field on the Product List toolbar.
	Select All	Highlights all rows in the table.
	Size All Columns To Fit	Resizes all columns in the table to fit the contents.
	Expand All	Expands the Product List to display all rows.
	Collapse All	Collapse all rows in the Product List.
	Customize	Launches the Customize Columns dialog box.

A IP shortcut menus

Appendix

Call Home Event Tables

B

In this appendix

This appendix provides information about the specific events that display when using Call Home. This information is shown in the following Event Table.

TABLE 118 IP Call Home Event

Event reason code	FRU code/Event type	Description	Severity
N/A	Ethernet	Switch is not reachable.	3
N/A	SW-Missing	Switch is missing from the fabric.	3
199130	IP30	Power supply state changed (snTrapChasPwrSupplyFailed).	1
199131	IP31	Fan failed (snTrapChasFanFailed).	1
199136	IP36	Temperature alert (snTrapTemperatureWarning).	1
1991167	IP167	Stacking power supply failed (snTrapStackingChasPwrSupplyFailed).	1
1991169	IP169	Stacking fan failed (snTrapStackingChasFanFailed).	1
1991171	IP171	Stacking temperature warning (snTrapStackingTemperatureWarning).	1
1991177	IP177	High-speed fans needed for chassis (snTrapChasHighSpeedFansNeeded).	4
1991181	IP181	System memory out threshold (snTrapSysMemoryOutThreshold).	4
19911002	IP1002	IP CAM full (snTrapCAMOverflow).	1
19911004	IP1004	Optical monitoring alarm (snTrapOpticalMonitoringAlarm).	1
19911007	IP1007	POS monitoring alarm (snTrapPosMonitoringAlarm).	1
19911009	IP1009	Optical incompatibility error (snTrapXfpSfpIncompatibleOptic).	1

TABLE 119 Network OS Call Home Event

Event reason code	FRU code/Event type	Description	Severity
N/A	Ethernet	Switch is not reachable.	3
N/A	SW-Missing	Switch is missing from the fabric.	3
1426	FW-1426	Faulty or missing power supply.	3
1427	FW-1427	Faulty power supply.	3
1428	FW-1428	Missing power supply.	3
1430	FW-1430	Faulty temperature sensors.	3

TABLE 119 Network OS Call Home Event (Continued)

Event reason code	FRU code/Event type	Description	Severity
1431	FW-1431	Faulty fans.	3
1432	FW-1432	Faulty WWN cards.	3
1433	FW-1433	Faulty CPs.	3
1434	FW-1434	Faulty blades.	3
1435	FW-1435	Flash usage is out of range.	3

Appendix

Event Categories

C

In this appendix

This section provides information about the events that display in each of the following categories:

Link incident events

The following link incident events indicate FICON link status changes:

- Link RNID device registration
- Link RNID device de-registration
- Link listener added RLIR
- Link listener removed
- Link RLIR failure

Traps that begin with OID 1.3.6.1.4.1.1588.2.1..1.50 are categorized as link incident events.

Product status events

Product status events indicate a change in the status of the product; for example, changes in the state of the port, the field replaceable unit (FRU), the sensor, or the CP.

Traps that begin with any of the following OIDs are categorized as product status events.

- 1.3.6.1.3.94.0.1 [connUnitStatusChange]
- 1.3.6.1.3.94.0.5 [connUnitSensorStatusChange]
- 1.3.6.1.3.94.0.6 [connUnitPortStatusChange]
- 1.3.6.1.4.1.1588.2.1.1.1.0.3 [swFCPortScn]
- 1.3.6.1.4.1.1588.2.1.1.1.0.15 [swDeviceStatusTrap]
- 1.3.6.1.4.1.1588.2.1.2.2.0.1 [fruStatusChanged]
- 1.3.6.1.4.1.1588.2.1.2.2.0.2 [cpStatusChanged]

If the event is a RASLOG and if the RASLOG ID matches any of the RASLOGS listed below, then the event is categorized as a product status event.

- FW-1424
- FW-1425
- FW-1426
- FW-1427
- FW-1428
- FW-1429
- FW-1430
- FW-1431
- FW-1432
- FW-1433
- FW-1434
- FW-1435
- FW-1436
- FW-1437
- FW-1438
- FW-1439
- FW-1440
- FW-1441
- FW-1442
- FW-1443
- FW-1444

Product audit events

Events that are used to track audit information are categorized as product audit events. Audit Syslog messages from HBAs and the messages with the IDs listed below are categorized as product audit events.

- TRCK-1001
- TRCK-1002
- TRCK-1003
- TRCK-1004
- TRCK-1005
- TRCK-1006

Security events

Security events are those that indicate authentication success or failure, a security violation, or user login and logout.

Security events for FC devices

For FOS switches, if the event is a RASLOG event and the RASLOG ID contains 'SEC', then the event is categorized as a security event.

Security events for IP devices

For IOS devices, if the event OID starts with any of the following OIDs, then the event is categorized as a security event.

- 1.3.6.1.2.1.14.16.2.6 [ospfIfAuthFailure]
- 1.3.6.1.2.1.14.16.2.7 [ospfVirtIfAuthFailure]
- 1.3.6.1.4.1.1991.0.9 [snOspfIfAuthFailure]
- 1.3.6.1.4.1.1991.0.10 [snOspfVirtIfAuthFailure]
- 1.3.6.1.4.1.1991.0.75 [snTrapUserLogin]
- 1.3.6.1.4.1.1991.0.76 [snTrapUserLogout]
- 1.3.6.1.4.1.1991.0.77 [snTrapPortSecurityViolation]
- 1.3.6.1.4.1.1991.0.78 [snTrapPortSecurityShutdown]
- 1.3.6.1.4.1.1991.0.85 [snTrapMacAuthEnable]
- 1.3.6.1.4.1.1991.0.86 [snTrapMacAuthDisable]
- 1.3.6.1.4.1.1991.0.87 [snTrapMacAuthMACAccepted]
- 1.3.6.1.4.1.1991.0.88 [snTrapMacAuthMACRejected]
- 1.3.6.1.4.1.1991.0.89 [snTrapMacAuthPortDisabled]
- 1.3.6.1.4.1.1991.0.110 [snTrapClientLoginReject]
- 1.3.6.1.4.1.1991.0.131 [snTrapDot1xSecurityViolation]
- 1.3.6.1.4.1.1991.0.143 [snTrapMacAuthRadiusTimeout]
- 1.3.6.1.4.1.1991.0.144 [snTrapDot1xRadiusTimeout]
- 1.3.6.1.4.1.1991.1.5.1.1.2.1.0.36 [swPortSecurityTrap]
- 1.3.6.1.4.1.1991.1.6.1.1.5.2.3 [sysRadiusServerChanged]
- 1.3.6.1.4.1.1991.1.6.1.1.6.2.3 [sysRadiusServerChanged]
- 1.3.6.1.4.1.1991.1.6.1.7.4.2.3 [dot11StationAuthentication]
- 1.3.6.1.4.1.1991.1.6.1.7.4.2.7 [dot1xMacAddrAuthSuccess]
- 1.3.6.1.4.1.1991.1.6.1.7.4.2.8 [dot1xMacAddrAuthFail]
- 1.3.6.1.4.1.1991.1.6.1.7.4.2.9 [dot1xAuthNotInitiated]
- 1.3.6.1.4.1.1991.1.6.1.7.4.2.10 [dot1xAuthSuccess]
- 1.3.6.1.4.1.1991.1.6.1.7.4.2.11 [dot1xAuthFail]
- 1.3.6.1.4.1.1991.1.6.1.7.4.2.12 [localMacAddrAuthSuccess]

- 1.3.6.1.4.1.1991.1.6.1.7.4.2.13 [localMacAddrAuthFail]
- 1.3.6.1.4.1.1991.1.6.1.7.4.2.14 [pppLogonFail]
- 1.3.6.1.4.1.1991.1.6.1.7.4.2.18 [dot1xSupplicantAuthenticated]
- 1.3.6.1.4.1.1991.1.7.2.2.2.9 [apAuthFailureTooMany]
- 1.3.6.1.4.1.1991.1.8.2.1.4.0.2 [userLoginNotification]
- 1.3.6.1.4.1.1991.1.8.2.1.4.0.3 [userLogOffNotification]
- 1.3.6.1.4.1.1991.1.8.2.1.4.0.4 [userLoginFailNotification]
- 1.3.6.1.4.1.1991.1.11.1.1.2.2.2.32 [mwlAuthFailure]
- 1.3.6.1.4.1.1991.1.11.1.1.2.2.2.33 [mwlRadiusServerSwitchover]
- 1.3.6.1.4.1.1991.1.11.1.1.2.2.2.34 [mwlRadiusServerSwitchoverFailure]
- 1.3.6.1.4.1.1991.1.11.1.1.2.2.2.35 [mwlRadiusServerRestored]
- 1.3.6.1.4.1.1991.1.11.1.1.2.2.2.36 [mwlAcctRadiusServerSwitchover]
- 1.3.6.1.4.1.1991.1.11.1.1.2.2.2.37 [mwlAcctRadiusServerSwitchoverFailure]
- 1.3.6.1.4.1.1991.1.12.1.1.5.100.0.4 [portSecurityViolation]
- 1.3.6.1.4.1.1991.1.12.1.1.5.109.0.1 [portSECViolation]
- 1.3.6.1.4.1.1991.1.12.1.1.111.1.0.3 [unauthorizedAccessViaCLI]
- 1.3.6.1.6.3.1.1.5.5 [authenticationFailure]

User action events

User action events are generated for user actions that are performed through the Management applications, such as:

- User creation
- User deletion
- Event action enable
- Event action disable

These events are usually generated to notify status of configuration or data collection operations initiated by the user from the Management application.

Management server events

Management Server Events are those that are generated by the Management application server, such as:

- Service start and stop
- Memory usage
- Device discovery status
- Asset collection status

These events are usually generated to notify the status of server tasks that are running regularly and periodically.

Product events

All other events originating from the product are categorized as product events.

IP Performance monitoring events

IP performance monitoring events, listed in Table 120, occur when users select the option to forward events to the vCenter during VM Manager discovery.

TABLE 120 Performance monitoring IP threshold events

Trap name	OID	Description
bnaRisingThresholdCrossed	1.3.6.1.4.1.1991.1.13.2.0.1	The value of monitored SNMP variable or expression has exceeded the value specified as the higher threshold.
bnaFallingThresholdCrossed	1.3.6.1.4.1.1991.1.13.2.0.1	The value of the monitored SNMP variable or expression has failed below the value specified as the lower threshold.

Appendix

D

User Privileges

In this appendix

About user privileges

The Management application provides the User Administrator with a high level of control over what functions individual users can see and use. This section describes the effect that each user privilege has on the application when placed in one of the three available configurations: no privilege, read-only, and read/write.

User privilege is the Management application's method of providing role-based access control (RBAC) to the software's user administrator.

In the Management application privileges are assigned to roles and devices are assigned to areas of responsibility (AOR). Privileges and devices are not directly assigned to users; users receive privileges and obtain access to devices from the roles and AORs to which they are assigned. You can assign multiple roles and AORs to a single user.

The following tables define all the privileges in the Management application and the behavior of the application if the privilege is not given, read only, or read/write.

TABLE 121 Application privileges and behavior

Privilege	Description	No Privilege	Read-Only	Read/Write
Active Session Management	Allows you view active client sessions and disconnect an unwanted user.	Disables the **Active Sessions** command from the **Server** menu.	Enables the **Active Sessions** command from the **Server** menu. Disables all commands and functions on the dialog box except the **Close** and **Help**.	Enables the **Active Sessions** command from the **Server** menu. Enables all commands and functions on the dialog box.
Call Home	Allows you to configure call home centers, devices, and event filters.	Disables the **Call Home** command on the **Monitor > Event Notification** menu.	Enables the **Call Home** command on the **Monitor > Event Notification** menu. Enables the **Add**, **Edit**, **Remove**, **Edit Centers**, and **Show/Hide Centers** buttons as well as the **Enabled** check boxes on the dialog box; however, disables the **OK** and **Apply** buttons on the **Call Home**, **Call Home Event Filter**, and **Configure Call Home Center** dialog box boxes.	Enables the **Call Home** command on the **Monitor > Event Notification** menu. Enables all functions in the dialog box.
Certificate Management	Allows you to access the **Certificate Management** dialog box and manage server truststores.	Disables **Certificates** on the **Options** dialog box.	Enables **Certificates** on the **Options** dialog box. Only viewing of the certificates is supported.	Enables **Certificates** on the **Options** dialog box. Enables all functions in the dialog box.
Configuration Management	Allows you to access the **Configuration Management** dialog box and perform configuration upload and replication.	Disables **Save**, **Restore**, **Configuration Repository**, and **Schedule Backup** under **Configure > Switch** and the **Configuration** command under **Configure > Switch > Replicate**.	Enables **Configuration Repository** under **Configure > Switch**. Only viewing of saved configuration is supported. Configuration upload and replication are disabled.	Enables all commands under **Configure > Switch**. Allows you to perform configuration upload, download and restore.
DCB Management	Allows you to configure DCB devices.	Disables the **DCB** command from the **Configure** menu.	Enables the **DCB** command from the **Configure** menu. Disables all commands and functions on the dialog box except the **Close** and **Help**.	Enables the **DCB** command from the **Configure** menu. Enables all commands and functions on the dialog box.
Element Manager	Allows you to access the device element manager.	Disables the Element Manager command.	Enables the Element Manager command. Allows you to open the Element Manager; however, disables all functions.	Enables the Element Manager command. Allows you to perform all Element Manager functions.

TABLE 121 Application privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
Element Manager - Product Administration	An Element Manager privilege that enables most functionally.	Disables the functions described in the Element Manager User Manual for which you do not have rights. Displays the message, "You do not have rights to perform this action."	Same as No Privilege.	Enables the functions described in the Element Manager User Manual.
E-mail Event Notification Setup	Allows you to define the e-mail server used to send e-mail.	Disables **Event Notification E-mail** command on the **Monitor** menu and the E-**mail Event Notification Setup** button in the **Users** dialog box. Disables the **E-mail** option in the Master Log shortcut menu. Currently asks, "Are you sure you want to assign Event Management privileges to this group that does not otherwise have read/write for: E-mail Event Notification Setup?".	Enables the **Event Notification E-mail** command on the **Monitor** menu and the **E-mail Event Notification Setup** button in the **Users** dialog box. Allows you to open the **E-Mail Event Notification Setup** dialog box; however, disables the **OK** button.	Enables **Event Notification E-mail** command on the **Monitor** menu and the **E-mail Event Notification Setup** button in the **Users** dialog box. Enables all functions in the **E-Mail Event Notification Setup** dialog box.
Event Management	Allows you to define rules with event triggers and actions.	Disables the **Event Policies** menu item.	Enables access to the **Event Policies** menu item and allows existing rules to be selected and viewed. Disables all action buttons on the tab.	Enables access to the **Event Policies** menu item and enables all functions on the tab.
Fabric Watch	Fabric Watch — Allows you to launch Fabric Watch. Port Fencing — Allows you to configure the function that logs ports out of fabrics automatically if they are misbehaving. Frame Monitor — Allows you to monitor frames. Performance Thresholds — Allows you to configure performance thresholds.	Disables the **Fabric Watch** command from the **Monitor** menu.	Enables the **Fabric Watch** commands from the **Monitor** menu. DIsables the functions on the **Port Fencing** dialog box. DIsables the functions on the **Frame Monitor** dialog box. DIsables the functions on the **Configure Thresholds** dialog box.	Enables the **Fabric Watch** commands from the **Monitor** menu. Enables you to launch Fabric Watch. Enables all functions on the **Port Fencing** dialog box. Enables all functions on the **Frame Monitor** dialog box. Enables the functions on the **Configure Thresholds** dialog box.

TABLE 121 Application privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
Fault Management	Allows you to control access to the **SNMP Trap Registration and Forwarding** dialog box, the **Event Storage** option of the **Options** dialog box, the **Syslog Registration and Forwarding** dialog box, as well as the **Export** and **Clear** functions in the **Event Log** dialog box and the **Show** and **Hide** functions in the **Customize Columns** dialog box.	Disables the **SNMP Trap** and **Syslog configuration** commands from the **Monitor** menu. Disables the **Event Storage** option on the **Options** dialog box. If you do not have other read/write privileges to **Options** dialog box functions, disables the **Server > Options** command. Enables the **Logs >** *<Log_Type>* from the **Monitor** menu.	Enables the **SNMP Trap** and **Syslog configuration**, commands from the **Monitor** menu. Enables the **Event Storage** option on the **Options** dialog box. Enables the **Server > Options** command. Only enables the **Cancel** function for the dialog box boxes. Enables the **Logs >** *<Log_Type>* from the **Monitor** menu.	Enables the **SNMP Trap** and **Syslog configuration**, commands from the **Monitor** menu. Enables the following functions from the dialog box boxes: • configure Management server registration • configure TRAP or Syslog forwarding • register other servers as a recipient • apply changes Enables the **Server > Options** command. Enables the **Event Storage** option on the **Options** dialog box. Enables the following functions from the dialog box: • configure max events • configure event purging policy • apply changes Enables the following functions from the **Master Log** right-click menu: • Clear events • Show events • Hide events • Export events Note that the **Export** command on the **Master Log** right-click menu also requires the Export privilege because it launches the **Export** dialog box. Enables the **Clear** and **Export** buttons on the individual log dialog box boxes.
FCoE Management	Allows you to configure FCoE devices.	Disables the **FCoE** command from the **Configure** menu.	Enables the **FCoE** command from the **Configure** menu. Disables all commands and functions on the dialog box except the **Close** and **Help**.	Enables the **FCoE** command from the **Configure** menu. Enables all commands and functions on the dialog box.

TABLE 121 Application privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
Firmware Management	Allows you to download firmware to selected switches and manage the firmware repository.	Disables the **Firmware Management** command from the **Configure** menu and right-click menu.	Enables the **Firmware Management** command from the **Configure** menu and right-click menu. Disables all commands and functions on the dialog box except the **Close** and **Help**.	Enables the **Firmware Management** command from the **Configure** menu and right-click menu. Enables all commands and functions on the dialog box.
Host Adapter Management	Allows you to configure a host.	Disables the **Element Manager** command on the right-click menu and the **Element Manager > HCM** command on the **Configure** menu.	Disables the **Element Manager** command on the right-click menu and the **Element Manager > HCM** command on the **Configure** menu.	Enables the **Element Manager** command on the right-click menu and the **Element Manager > HCM** command on the **Configure** menu.
L2 ACL	Allows you to configure a layer 2 access control list.	Disables the **Security > L2 ACL** command on the **Configure** menu.	Enables the **Security > L2 ACL** command on the **Configure** menu. Disables all functions on the dialog box.	Enables the **Security > L2 ACL** command on the **Configure** menu. Enables all functions on the dialog box.
License Update	Allows you to update your license. Allows you to control access to the **License** dialog box from the **Help** menu.	Disables the **License** command on the **Help** menu.	Enables the **License** command on the **Help** menu; however, disables the **Update** and **OK** buttons.	Enables the **License** command on the **Help** menu and enables you to change the license key.
Performance	Allows you to configure the performance subsystem, the display of performance graphs, and threshold settings.	Disables entire **Performance** submenu of the **Monitor** menu as well as the right-click **Performance Graph(s)** command on ports and switch products. Disables the **Port Optics** command on the right-click menu. Disables the **Performance** button in the **DCB Configuration** dialog box.	Enables entire **Performance** submenu off the **Monitor** menu as well as the right-click **Performance Graph(s)** command on ports and switch products. Allows you to open the **Performance Setup** dialog box; however, disables the **OK** button. No changes can be made. Allows you to open the **Performance Graphs** dialog box and enables all controls; however, disables the check boxes under the **Set Thresholds** label on the individual port dialog box (double-click a graph).	Enables entire **Performance** submenu of the **Monitor** menu and the right-click **Performance Graph(s)** command on ports and switch products. Enables changes to the **Performance Setup** dialog box. Allows you to open the **Performance Graphs** dialog box and enables all controls. Enables all functions on the individual port dialog box (double-click a graph). Enables the **Port Optics** command on the right-click menu.

TABLE 121 Application privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
Policy Monitor	Allows you to configure policy monitors.	Disables **Policy Monitor** command on the **Monitor** menu.	Enables **Policy Monitor** command on the **Monitor** menu. Allows you to open the **Policy Monitor** dialog box; however, disables the **Add**, **Delete**, and **Run** buttons. No changes can be made. Enables you to use the **Edit**, **Report**, and **History** buttons to view content.	Enables **Policy Monitor** command on the **Monitor** menu. Allows you to open the **Policy Monitor** dialog box and enables all controls.
Properties Edit	Allows you to edit many director and switch properties.	Enables the **Properties** command on **Edit** menu and right-click menus. Disables edit function (removes green triangles) from editable property fields. Disables the **Names** command on the **Configure** menu.	Enables the **Properties** command on **Edit** menu and right-click menus. Disables edit function (removes green triangles) from editable property fields. Enables the **Names** command on the **Configure** menu; however, disables all edit functions in the dialog box.	Enables **Properties** command on **Edit** menu and right-click menus. Enables editable properties (marked by a green triangle) in the Product List and the Properties Sheets. Enables the **Names** command on the **Configure** menu and enables all functions in the dialog box.
Reports	Allows you to generate and view the following reports: • Fabric Ports • Fabric Summary	Disables the **View** command and the **Generate** command on the **Reports** menu. If this privilege is removed and the Event Management privilege is assigned then this message appears: <title: <Product> Message> <Warning>Removing the Report privilege does not remove users' ability to generate reports in Event Management. You might also want to consider removing the Event Management privilege as well. <<OK>>	Enables the **View** command on the **Reports** menu. Disables the **Generate** command on the **Reports** menu.	Enables the **View** command and the **Generate** command on the **Reports** menu.

TABLE 121 Application privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
Security	Allows you to enable and configure SANtegrity features.	Disables the **Security** command from the **Configure > Switch > Replicate** menu. Disables the **Security Log** command on the **Monitor > Logs** menu. Disables the **Security Misc** command from the **Server > Options** menu.	Disables the **Security** command from the **Configure > Switch > Replicate** menu. Enables the **Security Log** command on the **Monitor > Logs** menu. Enables the **Security Misc** command from the **Server > Options** menu; however, disables the functions.	Enables the **Security** command from the **Configure > Switch > Replicate** menu. Enables the **Security Log** command on the **Monitor > Logs** menu. Enables the **Security Misc** command from the **Server > Options** menu. Enables all functions in the dialog box boxes.
Server Backup	Allows you to control the function that copies (backs up) the application data files to another disk.	Disables the **Backup Now** and **Configure** commands on the Backup icon right-click menu on the application status bar. Disables all controls for Backup on the **Options** dialog box.	Disables the **Configure** command on the Backup icon right-click menu on the application status bar. Disables all controls for Backup on the **Options** dialog box.	Enables the **Backup Now** and **Configure** commands on the Backup icon right-click menu on the application status bar. Enables all functions for Backup on the **Options** dialog box.
Server Software Configuration	Allows you to configure some of the properties of the client and server of the management application.	Disables the **Software Configuration Parameters** folder and subpages in the **Options** dialog box. The configuration cannot be viewed.	Enables the **Software Configuration Parameters** folder and subpages in the **Options** dialog box; however, disables the **OK** and **Apply** buttons when any of the subpages are selected.	Enables the **Software Configuration Parameters** folder and subpages in the **Options** dialog box. Enables all functions when any of those subpages are selected.
Setup Tools	Allows you to define and place commands on product icons and in the **Tools** menu.	Disables the **Setup Tools** command on the **Tools** menu. Any existing **Tools** and/or right-click commands already defined or defined by others are available for use; however, you cannot configure new items. If this privilege is removed and the Event Management privilege is assigned then this message appears: <title: <Product> Message> <Warning>Removing the Log Management privilege does not remove users' ability for Setup Tools in Event Management. You might also want to consider removing the Event Management privilege as well.	Enables the **Setup Tools** command on the Tools menu; however, disables the **OK** button.	Enables the **Setup Tools** command on the **Tools** menu. Enables all functions in the **Setup Tools** dialog box.

TABLE 121 Application privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
Technical Support Data Collection	Allows you to capture support data from Fabric OS switches.	Disables the **SupportSave**, **Upload Failure Data Capture**, and **View Repository** commands from the **Monitor > Technical Support** menu and right-click menu.	Enables the **View Repository** command from the **Monitor > Technical Support** menu and right-click menu. Disables the **SupportSave** and **Upload Failure Data Capture** commands from the **Monitor > Technical Support** menu and right-click menu.	Enables the **SupportSave**, **Upload Failure Data Capture**, and **View Repository** commands from the **Monitor > Technical Support** menu and right-click menu. Enables all functions on the dialog box boxes.
User Management	Allows you to create and define users and groups, as well as assign privileges and views to groups.	Disables the **Users** command on the main **Server** menu and the **Users** button on the main tool bar.	Enables the **Users** command on the **Server** menu and the **Users** button on the main tool bar; however, disables the **Add**, **Edit**, and **Remove Users**, **Add and Remove Groups**, and **OK** buttons on the **Users** dialog box. Enables the **Edit Groups** button to display the **Group** dialog box (with **OK** button disabled).	Enables the **Users** command on the **Server** menu and the **Users** button on the main tool bar. Enables all functions on the **Users** dialog box and the secondary **Group** dialog box.
Virtual Network Management	Allows you to perform VMM based host discovery and management.	Disables the **VM Manager** command on the **Discover** menu.	Enables the **VM Manager** command on the **Discover** menu. Disables all functions on the dialog box.	Enables the **VM Manager** command on the **Discover** menu. Enables all functions on the dialog box.
VLAN Manager	Allows you to manage VLAN Management	Disables the VLAN Manager command.	Enables the VLAN Manager command; however, disables functions on the dialog box.	Enables the VLAN Manager command and all functions on the dialog box.

TABLE 121 Application privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
Web Services	Allows you to use Web Services API.			
Zoning Activation (Fabric and offline zone database) **NOTE** You must also have the Zoning Offline and Zoning Online privileges to launch the **Zoning** dialog box. **NOTE** You must also have the LSAN privilege to launch the **Activate LSAN Zones** dialog box from the **Zone Database (DB)** tab of the **Zoning** dialog box.	Allows you to activate a zone configuration selected in the **Zoning** dialog box.	Disables the **Activate**, **Deactivate**, and **Zoning Policies** buttons in the **Zoning** dialog box.	Enables the **Zoning Policies** button; however, you cannot perform any operations within the **Zoning** dialog box. Disables the **Activate** and **Deactivate** buttons in the **Zoning** dialog box.	Enables the **Activate**, **Deactivate**, and **Zoning Policies** buttons in the **Zoning** dialog box.

TABLE 121 Application privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
Zoning Online **NOTE** You must also have the Zoning Activation privilege to enable the Activate button. **NOTE** You must also have the Zoning g Offline privilege to enable the **Save As** function in the in the **Zoning** and **Compare/Merge** dialog box boxes.	Allows you to edit any of the fabric zone databases in the available fabrics within the **Zoning** dialog box from the client side and then save to the switch.	In **Zoning** dialog box, the **Zone DB** list includes online and offline zones; however, if an online zone is selected, the contents are not loaded into the **Zoning** dialog box. To launch offline zones you must have the Zoning Offline privilege. Disables all zone database editing and switch pushing functions.	In **Zoning** dialog box, the **Zone DB** list includes online and offline zones. If you select an online zone, the contents are loaded into the **Zoning** dialog box. To launch offline zones you must have the Zoning Offline privilege. Disables all online zone database editing, activation, and persisting functions. In **Zoning** dialog box, enables the **Cancel** and **Help** buttons and the **Compare** and **Export** functions in the **Zone DB Operation** list. On the **Zone DB** tab, enables the find buttons. On the **Active Zone Config** tab, enables the **Zone Member Display** list and **Report** button. In the **Compare/Merge** dialog box, enables the **Cancel** and **Help** buttons. In the **Potential Members** table, enables all functions in the right-click menu. In the **Zones** table, enables the **Port Label**, **Search**, and **Properties** (not editable) functions in the right-click menu. In the **Zone Configs** table, enables the **Properties** (not editable) function in the right-click menu.	Enables all functions on the **Zoning** dialog box.

TABLE 121 Application privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
Zoning Offline **NOTE** You must also have the Zoning Activation privilege to enable the Activate button. **NOTE** You must also have the Zoning g Online privilege to enable the **Save to Switch**, **Activate**, **Deactivate**, and **Rollback** functions in the **Zoning** dialog box and the **Save** function in the **Compare/Merge** dialog box.	Allows you to edit the zone database in offline mode and save the zone database to the repository or to the switch.	In **Zoning** dialog box, the **Zone DB** list includes offline zones; however, if an offline zone is selected, the contents are not loaded into the **Zoning** dialog box. Only displays the Fabric Zone DB (if you have the Zoning Online privilege) in the **Zone DB** list. Disables the **Save As** function from **Zone DB Operation** list for Fabric Zone DBs. Disables the **Save To** function on the **Active Zone Config** tab.	In **Zoning** dialog box, the **Zone DB** list includes offline zones. If you select an offline zone, the contents are loaded into the **Zoning** dialog box. Disables all offline zone DB editing, activating, and persisting functions. In **Zoning** dialog box, enables the **Cancel** and **Help** buttons and the **Compare** and **Export** functions in the **Zone DB Operation** list. On the **Zone DB** tab, enables the find buttons. On the **Active Zone Config** tab, enables the **Zone Member Display** list and **Report** button. In the **Compare/Merge** dialog box, enables the **Cancel** and **Help** buttons. In the **Potential Members** table, enables all functions in the right-click menu. In the **Zones** table, enables the **Port Label**, **Search**, and **Properties** (not editable) functions in the right-click menu. In the **Zone Configs** table, enables the **Properties** (not editable) function in the right-click menu.	Enables all functions on the **Zoning** dialog box.

TABLE 121 Application privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
Zoning - LSAN	Allows you to edit and activate LSAN zones for the LSAN fabrics that are available within the **Zoning** dialog box. Prerequisite: Both the backbone fabrics as well as all directly connected edge fabrics must be added to a resource group and a user with LSAN Zoning privilege must be assigned to this specific resource group.	Disables the **Zoning > LSAN Zoning (Device Sharing)** command on the **Configure** menu. In **Zoning** dialog box, the **Zoning Scope** list does not include *LSAN_<FabricName>* as an entry.	Enables the **Zoning > LSAN Zoning (Device Sharing)** command on the **Configure** menu. In **Zoning** dialog box, the **Zoning Scope** list includes LSAN_<FabricName> as an entry, if discovered. If LSAN_<FabricName> is selected, LSAN zone contents are loaded into the **Zoning** dialog box. Disables LSAN zone functions on all dialog box boxes. Disables all online zone database editing, activation, and persisting functions. In **Zoning** dialog box, enables the **Cancel** and **Help** buttons. In the **Potential Members** table, enables all functions in the right-click menu. In the **LSAN Zones** table, enables the **Search** functions in the right-click menu.	Enables all LSAN zone functions on all dialog box boxes.
Zoning - Set Edit Limits	Allows you to set the number of zoning edit operations that can be performed on a fabric zone database before activating a zone configuration.	Disables the **Zoning > Set Edit Limits** command from the **Configure** menu.	Enables the **Zoning > Set Edit Limits** command from the **Configure** menu. Disables all commands and functions on the dialog box except the **Close** and **Help**.	Enables the **Zoning > Set Edit Limits** command from the **Configure** menu. Enables all commands and functions on the dialog box.

TABLE 122 IP privileges and behavior

Privilege	Description	No Privilege	Read-Only	Read/Write
IP - Address Finder	Allows you to use Address Finder. Address Finder finds MAC addresses that are in the forwarding tables at the moment when the search is performed.	Disables the Address Finder command.	Enables the Address Finder command; however, disables functions on the dialog box.	Enables the Address Finder command and all functions on the dialog box.
IP - CLI	Allows you to access the device from Element Manager. For ReadOnly/ReadWrite access to the device CLI.	Disables the Element Manager command.	Enables the Element Manager command; however, disables functions on the dialog box.	Enables the Element Manager command and all functions on the dialog box.
IP - CLI - Port Config	Allows you to access the device from Element Manager. For read-write access to a device CLI to manage specific ports, but not for global configuration of a device.	Disables the Element Manager command.	Enables the Element Manager command; however, disables functions on the dialog box.	Enables the Element Manager command and all functions on the dialog box.
IP - CLI Configuration	Allows you to create device configuration and reports for IP devices	Disables the CLI Configuration command.	Enables the CLI Configuration command; however, disables functions on the dialog box.	Enables the CLI Configuration command and all functions on the dialog box.
IP - CLI Configuration Deploy	Allows you to deploy a CLI configuration.	Disables the Deployment command.	Enables the Deployment command; however, disables function on the dialog box.	Enables the Deployment command and all functions on the dialog box.
IP - Deployment Reports	Allows you to access information about configurations created in device configuration deployments, VLAN deployments, software image backups, CLI Configuration Manager and Configuration Wizard, and configuration backups. These reports are available in case administrators want to know whether a deployment succeeded or failed.	Disables the Report > Deployment command.	Enables the Report > Deployment command; however, disables functions on the dialog box.	Enables the Report > Deployment command and all functions on the dialog box.
IP - Discover Setup	Allows you to discover the IP devices.	Disables the Discover > Setup command.	Enables the Discover > Setup command; however, disables functions on the dialog box.	Enables the Discover > Setup command and all functions on the dialog box.

TABLE 122 IP privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
IP - Element Manager - Port Config	Allows you to access the device from Element Manager. For read-write access to a device Web Management Interface to manage specific ports, but not for global configuration of a device.	Disables the Element Manager - Port Config command.	Enables the Element Manager - Port Config command; however, disables functions on the dialog box.	Enables the Element Manager - Port Config command and all functions on the dialog box.
IP - GSLB Manager	Allows you to create GSLB policies for Application products.	Disables the GSLB command.	Enables the GSLB command; however, disables functions on the dialog box.	Enables the GSLB command and all functions on the dialog box.
IP - L3 ACL	Allows you to configure a layer 3 access control list.	Disables the **Security > L3 ACL** command on the **Configure** menu.	Enables the **Security > L3 ACL** command on the **Configure** menu. Disables all functions on the dialog box.	Enables the **Security > L3 ACL** command on the **Configure** menu. Enables all functions on the dialog box.
IP - MAC Filter	Allows you to configure a media access control filter.	Disables the **Security > MAC Filter** command on the **Configure** menu.	Enables the **Security > MAC Filter** command on the **Configure** menu. Disables all functions on the dialog box.	Enables the **Security > MAC Filter** command on the **Configure** menu. Enables all functions on the dialog box.
IP - Main Display - Ethernet Fabric	Allows you to display the topology for the Ethernet Fabric network view.	Disables the Ethernet Fabric topology.	Enables the Ethernet Fabric topology; however, disables functions on the topology.	Enables the Ethernet Fabric topology and all functions on the topology.
IP - Main Display - IP	Allows you to display the topology for the IP network view.	Disables the IP topology.	Enables the IP topology; however, disables functions on the topology.	Enables the IP topology and all functions on the topology.
IP - Main Display - L2	Allows you to display the topology map for Layer 2. The Layer 2 Topology map displays connectivity for all IOS devices on the network.	Disables the L2 topology.	Enables the L2 topology; however, disables functions on the topology.	Enables the L2 topology and all functions on the topology
IP - Main Display - MRP	Allows you to display the topology for MRP rings.	Disables the MRP Topology command.	Enables the MRP Topology command; however, disables functions on the topology.	Enables the MRP Topology command and all functions on the topology.
IP - Main Display - VLAN	Allows you to display topologies for VLANs.	Disables the VLAN topology.	Enables the VLAN topology; however, disables functions on the topology.	Enables the VLAN topology and all functions on the topology.
IP - MPLS - VCID Pool	Allows you to create a pool of VCIDs which are used when creating new VLL and VPLS instances.	Disables the MPLS command.	Enables the MPLS command; however, disables functions on the dialog box.	Enables the MPLS command and all VCID Pool functions on the dialog box.

TABLE 122 IP privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
IP - MPLS - VLL	Allows you to manage VLL configurations.	Disables the MPLS command.	Enables the MPLS command; however, disables functions on the dialog box.	Enables the MPLS command and all VLL functions on the dialog box.
IP - MPLS - VPLS	Allows you to manage VPLS configurations	Disables the MPLS command.	Enables the MPLS command; however, disables functions on the dialog box.	Enables the MPLS command and all VPLS functions on the dialog box.
IP - MPLS- LSP	Allows you to manage LSP and LSP Topology	Disables the MPLS command.	Enables the MPLS command; however, disables functions on the dialog box.	Enables the MPLS command and all LSP functions on the dialog box.
IP - Port Profile Edit	Allows you to configure ports on VDX devices. **NOTE:** Ethernet Fabrics must be enabled in the Management application to view the **Port Profile** tab.	Disables the Add and Delete commands on the **Port Profiles** tab of the **Properties** dialog box.	Disables the Add and Delete commands on the **Port Profiles** tab of the **Properties** dialog box.	Enables the Add and Delete commands on the **Port Profiles** tab of the **Properties** dialog box.
IP - Power Management	Allows you monitor PoE-capable products.	Disables the Power Center command.	Enables the Power Center command; however, disables functions on the dialog box.	Enables the Power Center command and all functions on the dialog box.
IP - Reload Product	Allows you to save the configuration to the device flash memory and reboot the device.	Disables the Configuration Repository command.	Enables the Configuration Repository command; however, disables functions on the dialog box.	Enables the Configuration Repository command and all functions on the dialog box.
IP - SSL Certificate Manager	Allows you to manage SSL Certificate and Key for L4-7 SSL capable product	Disables the SSL Certificate command.	Enables the SSL Certificate command; however, disables functions on the dialog box.	Enables the SSL Certificate command and all functions on the dialog box.
IP - VIP-Server Mgr (Real Server Port View)	Allows you to manage VIP Server View using the Real Server Port View	Disables the VIP Server command.	Enables the VIP Server command; however, disables functions on the dialog box.	Enables the VIP Server command and all Real Server Port View functions on the dialog box.
IP - VIP-Server Mgr (Virtual Server Port View)	Allows you to manage VIP Server View using the Virtual Server Port View	Disables the VIP Server command.	Enables the VIP Server command; however, disables functions on the dialog box.	Enables the VIP Server command and all Virtual Server Port View functions on the dialog box.
IP - VIP-Server Mgr (Real Server View)	Allows you to manage VIP Server View using the Real Server View	Disables the VIP Server command.	Enables the VIP Server command; however, disables functions on the dialog box.	Enables the VIP Server command and all Real Server View functions on the dialog box.

TABLE 122 IP privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
IP - VIP-Server Mgr Leaf Node (Real Server Port View)	Allows you to manage VIP Server using the Real Server Port View. When assigned to user as Read-Write privilege, only leaf node can be disabled/enable	Disables the VIP Server command.	Enables the VIP Server command; however, disables functions on the dialog box.	Enables the VIP Server command and all Real Server Port View functions on the dialog box.
IP - VIP-Server Mgr Leaf Node (Virtual Server Port View)	Allows you to manage VIP Server using the Virtual Server Port View. When assigned to user as Read-Write privilege, only leaf node can be disabled/enable	Disables the VIP Server command.	Enables the VIP Server command; however, disables functions on the dialog box.	Enables the VIP Server command and all Virtual Server Port View functions on the dialog box.
IP - VIP-Server Mgr Leaf Node (Real Server View)	Allows you to manage VIP Server using the Real Server View. When assigned to user as Read-Write privilege, only leaf node can be disabled/enable.	Disables the VIP Server command.	Enables the VIP Server command; however, disables functions on the dialog box.	Enables the VIP Server command and all Real Server View functions on the dialog box.

About Roles and Access Levels

The Management application provides preconfigured roles (IP Administrator, Report User Group, and Network Administrator); however, the IP Administrator can also create roles manually (refer to "Creating a new role" on page 191 for instructions.)

TABLE 123 Application Features and Role Access Levels

Feature	Roles with Read/Write Access	Roles with Read-Only Access
Active Session Management	IP System Administrator, Security Officer	Operator
Call Home	IP System Administrator, Operator	
Certificate Management	IP System Administrator, Network Administrator, Host Administrator, Security Administrator	Operator
Configuration Management	IP System Administrator, Network Administrator	Operator
DCB Management	SAN System Administrator, Network Administrator	Security Administrator, Security Officer
E-mail Event Notification Setup	IP System Administrator, Operator	
Element Manager	IP System Administrator,	

TABLE 123 Application Features and Role Access Levels (Continued)

Feature	Roles with Read/Write Access	Roles with Read-Only Access
Element Manager - Product Administration	IP System Administrator,	
Event Management	IP System Administrator, Network Administrator	Operator
Fabric Watch	IP System Administrator,	
Fault Management	IP System Administrator, Network Administrator	Operator
FCoE Management	SAN System Administrator, Network Administrator	Security Administrator, Zone Administrator, Security Officer, Operator
Firmware Management	IP System Administrator, Network Administrator	Operator
Host Adapter Management	SAN System Administrator, Security Officer, Host Administrator	Operator
L2 ACL	IP System Administrator, Security Administrator	
License Update	IP System Administrator	Operator
Performance	IP System Administrator, Host Administrator, Network Administrator	Operator
Properties Edit	IP System Administrator, Host Administrator	Operator
Reports	IP System Administrator, Report User Group, Network Administrator	Operator
Security	IP System Administrator, Security Administrator, Security Officer, Host Administrator	Operator
Server Backup	IP System Administrator, Product Administrator, Operator	
Server Software Configuration	IP System Administrator	Operator
Setup Tools	IP System Administrator	Operator
Technical Support Data Collection	IP System Administrator	Operator
User Management	IP System Administrator, Security Officer	Operator
Virtual Network Management	IP System Administrator	Operator
VLAN Manager	IP System Administrator	Operator
Web Services	IP System Administrator	Operator
Zoning - LSAN	IP System Administrator, Zone Administrator	Operator
Zoning Set Edit Limits	IP System Administrator	Zone Administrator, Operator
Zoning Activation	IP System Administrator, Zone Administrator	Operator
Zoning Offline	IP System Administrator, Zone Administrator	Operator
Zoning Online	IP System Administrator, Zone Administrator	Operator

TABLE 124 IP Features and Role Access Levels

Feature	Roles with Read/Write Access	Roles with Read-Only Access
IP - Address Finder	IP System Administrator, Network Administrator	
IP - CLI	IP System Administrator	
IP - CLI Configuration	IP System Administrator, Network Administrator	
IP - CLI - Port Config	IP System Administrator	
IP - Deployment Reports	IP System Administrator, Report User Group, Network Administrator	
IP - Discover Setup	IP System Administrator	
IP - Element Manager - Port Config	IP System Administrator	
IP - GSLB Manager	IP System Administrator, Network Administrator	
IP - L3 ACL	IP System Administrator, Security Administrator	
IP - MAC Filter	IP System Administrator, Security Administrator	
IP - Server Mgr (Real Server View)	IP System Administrator	
IP - Main Display - IP	IP System Administrator, Network Administrator	
IP - Main Display - L2	IP System Administrator, Network Administrator	
IP - Main Display - MRP	IP System Administrator, Network Administrator	
IP - Main Display - VLAN	IP System Administrator, Network Administrator	
IP - MPLS - LSP	IP System Administrator	
IP - MPLS - VCID Pool	IP System Administrator	
IP - MPLS - VLL	IP System Administrator	
IP - MPLS - VPLS	IP System Administrator	
IP - Power Management	IP System Administrator	
IP - Reload Product	IP System Administrator, Network Administrator	
IP - SSL Certificate Manager	IP System Administrator, Network Administrator	
IP - VIP-Server Mgr (Real Server Port View)	IP System Administrator, Network Administrator	
IP - VIP-Server Mgr (Virtual Server Port View)	IP System Administrator, Network Administrator	
IP - VIP-Server Mgr Leaf Node (Real Server View)	IP System Administrator, Network Administrator	
IP - VIP-Server Mgr Leaf Node (Real Server Port View)	IP System Administrator, Network Administrator	
IP - VIP-Server Mgr Leaf Node (Virtual Server Port View)	IP System Administrator, Network Administrator	

Appendix

Device Properties

E

In this appendix

Viewing SAN device properties

NOTE
Only available for Fabric OS products.

You can customize the device and fabric **Properties** dialog boxes to display only the data you need by creating user-defined property labels. You can also edit property fields to change information.

Viewing Fabric properties

To view the properties for a fabric, complete the following step.

1. Right-click any fabric and select **Properties**.

   The *Fabric_Name* **Properties** dialog box displays, with information related to the selected fabric.

   To add user-defined property labels, refer to "Adding a property field" on page 1329.

   Fields containing a green triangle ( ) in the lower right corner are editable.

TABLE 125 Fabric properties

Field/Component	Description
Name	The name specified through the switch Element Manager.
FID Fabric Name	Enter a name for the fabric (up to 128 characters). Supported on seed switches running Fabric OS 7.0 or later.
Seed Switch	The IP address of the seed switch.
AD Enabled	Whether admin domain is enabled on the switch or not.
Status	The operational status.
Switch and AG Count	The number of switches and Access Gateway's in the fabric.
Description	A description of the customer site.
Principal Switch	The IP address of the principal switch.

TABLE 125 Fabric properties

Field/Component	Description
Active Zone Configuration	Whether active zone configuration is activated on the fabric.
Last Discovery	The date and time of last discovery.
Tracked	Whether the fabric is tracked.
Location	The customer site location.
Contact	The primary contact at the customer site.
Add button	Click to add a user-defined property. For more information, refer to "Adding a property field" on page 1329.
Edit button	Click to edit a user-defined property. For more information, refer to "Editing a property field" on page 1330.
Delete button	Click to delete a user-defined property. For more information, refer to "Deleting a property field" on page 1330.

2. Click **OK** on the *Fabric_Name* **Properties** dialog box to close.

Viewing SAN device properties

To view the properties for a device, complete the following steps.

1. Right-click any product icon and select **Properties**.

   The **Properties** dialog box displays, with information related to the selected device (such as, switches, directors, HBAs, trunks, tunnels, and nodes).

   To add user-defined property labels, refer to "Adding a property field" on page 1329.

   Fields containing a green triangle ( ) in the lower right corner are editable.

   Depending on the device type, some of the properties listed in the following table may not be available for all products.

TABLE 126 Device properties

Field/Component	Description
Addressing Mode	The addressing mode of the switch.
Bandwidth	The bandwidth of the FCIP tunnel.
Capability	The node capability.
Compression	Whether compression is On or Off for the FCIP tunnel.
Connected Virtual FCoE Port	The fabric name, switch name, and virtual FCoE port number of the connected virtual FCoE port.
Contact	The primary contact at the customer site.
Contributors	The device contributors.
Device Type	Whether the device is an initiator or target.
Description	A description of the customer site.
Destination IP Address	The IP address of the of the FCIP tunnel destination device.

TABLE 126 Device properties (Continued)

Field/Component	Description
Discovery Status	The discovery status of the switch. Examples include 'Discovered: Seed Switch' and 'Discovered: Not Reachable'.
Domain ID	The device's domain ID, which is the top-level addressing hierarchy of the domain.
Fabric	The fabric name.
Fabric Name	The name specified through the device Element Manager.
Fabric Watch	Whether Fabric Watch is up or down.
Factory Serial Number	The factory serial number.
Fastwrite	Whether fastwrite is On or Off for the FCIP tunnel.
FC Port	The FC port of the FCIP tunnel.
FCoE Capable	Whether the device is Fibre Channel over Ethernet capable.
FCS Role	Whether FCS is supported.
Firmware	The firmware version.
GigE Port	The GigE port of the FCIP tunnel.
Host Name	The Host name.
IKE Policy #	The IKE policy number. Also includes the following information: • Authentication Algorithm • Encryption Algorithm • Diffie-Hellman • SA Life
IP Address	The device's IP address.
IPSec Policy #	The IPSec policy number. Also includes the following information: • Authentication Algorithm • Encryption Algorithm • SA Life
L2 Capable	Whether the device is Layer 2 capable.
L3 Capable	Whether the device is Layer 3 capable.
L2 Mode	The Layer 2 mode. Options include Access, Converged, or Trunk.
LAG ID	The link aggregation group identifier.
Last Discovery	The date and time of the last discovery.
Location	The customer site location.
MAC address	In a network, the Media Access Control (MAC) address is a unique number that identifies a specific hardware interface. It is a 12-digit hexadecimal number.
Managed By	The management program used to manage the fabric.
Master Port	The master port of the trunk.
Member Ports	The member ports of the trunk.
Model	The model number of the device.
Name	The user-defined name of the switch.

TABLE 126 Device properties (Continued)

Field/Component	Description
Node Name	The name of the node.
Node WWN	The world wide name of the node.
Physical/Logical	Whether the device is a physical device or a logical device.
Port Count	The number of ports.
Port Type	The port type.
Preshared key configured	Whether the preshared key is configured for the FCIP tunnel.
Reason	The device status.
Remote Switch Name	The remote switch name of the trunk.
Remote Switch IP	The remote switch IP address of the trunk.
Remote Switch WWN	The remote switch world wide name of the trunk.
Remote Slot #	The remote slot number of the trunk.
Remote Master Port	The remote master port of the trunk.
Remote Member Ports	The remote member port of the trunk.
Sequence number	The sequence number of the switch.
Serial #	The hardware serial number.
Slot #	The slot number of the trunk.
Source IP Address	The IP address of the of the FCIP tunnel source device.
Speed (Gb/s)	The speed of the port in gigabytes per second.
State	The device's state, for example, online or offline.
Status	The operational status.
Switch Name	The switch name.
Switch IP	The switch IP address.
Switch WWN	The switch world wide name.
Tape Pipelining	Whether tape pipelining is On or Off for the FCIP tunnel.
Tunnel ID	The tunnel identifier.
Type	The device type.
Unit Type	The unit type of the node.
Vendor	The product vendor.
# Virtual FCoE port count	The number of virtual FCoE ports on the device. There is a one-to-one mapping of TE ports to virtual FCoE ports. Therefore, the number of virtual session ports is one for directly connected devices.
VLAN #	The VLAN number of the FCIP tunnel.
VLAN Class of Service for Control Connection	The VLAN class of service for the control connection of the FCIP tunnel.
VLAN Class of Service for Data Connection	The VLAN class of service for the data connection of the FCIP tunnel.
VLAN ID	The VLAN identification number.

TABLE 126 Device properties (Continued)

Field/Component	Description
WWN	The world wide name of the device.
Add button	Click to add a user-defined property. For more information, refer to "Adding a property field" on page 1329.
Edit button	Click to edit a user-defined property. For more information, refer to "Editing a property field" on page 1330.
Delete button	Click to delete a user-defined property. For more information, refer to "Deleting a property field" on page 1330.

2. To view port properties, select one of the following tabs:

   The following port types are available depending on the selected device:

   - FC Ports
   - GigE Ports
   - IP Ports
   - iSCSI Ports
   - Virtual Sessions Ports
   - Virtual FCoE Ports
   - Virtual Machine Ports

3. If you selected the FC Ports tab, select the port type.

   - FC
   - ICL
   - GigE

   For a description of the port properties, refer to "Port properties" on page 1310.

4. Click **OK** on the **Properties** dialog box to close.

Viewing Storage properties

NOTE
Only available for Fabric OS products.

The **Storage Properties** dialog box displays information related to a selected storage device. To view the properties for a storage device, complete the following steps.

1. Select a storage icon.
2. Select **Edit > Properties**.

   The **Properties** dialog box displays.

3. Click the **Storage** tab.

NOTE
Some fields may not be available for all products.

Field	Description
(**Status**)	Lists two kinds of data: the LUN's health and the state of the LUN's disks. The colored icon in the lower-left corner indicates the LUN's health. In most cases, there is also a number that represents the RAID type. The possible RAID types are 0, 1, 5, or 10, and the number does not display if the RAID type is different from those. The following are examples of generic LUN status icons: **Normal.** All disks are operating normally and online. **Transitioning.** One or more disks are in a transitioning state. For example, rebuilding or binding. RAID type is 1 in this case. **Faulted/Offline.** One or mores disks is offline or faulted. RAID type is 10 in this case. **Unknown.** Status is not available.
Array	A group of disks designated by the user to be managed by the RAID-5 technique.
Assigned LUNs (Count)	All LUNs assigned (masked) to host ports that currently exist on this storage device.
Assigned LUNs (Size GB)	The total amount of storage space carved into LUNs and assigned (masked) to host ports on the storage device.
Block Size (B)	The size of the individual blocks on the disk, in bytes.
Device Adapter	(IBM ESS products only) Displays one of eight ESS product adapters deployed in pairs, one for each cluster that provides communication between the cluster and storage products.
Disks	The number of disks across which this LUN is striped.
Free LUNs (Count)	All LUNs NOT assigned (masked) to any host ports (available) that currently exist on this storage device.
Free LUNs (Size GB)	The total amount of storage space carved into LUNs but NOT assigned (masked) to host ports on the storage device, in gigabytes.
Free Space (Count)	The number of contiguous free space instances not yet carved into LUNs (available to be carved) on the storage device. Typically, there is one free space for each disk group on a storage device.
Free Space (Size GB)	The total amount of storage space not carved into a LUN (available for new LUNs) on the storage device, in gigabytes.
Hosts Assigned	The number of hosts to which this LUN has been assigned.
Host Spares	The number of disks assigned as host spares in addition to the disks that make up the LUN.
Label	A user-specified label. The default value is the name of the label as specified in the storage product.
Loop	(IBM ESS products only) The physical connection between a pair of product adapters in the ESS product.
LSS ID	Specifies the logical subsystem of an IBM ESS product.
LUN Name	The name of the LUN.
LUN Status	The LUN status (online or offline).
Management Link	The management link status (Up/Down) of the product.
Model #	The model number of the product.
Name (in-band)	The name of the in-band product.

Field	Description
Operational Status	The operational status of the product.
OS Type	The operating system.
Protocol	The LUN protocol.
Size (GB)	The total size of this LUN's storage, in gigabytes.
State	The state of the LUN.
Storage LUN ID	The storage product's LUN ID number for this LUN.
Storage Ports	The total number of storage ports assigned to the server or the port, or bound to the LUN.
Type	The level or type of RAID storage. Possible values are as follows: • **0.** Striped disk array without fault tolerance. • **1.** Mirroring and duplexing. • **2.** Hamming code ECC. • **3.** Parallel transfer with parity. • **4.** Independent data disks with shared parity disk. • **5.** Independent data disks with distributed parity blocks. • **6.** Independent data disks with two independent distributed parity schemes. • **7.** Optimized asynchrony for high I/O rates as well as high data transfer rates. • **10.** Very high reliability combined with high performance. • **53.** High I/O rates and data transfer performance. • **0+1.** High data transfer performance.
Total (Count)	All LUNs, whether assigned or not, that currently exist on this storage device.
Total (Size GB)	The total amount of storage space on the storage device, in gigabytes.
Unique LUN ID	Identifies the unique LUN identifier.
Volume State	The volume state of the LUN.
Add button	Click to add a user-defined property. For more information, refer to "Adding a property field" on page 1329.
Edit button	Click to edit a user-defined property. For more information, refer to "Editing a property field" on page 1330.
Delete button	Click to delete a user-defined property. For more information, refer to "Deleting a property field" on page 1330.

4. Click **OK** on the **Properties** dialog box to close.

Viewing iSCSI Properties dialog box

NOTE
Only available for Fabric OS products.

The **iSCSI Properties** dialog box displays information related to iSCSI. To view the properties for an iSCSI device, complete the following steps.

1. Right-click a product icon and select **Properties** .

   The **Properties** dialog box displays.

2. Select the **iSCSI** tab.

NOTE
Some fields may not be available for all products.

Field	Description
Agent	The Caffeine agent version number.
Applications	The applications.
Assigned LUNs	The number of unique LUNs (not LUN paths) masked to this host.
Assigned LUNs Size (GB)	The total size of the unique LUNs (not LUN paths) in gigabytes.
Command Descriptor Block Count	The number of command descriptor blocks on the product.
Comments	Comments regarding the product.
Contact	A contact for the product.
Department	The department.
Description	A description of the product.
Device Type	The product type.
Digest Error Count	The number of digest errors on the product.
Driver	The iSCSI driver.
Driver Version	The iSCSI driver version.
Firmware	The firmware for the product.
Group	The name of the portal group.
Initiator Type	The type of initiator (such as, HBA or Software).
Interface	The name of the interface.
IP Address	The product's IP address.
iSCSI Alias	The name of the alias target.
iSCSI Node Name	The node name of the product.
iSCSI Node Type	The node type of the product.
iSCSI Service	The service status; for example, running or not running.
iSNS IP Address	The IP address of the server to which the product is pointed.
ISNS IP Address	A list of the iSNS IP addresses this product has been assigned by the user to query.
iSNS Service	Whether the product is registered with an iSNS server.
Location	The location of the product.
Management Link	The management link status (Up/Down) of the product.
Name (Product)	The name of the product.
OS	The name of the operating system running on the product.
OS Build	The operating system build running on the product.

Field	Description
OS Release	The operating system release running on the product.
Portal Addresses	The list of IP addresses.
Port	The port number.
Protocol Error Count	The number of protocol errors.
Tag	The group tag ID of the portal.
Sessions button	Select to display the **Filer Sessions** dialog box for the product.
Statistics button	Select to display the **Filer iSCSI Statistics** dialog box for the product.
Storage Arrays	The number of arrays containing LUNs masked to the server.
Storage Logins	The number of unique filers to which hosts on this server are logged in.
Target Portals table	Target portals of the product.
Total LUN Size (GB)	The size in gigabytes (GB) of all unique LUNs (not LUN paths) masked to the product.
Vendor	The vendor of the product.

3. Click **OK** on the **Properties** dialog box to close.

Viewing port properties

NOTE
Only available for Fabric OS products.

The following port types are available depending on the device:

- FC Ports
- GigE Ports
- IP Ports
- iSCSI Ports

  NOTE
  iSCSI ports that have an FC Address of all zeros are inactive. All others are active.

- Virtual Sessions Ports
- Virtual FCoE Ports

To view a port's properties, right-click on a port and select **Properties**, or double-click the port.

The port **Properties** dialog box displays (Figure 518).

To add user-defined property labels, refer to "Adding a property field" on page 1329.

Fields containing a green triangle ( ) in the lower right corner are editable.

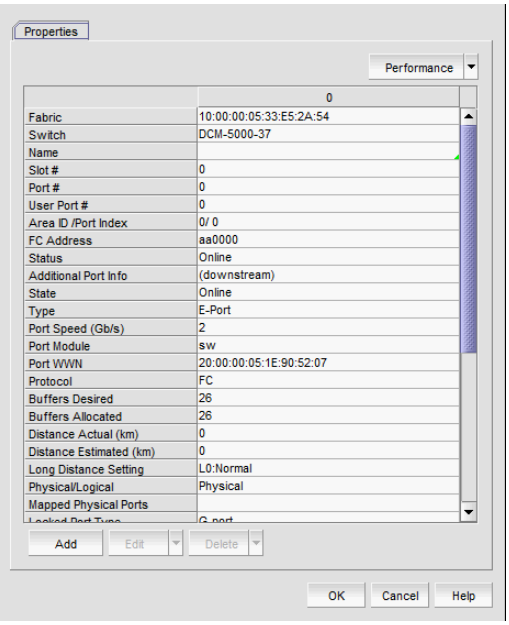


FIGURE 518 Port Properties dialog box

NOTE
Depending on the port type, some of the following properties may not be available for all products.

TABLE 127 Port properties

Field	Description
Additional Port Info	Additional error information relating to the selected port.
Address	The address of the port.
Addressing Mode	The addressing mode of the switch.
Active FC4 Types	The active FC4 types.
Active Tunnels	The number of active tunnels.
Area ID (hex)/Port Index (hex)	The area identifier, in hexadecimal, of the switch-to-product connection.
Associated GE Port	The port number of the associated GE port.
Attached Port #	The port number of the attached product.
Back to Edge Routing Support	Whether back to edge routing is supported.
Bandwidth	The bandwidth of the FCIP tunnel.
Blocked	The configuration of the switch (blocked or unblocked).
Bottleneck Status	Whether the port is bottlenecked or not.
Buffers Desired	The number of buffers desired but not allocated.
Buffers Allocated	The number of buffers allocated.
Capability	The node capability.
Class	The class of the port.
Class of Service	The class of service.

TABLE 127 Port properties (Continued)

Field	Description
Compression	Whether compression is enabled or disabled.
Connected Devices	The number of connected devices. Click the icon in the right side of the field to open the **Virtual FCoE Port <Number> Connected Devices** dialog box.
Connected Switch	The name of the connected switch.
Delete button	Click to delete.
Description	A description of the customer site.
Destination IP Address	The IP address of the of the FCIP tunnel destination device.
Device Type	Whether the device is an initiator or target.
Discovery Status	The discovery status of the switch. Examples include 'Discovered: Seed Switch' and 'Discovered: Not Reachable'.
Distance Actual (km)	The actual distance (in km) for -end port connectivity.
Distance Estimated (km)	The estimated distance (in km) for -end port connectivity.
Domain ID	The device's domain ID, which is the top-level addressing hierarchy of the domain.
Encryption	Whether encryption is enabled or disabled.
Fabric	The fabric's IP address.
Fabric Name	The name of the fabric.
Fabric Watch	Whether Fabric Watch is up or down.
Fastwrite	Whether fastwrite is On or Off for the FCIP tunnel.
FC Port	The FC port of the FCIP tunnel.
FC Port Count	The number of FC ports on the device.
FCIP Capable	Whether the port is FCIP capable.
FCoE Capable	Whether the device is Fibre Channel over Ethernet capable.
FCS Role	Whether FCS is supported.
Flag (FICON related)	Whether a flag is on or off.
Firmware	The firmware version.
Forward Error Correction (FEC)	Whether FEC is enabled or disabled.
GigE Port	The GigE port of the FCIP tunnel.
GigE Port Count	The number of GigE ports on the device.
Host Name	The Host name.
IKE Policy #	The IKE policy number. Also includes the following information: • Authentication Algorithm • Encryption Algorithm • Diffie-Hellman • SA Life
Inband Management Status	The inband management status (online or offline).
Index	The index of the Virtual FCoE Port.
Interface Count	The interface count.

TABLE 127 Port properties (Continued)

Field	Description
IP Address	The device's IP address.
IPSec Policy #	The IPSec policy number. Also includes the following information: • Authentication Algorithm • Encryption Algorithm • SA Life
iSCSI button	Click to launch the Element Manager.
iSCSI Capable	Whether the port is iSCSI capable or not.
L2 Capable	Whether the device is Layer 2 capable.
L3 Capable	Whether the device is Layer 3 capable.
L2 Mode	The Layer 2 mode. Options include Access, Converged, or Trunk.
LAG ID	The link aggregation group identifier.
Last Discovery	The date and time of the last discovery.
Location	The customer site location.
Locked Port Type	The port type of the locked product.
Long Distance Setting	Whether the connection is considered to be normal or longer distance.
MAC Address	The Media Access Control address assigned to a network adapters or network interface cards (NICs).
Managed By	The management program used to manage the fabric.
Manufacturer Plant	The name of the manufacturer plant.
Master Port	The master port of the trunk.
Member Ports	The member ports of the trunk.
Model	The model number of the device.
Modify button	Click to launch the Element Manager.
Name	The name of the port (up to 128 characters). This field is editable.
Node Name	The name of the node.
Node WWN	The world wide name of the node.
Performance list	Select to launch the dialog box of one of the following performance options: • Real Time Graph • HIstorical Graph • HIstorical Report
Physical/Logical	Whether the port is a physical port or a logical port.
Port #	The number of the port.
Port Address	The address of the port.
Port Count	The number of ports.
Port ID	The identifier of the port.
Port Module	The port's module.
Port NPIV	Number of NPIV ports.

TABLE 127 Port properties (Continued)

Field	Description
Port Speed (Gb/s)	The port speed, in Gbits per second.
Port State	The port state (online or offline).
Port Status	The port's operational status (online or offline).
Port Type	The port type.
Port WWN	The port's world wide name.
Preshared key configured	Whether the preshared key is configured for the FCIP tunnel.
Prohibited	Whether the port is prohibited.
Protocol	The network protocol, for example, Fibre Channel.
Reason	The device status.
Remote Switch Name	The remote switch name of the trunk.
Remote Switch IP	The remote switch IP address of the trunk.
Remote Switch WWN	The remote switch world wide name of the trunk.
Remote Slot #	The remote slot number of the trunk.
Remote Master Port	The remote master port of the trunk.
Remote Member Ports	The remote member port of the trunk.
Sequence number	The sequence number of the switch.
Serial #	The hardware serial number.
Slot #	The location (slot) of the port.
Source IP Address	The IP address of the of the FCIP tunnel source device.
Speed (Gb/s)	The port speed, in Gbits per second.
State	The port state (online or offline).
Status	The port's operational status (online or offline).
Switch Name	The switch name.
Switch IP	The switch IP address.
Switch WWN	The switch world wide name.
Symbolic Name	The symbolic name of the port.
Tag	The tag number of the port.
Tape Pipelining	Whether tape pipelining is On or Off for the FCIP tunnel.
Troubleshooting list	Select to launch the dialog box of one of the following troubleshooting options: • IP Ping • IP Traceroute • IP Performance
Tunnel Count	The number of tunnels.
Tunnel ID	The tunnel identifier.
Type	The type of port, for example, U_port.
Unit Type	The unit type of the node.

TABLE 127 Port properties (Continued)

Field	Description
User Port #	The number of the user port.
Vendor	The product vendor.
# Virtual FCoE port count	The number of virtual FCoE ports on the device. There is a one-to-one mapping of TE ports to virtual FCoE ports. Therefore, the number of virtual session ports is one for directly connected devices.
# Virtual Session Ports	The number of virtual session ports associated with the GE port.
VLAN #	The VLAN number of the FCIP tunnel.
VLAN Class of Service for Control Connection	The VLAN class of service for the control connection of the FCIP tunnel.
VLAN Class of Service for Data Connection	The VLAN class of service for the data connection of the FCIP tunnel.
VLAN ID	The VLAN identification number.
WWN	The world wide name of the device.
Add button	Click to add a user-defined property. For more information, refer to "Adding a property field" on page 1329.
Edit button	Click to edit a user-defined property. For more information, refer to "Editing a property field" on page 1330.
Delete button	Click to delete a user-defined property. For more information, refer to "Deleting a property field" on page 1330.

IP device properties

You can view device and port properties from any view in the IP Topology.

You can customize the device and fabric **Properties** dialog boxes to display only the data you need by creating user-defined property labels (refer to "Adding a property field" on page 1329).

You can also edit property fields to change information. Fields containing a green triangle ( ) in the lower right corner are editable.

Viewing IP device and port properties

To view properties for a device, complete the following steps.

1. Select one of the following view types from the view list on the Product List toolbar.
   - Network Object
   - IP Topology
   - L2 Topology
   - Ethernet Fabrics (refer to "Viewing VCS fabric properties" on page 1319)
   - VLAN Topology
2. Right-click the device in the Product List and select **Properties**.

The *Device_Name* **Properties** dialog box displays.

3. Review the device and port properties.

   To add user-defined property labels, refer to "Adding a property field" on page 1329.

   Fields containing a green triangle ( ) in the lower right corner are editable.

NOTE
Some fields are not available for all products.

Field/Component	Description
Properties tab	Select to display information about the device.
Detailed Report button	Click to launch the detailed product report.
Name	The name of the product.
Alias	The alias.
Host Name	The host name.
System Name	The system name.
IP Address	The IP address (IPv4 or IPv6 format) of the product.
System OID	The system's object identifier.
Product Type	The type of device.
VCS Mode	Whether or not the device is in VCS mode.
VCS ID	The VCS ID number for the fabric.
Node Count	The number of nodes in the fabric.
Principal Switch	The identifier of the principal switch.
Config Mode	The configuration mode.
Device Type	The type of device.
Serial #	The serial number of the product.
Status	The status for the product and the port.
Admin Status	The admin status of the product. Options include: Normal mode Troubleshooting mode
Memo	Additional information about the product.
Vendor	The name of the product's vendor.
Model	The model number of the product.
Port Count	The number of ports on the product.
Firmware	The firmware version of the product.
Build Label	The firmware build number.
FDMI Serial Number	The serial number of the FDMI.
FDMI Firmware	The FDMI firmware version and build number.
FDMI Driver version	The FDMI driver version.
FDMI Manufacturer	The manufacturer of the FDMI.

Field/Component	Description
Location	The physical location of the product.
Contact	The name of the person or group you should contact about the product.
Description	The description of the product.
Connected AP count	Number of APs connected to the controller or switch.
Managed AP count	Only applicable to the selected controller. Number of APs that the selected controller manages.
Controller cluster mode	Only applicable to the selected controller. Cluster mode of the controller: Active, Standby and None.
Controller cluster name	Only applicable to the selected controller. Cluster name.
Controller cluster members	Only applicable to the selected controller. IP addresses of the controller cluster peers.
Cluster (MCT switches only)	The cluster details of the Multi-Chassis Trunk (MCT) switch. MCT cluster details include: • **Cluster ID** — The MCT cluster ID. • **Cluster Name** — The MCT cluster name. • **Cluster RBridge ID** — The RBridge ID of the MCT cluster. • **Cluster State** — Whether the MCT cluster is deployed or undeployed. • **Isolation Mode** — Whether isolation mode is loose or strict. • **Active Member VLAN Range** — The active member VLAN for data. • **Configure Member VLAN Range** — The configured member VLAN for data. • **Keep Alive VLAN** — An alternate VLAN for Cluster Communication Protocol (CCP) when the Inter-Chassis Link (ICL) is down. • **Session VLAN** — The VLAN used by the cluster for control operations. • **ICL Name** — The ICL name.
Cluster Peer (MCT switches only)	The cluster peer details of the MCT switch. MCT cluster peer details include: • **Peer Product** — The name and IP address of the MCT peer product. • **Peer IP Address** — The VE interface IP address of the MCT peer. • **Peer RBridge ID** — The RBridge ID of the MCT peer. • **ICL Name** — The name of the ICL used to reach the MCT peer. • **Keep Alive Interval** — The interval time for CCP over the keep-alive VLAN. • **Hold Time** — The hold-time before making the CCP down state when the ICL goes down. • **Fast Failover** — Whether fast failover is enabled or disabled. • **Active VLAN Range** — The active member VLAN for data. • **Peer State** — Whether the peer state is CCP up or CCP down. • **Peer State Up Time** — How long the peer has been up. • **Peer State Down Reason** — The reason the peer is down.
Add button	Click to add a user-defined property. For more information, refer to "Adding a property field" on page 1329.
Edit button	Click to edit a user-defined property. For more information, refer to "Editing a property field" on page 1330.
Delete button	Click to delete a user-defined property. For more information, refer to "Deleting a property field" on page 1330.

Field/Component	Description
Nodes tab	Select to display information about nodes in the fabric. For detailed information about this tab, refer to "Viewing VCS fabric properties" on page 1319.
Port Profiles tab	Select to display information about port profiles for the fabric members. For detailed information about this tab, refer to "Viewing VCS fabric properties" on page 1319.
Ports tab	Select to display information about ports on the device.
Show list	Select the port type you want to display. Options include: • All • Trunked Ports • ICLs • MCT Ports
Port Count	The number of ports in the group.
Port Actions list	Select to enable or disable port actions.
Performance list	Select to launch the **Performance** dialog box.
Identifier	The identifier of the port.
Name	The name of the port.
MAC Address	The MAC address of the port.
Port Status	The status of the port.
Port State	The state of the port.
Type	The port type.
Speed	The speed of the port.
L2/Tag Mode	Whether the port is tagged or untagged.
Untagged VLAN ID	The untagged VLAN identifier of the port.
Duplex Mode	The duplex mode of the port.
Role	The role of the port. Possible values include the following roles: • Fabric • Edge • Stacking • Peri Port For MCT switches, the port role is either ICL or MCT.
Profile Mode	Displays the profile mode status of the port; for example, Enabled or Disabled.
Active Profiles	Displays the active profiles associated with the port.
LAG/Trunk ID	Displays the LAG name and the trunk port identifier.
Attached MAC	Displays the MAC address of the attached device. The value is empty when the port is not connected. The value contains a comma-separated list of MAC address when more than one MAC address is found.
Stacking Port	Whether or not the port stacked.
MCT Client Name	The MCT client name.
Access Points tab	Select to display information about access ports (APs) connected to the device.

Field/Component	Description
Connected AP count	Number of APs connected to the controller or switch.
Managed AP count	Only applicable to the selected controller. Number of APs that the selected controller manages.
Name	The device name used to identify the AP.
Device MAC	The AP device MAC address.
Model	The model of the AP.
Serial Number	The serial number of the AP.
Firmware version	The firmware level of the AP.
Status	The status of the AP.
Controller \ Port	The IP address of the controller or switch connected to the AP. Also displays the port number if the AP is directly connected.
Connected switch \ Port	The IP address of the switch connected to the AP. Also displays the port number if the AP is directly connected.
Profile Name	AP profile name.
RF Domain Name	The RF domain name set for the AP.
Location	Location set for the AP.
Contact	Contact set for the AP.
Time Zone	The time zone set for the AP.
Country	The country set for the AP.
VLAN for Control Traffic	The VLAN for control traffic set for the AP.
Client count	The number of wireless clients or stations connected or associated to the AP.
SFP/Port Optics tab	Select to display the details of all the SFP and port optics. **NOTE:** To export the SFP details, click the link under the **Physical Ports** - **SFP Details** section of **Detailed Report.**
TX Power	The power transmitted by the port in a device.
RX Power	The power received by the port in a device.
Transceiver Temperature	The temperature of the port, in Celsius.
TX Bias Current	The current supplied to the SFP transceiver. **NOTE:** To export power supply details, click the link under the **Chassis-Power Supply** section of **Detailed Report**.
Wavelength	The wavelength of the port.
Serial #	The number to identify the port.
Media	The type in which the port is present.
vNetwork Connectivity tab	Select to display information about vNetwork connectivity for the fabric members. For detailed information about this tab, refer to "VM Connectivity tab" on page 2744.

4. Click **OK** to close the dialog box.

Viewing VCS fabric properties

To view properties for a VCS fabric, complete the following steps.

1. Select **Ethernet Fabrics** from the view list on the Product List toolbar.
2. Right-click the VCS fabric in the Product List and select **Properties**.

   The *Fabric_Name* **Properties** dialog box displays.
3. Review the device and port properties.

Field/Component	Description
Properties tab	Select to display information about the fabric.
Detailed Report button	Click to launch the detailed cluster report.
Name	The name of the fabric.
Alias	The alias name. This is an editable field.
Host Name	The host name associated with the fabric.
System Name	The name of the product.
IP Address	The IP address (IPv4 or IPv6 format) of the product.
Product Type	The fabric's product type, which is a Layer 2 switch.
VCS Mode	The VCS mode of the switch, which can be enabled or disabled.
VCS ID	The VCS ID configured in the fabric.
Config Mode	The configuration mode of the fabric.
Node Count	The number of fabric nodes in the fabric.
Principal Switch	The name and IP address of the principal switch.
Status	The health status of the cluster.
Admin Status	The administrative status of the switch, for example, Normal.
Memo	Additional comments regarding the switch.
Vendor	The switch vendor.
Model	The switch model type (VDX 6710, VDX 6720, or VDX 6730).
Port Count	The number of ports on the switch.
Firmware	The firmware version and build number.
Location	The physical location of the product. This is an editable field.
Contact	The name of the person or group you should contact about the product, for example, Technical Support. This is an editable field.
Description	The description of the product.
Connected AP Count	The number of AP devices connected to the device.
Add button	Click to add a user-defined property. For more information, refer to "Adding a property field" on page 1329.
Edit button	Click to edit a user-defined property. For more information, refer to "Editing a property field" on page 1330.
Delete button	Click to delete a user-defined property. For more information, refer to "Deleting a property field" on page 1330.

Field/Component	Description
Nodes tab	Select to display information about nodes on the fabric.
Name	The name of the VCS fabric member.
Alias	The fabric member alias name.
Host Name	The host name associated with the VCS fabric member.
System Name	The name of the switch.
IP Address	The IP address of the switch.
System OID	The system's object identifier.
Product Type	The fabric's product type, which is a Layer 2 switch.
Serial #	The VCS fabric member's serial number.
VCS Mode	The VCS mode of the switch, which can be standalone or VCS fabric.
VCS ID	The VCS ID configured in the fabric.
Config Mode	The configuration mode of the fabric, which is Local Only or Distributed.
Licensed Features	The licensed features available on the device.
RBridge ID	The routing bridge identifier associated with the VCS fabric member.
Access Gateway Mode	Indicates whether the Access Gateway mode is enabled or disabled.
State	The device's state (online or offline).
Fabric Status	The state of the fabric that is least operational, based on ISL status. The possible states are: operational, unknown, degraded or failed.
Status	The health status of the switch.
Admin Status	The administrative status of the switch, for example, Normal.
Memo	Additional comments regarding the switch.
Vendor	The switch vendor.
Model	The switch model type (VDX 6710, VDX 6720, or VDX 6730).
Port Count	The number of ports on the switch.
Firmware	The firmware version and build number.
Location	The physical location of the product.
Contact	The name of the person or group you should contact about the product, for example, Technical Support.
Description	The description of the product.
Connected AP Count	The number of AP devices connected to the device.
Add button	Click to add a user-defined property. For more information, refer to "Adding a property field" on page 1329.
Edit button	Click to edit a user-defined property. For more information, refer to "Editing a property field" on page 1330.
Delete button	Click to delete a user-defined property. For more information, refer to "Deleting a property field" on page 1330.
Port Profiles tab	Select to display information about port profiles on the fabric.
Name	The name of the port profile (not editable). There are multiple default profiles in a fabric (one per member).

Field/Component	Description
Status	Port profile states can be one of the following, all of which are configured using the command line interface: • Created • Activated • Associated • Applied
MAC Count	The number of MAC addresses associated with the port profile.
VLANs	The number of virtual LANs (VLANs) associated with the port profile, along with the following VLAN information: • All — Indicates that the port profile will allow all VLAN IDs. • None — Indicates that the port profile will not allow any VLAN IDs. • All Except <*VLAN IDs*> — Indicates that the port profile will allow any packet except the VLAN IDs specified. • <*VLAN IDs*> — Indicates that the port profile will allow any packet with the VLAN IDs specified.
Domain Count	The number of domains associated with the port profile.
QoS	Indicates whether the QoS profile is associated with the port profile and, if there is an associated QoS profile, whether it is in DCB or non-DCB mode.
ACL	Displays the type of access control list (ACL) profile (Standard or Extended), if an ACL is associated with the port profile.
Associated MACs list	Lists the following details of the Media Access Control (MAC) addresses associated with the port profile: • MAC — The MAC address associated with the port profile. • Name — The name of the vNIC associated with the selected MAC address. • Switch Port — The switch port associated with the selected MAC address. • VM — The virtual machine associated with the selected MAC address. • vNIC — The virtual network interface card (vNIC) associated with the selected MAC address. • Port Group — The port group associated with the selected MAC address. • vCenter — The virtual center associated with the selected MAC address.
Add button	Click to launch the **Assign MACs** dialog box, which you can use to select discovered MAC addresses and add offline MAC addresses for the selected port profile.
Delete button	Click to delete the selected MAC address from the port profile list.
Compare button	Click to launch the **Profile Comparison Summary** dialog box, where you can compare selected products to profiles using filtered criteria.
VLANs tab	
Port Mode	The switch port mode of the port profile (access or trunk).

Field/Component	Description

Configuration	Displays one of the following VLAN configuration options:
	• Access mode — Supports MAC address and MAC group classification.
	• Trunk mode
	  • Add — Adds VLAN IDs to the port profiles.
	  • Remove — Deletes VLAN IDs to the port profiles.
	  • All — Indicates that the port profile allows all VLAN IDs.
	  • None — Indicates that the port profile does not allow any VLAN IDs.
	  • All Except <*VLAN IDs*> — Indicates that the port profile allows any packet except the VLAN IDs specified.
	  • <*VLAN IDs*> — Indicates that the port profile allows any packet with the VLAN IDs specified.
	NOTE: GVLAN supported Trunk Mode supports the Trunk VLAN and the Native Trunk classifications with the cTag information.

Native VLAN/VLAN	Displays one of the following based on the VLAN configuration: • Access Mode — Displays the associated MAC address or MAC group or both to a VLAN ID. • Trunk Mode — Displays the cTag for a VLAN ID or Native VLAN ID or both.
Associated Domain	Lists the domain names associated with the port profile.
QoS tab — DCB mode	
Mode	The mode of Quality of Service (QoS) assigned to the port (DCB).
DCB Map	The DCB map name.
Precedence	This number determines the map's priority. Valid values are from 1 through 100.
Fabric Remap Priority	The fabric remap priority of the port. Valid values are CoS 0 through CoS 6, and the default is CoS 0.
Lossless Remap Priority	The FCoE lossless remap priority of the port. Valid values are CoS 0 through CoS 6, and the default is CoS 0.
QoS tab — Non-DCB mode (Ethernet PFC with Trust)	
Mode	The mode of Quality of Service (QoS) assigned to the port (non-DCB).
Trust	Indicates whether the Ethernet trust of the port is enabled or disabled.
Flow Control	The Ethernet priority flow control mode of the port. Possible modes are as follows: • Off (the default) • 802.3x pause • Tx On or Off • Rx On or Off • Priority Flow Control. For this mode, the Tx and Rx values for each CoS display in the table.
Maps	Displays details about the following DCB maps: • CoS to CoS — Displays the details of the CoS to CoS map assigned to the port. • Traffic Class — Displays the details of the Traffic Class map assigned to the port. **NOTE:** The CoS to CoS map is the default.

Field/Component	Description
QoS tab — Non-DCB mode (Ethernet Pause and Ethernet PFC)	
Mode	The mode of Quality of Service (QoS) assigned to the port (non-DCB).
Flow Control	The Ethernet priority flow control mode of the port. The default flow control mode is Off. Possible modes are as follows: • Off • 802.3x pause • Tx On or Off • Rx On or Off • Priority Flow Control. For this mode, the Tx and Rx values for each CoS display in the table.
Maps	Displays details about the following DCB maps: • CoS to CoS — Displays the details of the CoS to CoS map (the default) assigned to the port. • Traffic Class — Displays the details of the Traffic Class map assigned to the port.
L2 ACLs tab	
Name	The name of the Access Control List (ACL).
Type	The ACL type. Options include Extended and Standard.
L2 ACLs list	The list includes the following details: • Sequence — The Layer 2 ACL entry sequence number. • Action — Whether the ACL permits or denies traffic. • Source — The source MAC address on which the ACL filters traffic. • Count — Whether count is enabled or disabled.
Ports tab	Select to display information about ports on the fabric.
Show list	Select what ports you want to display. Options include: • **Fabric and Edge Ports** • **Edge Ports** • **Fabric Ports** • **FC Ports**
Port Count	The number of ports in the group.
Port Actions list	Select one of the following options: • **Enable** • **Disable** • **Display Attached Port Properties**
Performance list	Select to launch the Performance dialog box.

Field/Component	Description
Fabric and Edge Ports properties	• **Identifier** — The identifier of the port. • **Name** — The name of the port. This is an editable field. Enter a name (up to 64 characters) for the port. • **MAC Address** — The MAC address of the port. • **Port Status** — The status of the port. • **Port State** — The state of the port. • **Type** — The port type. • **Speed** — The speed of the port. • **L2/Tag Mode** — Indicates whether L2 tag mode is enabled or disabled. • **Untagged VLAN ID** — The untagged VLAN identifier of the port. • **Duplex Mode** — The duplex mode of the port. • **Role** — The role of the port. Possible values include the following roles: - Fabric - Edge - Stacking • **Profile Mode** — Displays the profile mode status of the port; for example, Enabled or Disabled. • **Active Profiles** — Displays the active profiles associated with the port. • **Port Profile Domains** — Displays the port profile domain name. • **Attached Device [MACs]** — Displays the MAC address of the attached device.The value is empty when the port is not connected. The value contains a comma-separated list of MAC addresses when more than one MAC address is found. • **LAG/Trunk ID** — Displays the LAG or trunk ID.

Field/Component	Description
FC Ports properties	• **Identifier** — The identifier of the port. • **Name** — The name of the port. This is an editable field. Enter a name (up to 64 characters) for the port. • **WWN** — The world wide name of the device. • **FC Address** — The Fibre Channel address. Each FC port has both an address identifier and a world wide name. • **Status** — The operational status. • **Additional Info** — Additional information about the port. • **Calculated Status** — The calculated operational status. There are four possible operation status values (Up, Down, Disabled , or Backup Active). • **State** — The state for the port. • **Blocked** — The configuration of the switch (blocked or unblocked). • **Type** — The port type. • **Locked Type** — The port type of the locked product. **NOTE:** Offline ports of a Network OS device in AG mode are displayed as N_Port. • **Speed (Gbps)** — The speed of the port. • **Buffers Desired** — The number of buffers desired but not allocated. • **Buffers Allocated** — The number of buffers allocated. • **Distance Actual (km)** — The actual distance (in km) for -end port connectivity. • **Distance Estimated (km)** — The estimated distance (in km) for -end port connectivity. • **Distance setting** — Whether the connection is considered to be normal or longer distance. • **Attached Switch** — The IP address of the attached device. • **Attached Port #** — The port number of the attached product. • **Connected Devices** — The WWN for each connected device. • **NPIV Status** — Whether NPIV is enabled or disabled on the port.

Field/Component	Description
SFP/Port Optics	Click to view the SFP/Port Optic information: • **TX Power** — The power transmitted to the SFP in dBm and uWatts. • **RX Power** — The power received from the port in dBm and uWatts. • **Transceiver Temp (C)** — The temperature of the SFP transceiver. • **Voltage (mVolts)** — The voltage across the port in mVolts. • **Transceiver Current (mAmps)** — The laser bias current value in mAmps. • **Powered on Years (Hours)** — The powered on time in years and hours for 16 Gbps capable ports. Empty for unsupported ports. • Requires a 16 Gbps capable port running Fabric OS 7.0 or later. • **FC Speed (GB/s)** (Fabric OS 7.0 or later) — The FC port speed; for example, 4 Gbps. • **FC Speed (MB/s)** (Fabric OS 6.4 or earlier) — The FC port speed; for example, 400 Mbps. • **Distance** — The length of the fiber optic cable. • **Vendor** — The vendor of the SFP. • **Vendor OUI** — The vendor's organizational unique identifier (OUI). • **Vendor PN** — The part number of the SFP. • **Vendor Rev** — The revision number of the SFP. • **Serial #** — The serial number of the SFP. • **Data Code** — The data code. • **Media Form Factor** — The type of media for the transceiver; for example, single mode. • **Connector** — The type of port connector. • **Wave Length** — The wave length. • **Encoding** — Displays how the fiber optic cable is encoded.
Add button	Click to add a user-defined property. For more information, refer to "Adding a property field" on page 1329.
Edit button	Click to edit a user-defined property. For more information, refer to "Editing a property field" on page 1330.
Delete button	Click to delete a user-defined property. For more information, refer to "Deleting a property field" on page 1330.

4. Click **OK** to close the dialog box.

Host properties

You can view device and port properties from the Product List or the map.

You can customize the Host **Properties** dialog boxes by creating user-defined property labels (refer to "Adding a property field" on page 1329).

NOTE
You cannot create user-defined property labels at the adapter level.

You can also edit property fields to change information. Fields containing a green triangle ( ) in the lower right corner are editable.

Viewing adapter port properties

To view adapter port properties, complete the following steps.

1. Right-click an HBA icon and select **Show Ports**.
2. Right-click the port and select **Properties**, or double-click the port.

   Fields containing a green triangle ( ) in the lower right corner are editable.

   The *HBA_Port* **Properties** dialog box displays. Table 31 details the properties of the selected port.

TABLE 31 Adapter port properties

Field	Description
Port Attributes	
Port #	The port number: 0 or 1.
Name	The name that is manually assigned to the port.
Zone Alias	The alternate name of the zone.
Symbolic Name	The symbolic name (nickname) for the HBA port.
HCM Name	The version of the Host Connectivity Manager (HCM) application.
Associated VMs	Virtual machines associated with the HBA port.
Port WWN	The port's world wide name.
Node WWN	The node's (parent device) world wide name.
Factory Port WWN	The world wide name assigned at the factory for the HBA port.
Factory Node WWN	The world wide name assigned at the factory for the HBA.
Media	The type of media; for example, 8G-sw (8 Gbps software).
Product Type	The device port type; for example, N_Port.
Vendor	The port's vendor.
Type	The port type; for example, N_Port.
FC Address	The port's Fibre Channel address.
Attached Port #	The port number of the attached product.
Active FC4 Types	The active FC4 types; for example, SCSI or IP.
Class of Service	The class of the port; for example, Class-2 or Class-3.
Switch	The name of the switch.
Fabric	The name of the Fabric.
VM Port Name	The port name of the virtual machine associated with the host.
Preboot Created	Indicates whether preboot was created on the virtual port.
PCI Function Index	The PCI function number associated with the physical port.
Fabric Assigned Address	The state (enabled or disabled) of the fabric assigned address for the adapter.

TABLE 31 Adapter port properties (Continued)

Field	Description
WWN Source	The source of the world wide name. Options include: Fabric — The WWN is assigned from the fabric. The fabric assigned address must be enabled. Factory — The WWN is assigned at the factory.
Configuration	
Configured State	Indicates whether the port is enabled or disabled.
Max Bandwidth	The maximum allowable bandwidth output for the selected port.
Operating State	Indicates whether the port is online or offline.
Configured Speed	The configured port speed.
Operating Speed	The speed at which the port is operating.
Max Speed Supported	The maximum speed that is supported on the port. For the FC port, the maximum speed is 8 Gbps.
Configured Topology	The configured topology setting: auto, point-to-point, or loop.
Operating Topology	The operating topology setting: auto, point-to-point, or loop.
Boot over SAN	Indicates whether boot over SAN is enabled.
Receive BB Credits	The number of buffer credits received.
Transmit BB Credits	The number of buffer credits transmitted.
IOC ID	The IO Controller identifier.
Frame Field Size	The frame size, in bytes, of the port.
Hardware Path	The hardware path of the HBA.
Virtual Port Count	The number of virtual ports associated with the HBA.
Operating State	Displays details about the state of the following operating parameters: • Beacon State • Link Beacon State • MPIO Mode State • Path Time Out • Logging Level • Target Rate Limit • Default Rate Limit
FC-SP	
Authentication	Indicates whether FC-SP authentication is enabled or disabled.
FCSP Status	Whether FC-SP authentication is being used.
Algorithm	The configured authentication algorithm.
Group	The DH group, which is DH-null (group 0), which is the only option.
Error Status	The health status of the Fibre Channel Security Protocol parameters.
QoS	
Configured QoS State	Indicates whether QoS is enabled or disabled.
Operating QoS State	Indicates whether QoS is on or off.

TABLE 31 Adapter port properties (Continued)

Field	Description
Total BB Credit	The total number of buffer credits.
Priority Levels	Lists the available priorities (High, Medium, Low).
Add button	Click to add a user-defined property. For more information, refer to "Adding a property field" on page 1329.
Edit button	Click to edit a user-defined property. For more information, refer to "Editing a property field" on page 1330.
Delete button	Click to delete a user-defined property. For more information, refer to "Deleting a property field" on page 1330.

3. Click **OK** to close.

Properties customization

NOTE
Properties customization requires read and write permissions to the Properties - Add / Delete Columns privilege.

You can customize the product **Properties** dialog boxes by creating user-defined product and port properties. You can also edit or delete user-defined properties, as needed.

You can create up to three user-defined property labels from the **Properties** dialog box for each of the following object types: product and port properties. Product property labels created from the **Properties** dialog box display in the Product List and the **Properties** dialog box. You can only view port property labels on the **Ports** tab of the **Properties** dialog box. User-defined properties must be unique across all **Properties** dialog boxes and the Product List.

You cannot edit the user-defined property field contents from the Product List; however, you can edit the field in the **Properties** dialog box.

Property fields containing a green triangle ( ) in the lower right corner are editable. To edit a field with a green triangle ( ), click in the field and make your changes.

Adding a property field

You can add up to three new user-defined properties to the **Properties** and **Ports** tabs of the device **Properties** dialog box.

To add a user-defined property, complete the following steps.

1. Right-click any product icon and select **Properties**.

   The **Properties** dialog box displays.

2. Select the tab to which you want to add a property, if necessary.
3. Click **Add**.

   The **Add Property** dialog box displays.

4. Enter a label and description for the property.

The label must be unique and can be up to 30 characters.

The description can be up to 126 characters.

5. Select **Port** or **Property** from the **Type** list, if available.
6. Click **OK**.

   The new property displays in the properties list as well as the Product List. To edit the user-defined property field, click in the field and make your changes.

Editing a property field

NOTE
Properties customization requires read and write permissions to the Properties - Add / Delete Columns privilege.

You can edit any property that you create on the **Properties** dialog box.

Fields containing a green triangle ( ) in the lower right corner are editable. To edit a field with a green triangle ( ), click in the field and make your changes.

To edit a user-defined property, complete the following steps.

1. Right-click any product icon and select **Properties**.

   The **Properties** dialog box displays.
2. Select the tab on which you want to edit a property, if necessary.
3. Click **Edit** > *Property_Label*.

   The **Edit Property** dialog box displays.
4. Change the label and description for the property, as needed.

   The label must be unique and can be up to 30 characters.

   The description can be up to 126 characters.
5. Select **Port** or **Property** from the **Type** list, if available.
6. Click **OK**.

Deleting a property field

NOTE
Properties customization requires read and write permissions to the Properties - Add / Delete Columns privilege.

You can delete any user-defined property from the **Properties** dialog box. To delete a user-defined property, complete the following steps.

1. Right-click any product icon and select **Properties**.

   The **Properties** dialog box displays.
2. Select the tab on which you want to delete a user-defined property, if necessary.
3. Click **Delete** > *Property_Label* (where *Property_Label* is the user-defined property you want to delete).

4. Click **Yes** on the confirmation message.

   The property you selected is deleted.

Editing a property field directly

You can edit fields containing a green triangle ( ) in the lower right corner. To edit a field, complete the following steps.

1. Right-click any product icon and select **Properties**.

   The **Properties** dialog box displays.

2. Select the tab on which you want to edit a field.

   Fields containing a green triangle ( ) in the lower right corner are editable.

3. Click in an editable field and change the information.
4. Click **OK**.

Appendix

F

Regular Expressions

In this appendix

This appendix presents a summary of Unicode regular expression constructs that you can use in the Management application.

TABLE 1 Characters

Construct	Matches
x	The character x
\\	The backslash character
\0n	The character with octal value 0n (0 <= n <= 7)
\0nn	The character with octal value 0nn (0 <= n <= 7)
\0mnn	The character with octal value 0mnn (0 <= m <= 3, 0 <= n <= 7)
\xhh	The character with hexadecimal value 0xhh
\uhhhh	The character with hexadecimal value 0xhhhh
\t	The tab character ('\u0009')
\n	The newline (line feed) character ('\u000A')
\r	The carriage-return character ('\u000D')
\f	The form-feed character ('\u000C')
\a	The alert (bell) character ('\u0007')

TABLE 1 Characters

Construct	Matches
\e	The escape character ('\u001B')
\cx	The control character corresponding to x

TABLE 2 Character classes

Construct	Matches
[abc]	a, b, or c (simple class)
[^abc]	Any character except a, b, or c (negation)
[a-zA-Z]	a through z or A through Z, inclusive (range)
[a-d[m-p]]	a through d, or m through p: [a-dm-p] (union)
[a-z&&[def]]	d, e, or f (intersection)
[a-z&&[^bc]]	a through z, except for b and c: [ad-z] (subtraction)
[a-z&&[^m-p]]	a through z, and not m through p: [a-lq-z](subtraction)

TABLE 3 Predefined character classes

Construct	Matches
.	Any character (may or may not match line terminators)
\d	A digit: [0-9]
\D	A non-digit: [^0-9]
\s	A whitespace character: [\t\n\x0B\f\r]
\S	A non-whitespace character: [^\s]
\w	A word character: [a-zA-Z_0-9]
\W	A non-word character: [^\w]

TABLE 4 POSIX character classes (US-ASCII only)

Construct	Matches
\p{Lower}	A lower-case alphabetic character: [a-z]
\p{Upper}	An upper-case alphabetic character:[A-Z]
\p{ASCII}	All ASCII:[\x00-\x7F]
\p{Alpha}	An alphabetic character:[\p{Lower}\p{Upper}]
\p{Digit}	A decimal digit: [0-9]
\p{Alnum}	An alphanumeric character:[\p{Alpha}\p{Digit}]
\p{Punct}	Punctuation: One of !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
\p{Graph}	A visible character: [\p{Alnum}\p{Punct}]
\p{Print}	A printable character: [\p{Graph}\x]

TABLE 4 POSIX character classes (US-ASCII only)

Construct	Matches
\p{Blank}	A space or a tab: [\t]
\p{Cntrl}	A control character: [\x00-\x1F\x7F]
\p{XDigit}	A hexadecimal digit: [0-9a-fA-F]
\p{Space}	A whitespace character: [\t\n\x0B\f\r]

TABLE 5 java.lang.Character classes (simple java character type)

Construct	Matches
\p{javaLowerCase}	Equivalent to java.lang.Character.isLowerCase()
\p{javaUpperCase}	Equivalent to java.lang.Character.isUpperCase()
\p{javaWhitespace}	Equivalent to java.lang.Character.isWhitespace()
\p{javaMirrored}	Equivalent to java.lang.Character.isMirrored()

TABLE 6 Classes for Unicode blocks and categories

Construct	Matches
\p{InGreek}	A character in the Greek block (simple block)
\p{Lu}	An uppercase letter (simple category)
\p{Sc}	A currency symbol
\P{InGreek}	Any character except one in the Greek block (negation)
[\p{L}&&[^\p{Lu}]]	Any letter except an uppercase letter (subtraction)

TABLE 7 Boundary matches

Construct	Matches
^	The beginning of a line
$	The end of a line
\b	A word boundary
\B	A non-word boundary
\A	The beginning of the input
\G	The end of the previous match
\Z	The end of the input but for the final terminator, if any
\z	The end of the input

TABLE 8 Greedy quantifiers

Construct	Matches
X?	X, once or not at all
X*	X, zero or more times
X+	X, one or more times
X{n}	X, exactly n times
X{n,}	X, at least n times
X{n,m}	X, at least n but not more than m times

TABLE 9 Reluctant quantifiers

Construct	Matches
X??	X, once or not at all
X*?	X, zero or more times
X+?	X, one or more times
X{n}?	X, exactly n times
X{n,}?	X, at least n times
X{n,m}?	X, at least n but not more than m times

TABLE 10 Possessive quantifiers

Construct	Matches
X?+	X, once or not at all
X*+	X, zero or more times
X++	X, one or more times
X{n}+	X, exactly n times
X{n,}+	X, at least n times
X{n,m}+	X, at least n but not more than m times

TABLE 11 Logical operators

Construct	Matches
XY	X followed by Y
X|Y	Either X or Y
(X)	X, as a capturing group

TABLE 12 Back references

Construct	Matches
\n	Whatever the nth capturing group matched
Quotation	
\	Nothing, but quotes the following character
\Q	Nothing, but quotes all characters until \E
\E	Nothing, but ends quoting started by \Q

TABLE 13 Special constructs (non-capturing)

Construct	Matches
(?:X)	X, as a non-capturing group
(?idmsux-idmsux)	Nothing, but turns match flags on–off
(?idmsux-idmsux:X)	X, as a non-capturing group with the given flags on–off
(?=X)	X, through zero-width positive lookahead
(?!X)	X, through zero-width negative lookahead
(?<=X)	X, through zero-width positive lookbehind
(?<!X)	X, through zero-width negative lookbehind
(?>X)	X, as an independent, non-capturing group

Appendix

CLI Templates

G

In this appendix

The Management application provides preconfigured Configuration templates for IronWare and Network OS devices. By default, all preconfigured templates are configure to prompt for additional targets during manual deployment. The preconfigured templates include the following:

TABLE 14 HyperEdge – Stack Enable

Feature	Description	CLI Commands
HyperEdge	To enable stacking mode.	stack enable

TABLE 15 HyperEdge – Stack Disable

Feature	Description	CLI Commands
HyperEdge	To disable stacking mode.	stack disable

TABLE 16 HyperEdge – Stack Port Creation

Feature	Description	CLI Commands
HyperEdge	To create stacking ports.	stack unit $<STACKID|INTEGER> stack-port $<STACKID1/SLOT/PORT|STRING> $<STACKID2/SLOT/PORT|STRING>

TABLE 17 HyperEdge – Stack Port Deletion

Feature	Description	CLI Commands
HyperEdge	To delete stacking ports.	stack unit $<STACKID|INTEGER> no stack-port $<STACKID1/SLOT/PORT|STRING> $<STACKID2/SLOT/PORT|STRING>

TABLE 18 HyperEdge – Stack Trunk Creation

Feature	Description	CLI Commands
HyperEdge	To create stacking trunks.	stack unit $<STACKID|INTEGER> stack-trunk $<SRC_STACKID/SLOT/PORT|STRING> to $<DST_STACKID/SLOT/PORT|STRING>

TABLE 19 HyperEdge – Stack Trunk Deletion

Feature	Description	CLI Commands
HyperEdge	To delete stacking trunks.	stack unit $<STACKID|INTEGER> no stack-trunk $<SRC_STACKID/SLOT/PORT|STRING> to $<DST_STACKID/SLOT/PORT|STRING>

TABLE 20 HyperEdge – Peri Port Creation

Feature	Description	CLI Commands
HyperEdge	To create peripheral ports.	stack unit $<STACKID|INTEGER> peri-port $<STACKID/SLOT/PORT|STRING>

TABLE 21 HyperEdge – Peri Port Deletion

Feature	Description	CLI Commands
HyperEdge	To delete peripheral ports.	stack unit $<STACKID|INTEGER> no peri-port $<STACKID/SLOT/PORT|STRING>

TABLE 22 HyperEdge – Peri Trunk Creation

Feature	Description	CLI Commands
HyperEdge	To create peripheral trunks.	stack unit $<STACKID|INTEGER> peri-trunk $<SRC_STACKID/SLOT/PORT|STRING> to $<DST_STACKID/SLOT/PORTD|STRING>

TABLE 23 HyperEdge – Peri Trunk Deletion

Feature	Description	CLI Commands
HyperEdge	To delete peripheral trunks.	stack unit $<STACKID\|INTEGER> no peri-trunk$<SRC_STACKID/SLOT/PORT|STRING> to$<DST_STACKID/SLOT/PORTD|STRINGG>

TABLE 24 HyperEdge – Peri Port Connection Creation

Feature	Description	CLI Commands
HyperEdge	To create peripheral port connections.	stack unit $<STACKID|INTEGER> connect $<STACKID/SLOT/PORT|STRING>

TABLE 25 IronWare OS – Enable Web Element Manager

Feature	Description	CLI Commands
IronWare OS	Enable Web Element Manager for IronWare products	web-management http

TABLE 26 IronWare OS – Configure L3-Access-List

Feature	Description	CLI Commands
ACL	Configure L3 access list for IronWare products	access-list $<aclNumber|INTEGER> deny $<IPAddress|IP_ADDRESS>

TABLE 27 IronWare OS – Configure L2-Access-List

Feature	Description	CLI Commands
ACL	Configure L2 access list for IronWare products.	access-list $<aclNumber|INTEGER> deny $<srcmac|MAC> $<srcmask|MAC> any access-list $<aclNumber|INTEGER> deny any $<destmac|MAC> $<destMask|MAC> access-list $<aclNumber|INTEGER> permit $<sourcemac2|MAC> $<sourcemask2|MAC> any access-list $<aclNumber|INTEGER> permit any any no access-list $<aclNumber|INTEGER> permit any any no access-list $<aclNumber|INTEGER> permit $<sourcemac2|MAC> $<sourcemask2|MAC> any

TABLE 28 MCT Cluster Creation

Feature	Description	CLI Commands
MCT	Create a session VLAN.	vlan $<SESSION_VLAN|INTEGER> name Session-VLAN tagged ethernet $<SESSION_VLAN_PORT|SLOT_PORT> router-interface ve $<SESSION_VE_INTERFACE|INTEGER> interface ve $<SESSION_VE_INTERFACE|INTEGER> ip address $<SESSION_VE_INTERFACE_IP|STRING>
MCT	Create a keep–alive VLAN.	vlan $<KEEP_ALIVE_VLAN|INTEGER> name MCT-keep-alive tagged ethernet $<KEEP_ALIVE_VLAN_PORT|SLOT_PORT>
MCT	Create cluster configuration.	cluster $<CLUSTER_NAME|STRING> $<CLUSTER_ID|INTEGER> rbridge-id $<RBRIDGE_ID|INTEGER> session-vlan $<SESSION_VLAN|INTEGER> keep-alive-vlan $<KEEP_ALIVE_VLAN|INTEGER> icl $<ICL_NAME|STRING> ethernet $<ICL_PORT|SLOT_PORT> peer $<PEER_SESSION_VE_INTERFACE_IP|STRING> rbridge-id $<PEER_RBRIDGE_ID|INTEGER> icl $<ICL_NAME|STRING>
MCT	Specify single VLAN ID or range <DECIMAL> [to <DECIMAL>].	member-vlan $<MEMBER_VLANS|STRING> **NOTE:** ICL ports should also be added to MCT Member VLANs.

TABLE 29 MCT Cluster Deployment

Feature	Description	CLI Commands
MCT	Deploy cluster.	cluster $<CLUSTER_NAME|STRING> $<CLUSTER_ID|INTEGER> deploy

TABLE 30 MCT Cluster Undeployment

Feature	Description	CLI Commands
MCT	Undeploy cluster.	cluster $<CLUSTER_NAME|STRING> $<CLUSTER_ID|INTEGER> undeploy

TABLE 31 MCT Cluster Deletion

Feature	Description	CLI Commands
MCT	Delete cluster.	no cluster $<CLUSTER_NAME|STRING> $<CLUSTER_ID|INTEGER> no vlan $<SESSION_VLAN|INTEGER> no vlan $<KEEP_ALIVE_VLAN|INTEGER>

TABLE 32 MCT Client Creation

Feature	Description	CLI Commands
MCT	Create a cluster client.	cluster $<CLUSTER_NAME|STRING> $<CLUSTER_ID|INTEGER> client $<CLIENT_NAME|STRING> rbridge-id $<CLIENT_RBRIDGE_ID|INTEGER> client-interface ethernet $<CLIENT_PORT|SLOT_PORT> deploy

TABLE 33 MCT Client Deletion

Feature	Description	CLI Commands
MCT	Delete a cluster client.	cluster $<CLUSTER_NAME|STRING> $<CLUSTER_ID|INTEGER> no client $<CLIENT_NAME|STRING>

TABLE 34 MPLS – Loopback Interface Configuration

Feature	Description	CLI Commands
MPLS	Loopback interface configuration used for device reachability using OSPF. It assigns an IP address and advertises the interface through OSPF.	! Required for LSP egress address in LSP Manager as well as a soft interface for IP routing interface loopback $<LOOPBACK_INTERFACE|INTEGER> enable ip ospf area $<OSPF_AREA|INTEGER> ip address $<LOOPBACK_INTERFACE_IP|STRING>

TABLE 35 MPLS – Core Interface Configuration

Feature	Description	CLI Commands
MPLS	MPLS core interface configuration such as assigning an IP address and advertising using OSPF	! Core facing interfaces need IP address for MPLS ! Repeat the following commands for all MPLS core interfaces in the product interface ethernet $<CORE_INTERFACE_1|SLOT_PORT> enable ip ospf area $<OSPF_AREA|INTEGER> ip address $<CORE_INTERFACE_1_IP|STRING> router mpls mpls-interface ethernet $<CORE_INTERFACE_1|SLOT_PORT>

TABLE 36 MPLS – Endpoint Configuration

Feature	Description	CLI Commands
MPLS	Used to configure MPLS endpoints. Disable FDP, CDP as they are not supported in MPLS endpoints.	! FDP, CDP should not be enabled on MPLS endpoints ! Repeat the following commands for all the MPLS endpoints interface ethernet $<MPLS_END_POINT_1|SLOT_PORT> enable no fdp enable no cdp enable

TABLE 37 Network OS – Associate MAC to Port Profile

Feature	Description	CLI Commands
AMPP	Associates the MAC to the existing port profile	no port-profile $<ProfileName|STRING> activate no port-profile $<ProfileName|STRING> static $<DisAssosicateMACAddress1|MAC> no port-profile $<ProfileName|STRING> static $<DisAssosicateMACAddress2|MAC> no port-profile $<ProfileName|STRING> static $<DisAssosicateMACAddress3|MAC> port-profile $<ProfileName|STRING> activate port-profile $<ProfileName|STRING> static $<AssosicateMACAddress1|MAC> port-profile $<ProfileName|STRING> static $<AssosicateMACAddress2|MAC> port-profile $<ProfileName|STRING> static $<AssosicateMACAddress3|MAC>

TABLE 38 Network OS – Configure CRC Align Errors Monitor

Feature	Description	CLI Commands
Network OS	This template is used to configure threshold and alert values for CRC Align Errors (due to FCS Error or Alignment Error). Possible values for timebase are day, hour, minute and none. Buffer value cannot be more than average of high plus low threshold. Supported Values for High and Low Threshold Action Parameters are email, raslog, all, and none.	threshold-monitor interface custom type Ethernet area CRCAlignErrors threshold timebase $<Timebase|STRING> high-threshold $<HighThresholdValue|INTEGER> low-threshold $<LowThresholdValue|INTEGER> buffer $<BufferValue|INTEGER> threshold-monitor interface custom type Ethernet area CRCAlignErrors alert above highthresh-action $<AboveHighThreshAction|STRING> lowthresh-action $<AboveLowThreshAction|STRING> threshold-monitor interface custom type Ethernet area CRCAlignErrors alert below highthresh-action $<BelowHighThreshAction|STRING> lowthresh-action $<BelowLowThreshAction|STRING> threshold-monitor interface apply custom-monitoring

TABLE 39 Network OS – Configure Extended L2 Access List

Feature	Description	CLI Commands
ACL	This template is used to configure an extended L2 ACL on Network OS products running 3.0 or later.	mac access-list extended $<extdAclName|STRING> deny $<mac1|MAC> $<mask1|MAC> any deny any $<mac2|MAC> $<mask2|MAC> deny $<mac3|MAC> $<mask3|MAC> $<mac4|MAC> $<mask4|MAC> permit $<mac5|MAC> $<mask5|MAC> $<mac6|MAC> $<mask6|MAC> permit any any

TABLE 40 Network OS – Configure Inter Frame Gap Violation Fencing

Feature	Description	CLI Commands
Network OS	This template is used to configure high threshold value to fence an interface when Inter Frame Gap(IFG) minimum length (typical value is 12) violation occurs. Possible values for timebase are day, hour, minute and none.	threshold-monitor interface custom type Ethernet area IFG threshold timebase $<Timebase|STRING> high-threshold $<HighThresholdValue|INTEGER> threshold-monitor interface custom type Ethernet area IFG alert above highthresh-action fence threshold-monitor interface apply custom-monitoring

TABLE 41 Network OS – Configure Inter Frame Gap Violation Monitor

Feature	Description	CLI Commands
Network OS	This template is used to configure threshold and alert values for Inter Frame Gap(IFG) minimum length (typical value is 12) Violation monitoring. Possible values for timebase are day, hour, minute and none. Buffer value cannot be more than average of high plus low threshold. Supported Values for High and Low Threshold Action Parameters are email, raslog, all, and none.	threshold-monitor interface custom type Ethernet area IFG threshold timebase $<Timebase|STRING> high-threshold $<HighThresholdValue|INTEGER> low-threshold $<LowThresholdValue|INTEGER> buffer $<BufferValue|INTEGER> threshold-monitor interface custom type Ethernet area IFG alert above highthresh-action $<AboveHighThreshAction|STRING> lowthresh-action $<AboveLowThreshAction|STRING> threshold-monitor interface custom type Ethernet area IFG alert below highthresh-action $<BelowHighThreshAction|STRING> lowthresh-action $<BelowLowThreshAction|STRING> threshold-monitor interface apply custom-monitoring

TABLE 42 Network OS – Configure RX Missing Terminations Characters Monitor

Feature	Description	CLI Commands
Network OS	This template is used to configure threshold and alert values for RX Missing Termination Characters monitoring. Possible values for timebase are day, hour, minute and none. Buffer value cannot be more than average of high plus low threshold. Supported Values for High and Low Threshold Action Parameters are email, raslog, all, and none.	threshold-monitor interface custom type Ethernet area AbnormalFrameTerminations threshold timebase $<Timebase|STRING> high-threshold $<HighThresholdValue|INTEGER> low-threshold $<LowThresholdValue|INTEGER> buffer $<BufferValue|INTEGER> threshold-monitor interface custom type Ethernet area AbnormalFrameTerminations alert above highthresh-action $<AboveHighThreshAction|STRING> lowthresh-action $<AboveLowThreshAction|STRING> threshold-monitor interface custom type Ethernet area AbnormalFrameTerminations alert below highthresh-action $<BelowHighThreshAction|STRING> lowthresh-action $<BelowLowThreshAction|STRING> threshold-monitor interface apply custom-monitoring

TABLE 43 Network OS – Configure RX Symbol Errors Monitor

Feature	Description	CLI Commands
Network OS	This template is used to configure threshold and alert values for RX Symbol Errors Monitoring. Possible values for timebase are day, hour, minute and none. Buffer value cannot be more than average of high plus low threshold. Supported Values for High and Low Threshold Action Parameters are email, raslog, all, and none.	threshold-monitor interface custom type Ethernet area SymbolErrors threshold timebase $<Timebase|STRING> high-threshold $<HighThresholdValue|INTEGER> low-threshold $<LowThresholdValue|INTEGER> buffer $<BufferValue|INTEGER> threshold-monitor interface custom type Ethernet area SymbolErrors alert above highthresh-action $<AboveHighThreshAction|STRING> lowthresh-action $<AboveLowThreshAction|STRING> threshold-monitor interface custom type Ethernet area SymbolErrors alert below highthresh-action $<BelowHighThreshAction|STRING> lowthresh-action $<BelowLowThreshAction|STRING> threshold-monitor interface apply custom-monitoring

TABLE 44 Network OS – Configure Standard L2 Access List

Feature	Description	CLI Commands
ACL	This template is used to configure standard L2 ACL on Network OS products running 3.0 or later.	mac access-list standard $<stdAclName|STRING> deny $<denyMAC|MAC> $<mask1|MAC> permit $<permitMAC|MAC> $<mask2|MAC> permit any

TABLE 45 Network OS – Create CoS Mutation Map

Feature	Description	CLI Commands
QoS	This template is used to create the CoS-to-CoS mutation QoS map name	qos map cos-mutation $<MapName|STRING> $<MapValue|STRING>

TABLE 46 Network OS – Create LLDP Profile

Feature	Description	CLI Commands
QoS	This template is used to create LLDP profile and configure LLDP profile parameters	protocol lldp profile $<profileName|STRING> description $<description|STRING> hello $<frequency|INTEGER> multiplier $<holdTime|INTEGER> advertise dcbx-fcoe-logical-link-tlv advertise dcbx-fcoe-app-tlv

TABLE 47 Network OS – Create Port Profile

Feature	Description	CLI Commands
AMPP	Creates the port profile and its sub profile.	port-profile $<ProfileName|STRING> ! create vlan profile in access mode vlan-profile switchport switchport mode access switchport access vlan $<AccessVlanId|INTEGER> exit ! create qos-profile qos-profile cee default exit !create security-profile security-profile mac access-group $<ACLName|STRING> in exit exit ! activate port profile port-profile $<ProfileName|STRING> activate ! associate mac statically port-profile $<ProfileName|STRING> static $<AssosicateMACAddress1|MAC> port-profile $<ProfileName|STRING> static $<AssosicateMACAddress2|MAC> port-profile $<ProfileName|STRING> static $<AssosicateMACAddress3|MAC>

TABLE 48 Network OS – Create Traffic Class Map

Feature	Description	CLI Commands
QoS	This template is used to create the CoS-Traffic-Class mapping by specifying a name and the mapping	qos map cos-traffic-class $<MapName|STRING> $<MapValue|STRING>

TABLE 49 Network OS – Create VLAN Classifier Group

Feature	Description	CLI Commands
QoS	This template is used to create a VLAN classifier group and add a VLAN classifier	vlan classifier group $<GroupId|INTEGER> add rule $<RuleId|INTEGER>

TABLE 50 Network OS – Create VLAN Classifier Rule

Feature	Description	CLI Commands
QoS	This template is used to create a protocol-based or MAC address-based VLAN classifier rule	vlan classifier rule $<RuleId|INTEGER> $<VlanRule|STRING>

TABLE 51 Network OS – Delete Port Profiles

Feature	Description	CLI Commands
AMPP	Removes the port profile.	no port-profile $<ProfileName|STRING> activate no port-profile $<ProfileName|STRING>

TABLE 52 Network OS – Update ACL on Port Profile

Feature	Description	CLI Commands
AMPP	Adds a security profile to a port profile.	no port-profile $<ProfileName|STRING> activate port-profile $<ProfileName|STRING> security-profile mac access-group $<ACLToAdd|STRING> in exit port-profile $<ProfileName|STRING> activate

TABLE 53 Network OS – Update QoS on Port Profile

Feature	Description	CLI Commands
AMPP	Adds a QoS profile to a port profile.	no port-profile $<ProfileName|STRING> activate port-profile $<ProfileName|STRING> qos-profile qos cos-mutation $<CosMutationName|STRING> exit port-profile $<ProfileName|STRING> activate

TABLE 54 Network OS – Update VLAN on Port Profile

Feature	Description	CLI Commands
AMPP	Adds a VLAN profile to a port profile.	no port-profile $<ProfileName|STRING> activate port-profile $<ProfileName|STRING> vlan-profile switchport switchport mode trunk switchport trunk allowed vlan all switchport trunk allowed vlan remove $<TrunkVlanIdToRemove|INTEGER> switchport trunk native-vlan $<TrunkNativeVlanId|INTEGER> exit port-profile $<ProfileName|STRING> activate

TABLE 55 Private VLAN – Configure VLAN as a PVLAN

Feature	Description	CLI Commands
VLAN	To configure PVLAN type (Isolated, community or primary) to a VLAN.	interface vlan $<VLAN_ID|INTEGER private-vlan isolated private-vlan community private-vlan primary

TABLE 56 Private VLAN – Delete PVLAN configuration from VLAN

Feature	Description	CLI Commands
VLAN	To remove PVLAN type from VLAN interface.	interface vlan $<VLAN_ID|INTEGER> no private-vlan

TABLE 57 Private VLAN – Associate Secondary VLAN with Primary VLAN

Feature	Description	CLI Commands
VLAN	To associate secondary VLAN with primary VLAN.	interface vlan $<PRIMARY_VLAN_ID|INTEGER> private-vlan association add $<SECONDARY_VLAN_ID|INTEGER>

TABLE 58 Private VLAN – Configure PVALN mode in L2 interface

Feature	Description	CLI Commands
VLAN	To configure Layer 2 Interface as a PVLAN mode (host or promiscuous).	interface tengigabitethernet $<CEE_INTERFACE|SLOT_PORT> switchport mode private-vlan promiscuous switchport mode private-vlan host

TABLE 59 Private VLAN – Add native VLAN mode to PVLAN trunk

Feature	Description	CLI Commands
VLAN	To configure native VLAN in PVLAN trunk port.	interface tengigabitethernet $<CEE_INTERFACE|SLOT_PORT> switchport private-vlan trunk native vlan $<VLAN_ID|INTEGER>

TABLE 60 Private VLAN – Remove native VLAN from PVLAN trunk

Feature	Description	CLI Commands
VLAN	To remove native VLAN from PVLAN trunk port.	interface tengigabitethernet $<CEE_INTERFACE|SLOT_PORT> no switchport private-vlan trunk native vlan

TABLE 61 Private VLAN – Configure normal VLAN on a PVLAN trunk

Feature	Description	CLI Commands
VLAN	To configure normal VLANs on a PVLAN trunk port.	interface tengigabitethernet $<CEE_INTERFACE|SLOT_PORT> switchport switchport private-vlan trunk allowed vlan all switchport private-vlan trunk allowed vlan none switchport private-vlan trunk allowed vlan add $<VLAN_ID|INTEGER> switchport private-vlan trunk allowed vlan remove $<VLAN_ID|INTEGER> switchport private-vlan trunk allowed vlan except $<VLAN_ID|INTEGER>

TABLE 62 Private VLAN – Map primary and secondary VLAN to promiscuous port

Feature	Description	CLI Commands
VLAN	To assign Primary Vlan to Promiscuous port. This command also maps a Promiscuous port to selected secondary VLANs.	interface tengigabitethernet $<CEE_INTERFACE|SLOT_PORT> switchport switchport mode private-vlan promiscuous switchport private-vlan mapping $<PRIMARY_VLAN_ID|INTEGER> add $<SECONDARY_VLAN_ID|INTEGER>

TABLE 63 Private VLAN – Delete PVLAN mapping from promiscuous port

Feature	Description	CLI Commands
VLAN	To remove VLAN mapping from Promiscuous port.	interface tengigabitethernet $<CEE_INTERFACE|SLOT_PORT> no switchport private-vlan mapping

TABLE 64 Private VLAN – Associate Primary and Secondary VLANs to host port

Feature	Description	CLI Commands
VLAN	To associate Primary and Secondary VLANs to host port.	interface tengigabitethernet $<CEE_INTERFACE|SLOT_PORT> switchport switchport mode private-vlan host switchport private-vlan host-association $<PRIMARY_VLAN_ID|INTEGER> $<SECONDARY_VLAN_ID|INTEGER>

TABLE 65 Private VLAN – Delete PVLAN associations from host port

Feature	Description	CLI Commands
VLAN	To delete all associations from Primary VLAN to a host port.	interface tengigabitethernet $<CEE_INTERFACE|SLOT_PORT> no switchport private-vlan host-association

TABLE 66 Private VLAN – Associate Primary and Secondary VLANs to trunk port

Feature	Description	CLI Commands
VLAN	To associate Primary and Secondary VLANs to trunk port.	interface tengigabitethernet $<CEE_INTERFACE|SLOT_PORT> switchport private-vlan association trunk $<PRIMARY_VLAN_ID|INTEGER> $<SECONDARY_VLAN_ID|INTEGER>

TABLE 67 Private VLAN – Delete PVALN associations from trunk port

Feature	Description	CLI Commands
VLAN	To delete all VLAN associations from trunk port.	interface tengigabitethernet $<CEE_INTERFACE|SLOT_PORT> no switchport private-vlan association trunk $<PRIMARY_VLAN_ID|INTEGER> no switchport private-vlan association trunk $<PRIMARY_VLAN_ID|INTEGER> $<SECONDARY_VLAN_ID|INTEGER> no switchport private-vlan association trunk

TABLE 68 Private VLAN – Display private VLAN Configuration

Feature	Description	CLI Commands
VLAN	To display the private vlan status.	show vlan private-vlan

TABLE 69 VRF – VRF Creation

Feature	Description	CLI Commands
VRF	To create VRF in specific RBridge.	rbridge-id $<RBRIDGE_ID|INTEGER> vrf $<VRF_NAME|STRING>

TABLE 70 VRF – VRF Deletion

Feature	Description	CLI Commands
VRF	To delete VRF from specific RBridge.	rbridge-id $<RBRIDGE_ID|INTEGER> no vrf $<VRF_NAME|STRING>

TABLE 71 VRF – Route Distinguisher Configuration

Feature	Description	CLI Commands
VRF	To configure Route Distinguisher global to VRF context.	rbridge-id $<RBRIDGE_ID|INTEGER> vrf $<VRF_NAME|STRING> rd $<ASN:NN|STRING>

TABLE 72 VRF – Maximum routes configuration for IPV4 Address Family

Feature	Description	CLI Commands
VRF	To configure maximum number of routes per VRF for IPV4 family.	rbridge-id $<RBRIDGE_ID|INTEGER> vrf $<VRF_NAME|STRING> rd $<ASN:NN|STRING> address-family ipv4 max-route $<MAX_ROUTE|INTEGER>

TABLE 73 VRF – Route Targets Export and/or Import Configuration

Feature	Description	CLI Commands
VRF	To configure list of import and/or export route target communities for the specified VRF.	rbridge-id $<RBRIDGE_ID|INTEGER> vrf $<VRF_NAME|STRING> address-family ipv4 route-target export $<ASN:NN_EXPORT|STRING> route-target import $<ASN:NN_IMPORT|STRING> route-target both $<ASN:NN_BOTH|STRING>

TABLE 74 VRF – Delete Route Targets Export and/or Import Configuration

Feature	Description	CLI Commands
VRF	To delete list of import and/or export route target communities for the specified VRF.	rbridge-id $<RBRIDGE_ID|INTEGER> vrf $<VRF_NAME|STRING> address-family ipv4 no route-target export $<ASN:NN|STRING> no route-target import $<ASN:NN|STRING> no route-target both $<ASN:NN|STRING>

TABLE 75 VRF – Display VRF Information

Feature	Description	CLI Commands
VLAN	To display the VRF details.	show vrf detail show vrf rbridge-id $<RBRIDGE_ID|INTEGER> show vrf $<VRF_NAME|STRING>

TABLE 76 IronWare OS VLAN – Remove interfaces from VLAN as untagged

Feature	Description	CLI Commands
VLAN	To remove interfaces from the VLAN as untagged.	vlan $<VLAN_ID|INTEGER> no untagged ethernet $<STACKID_SLOT_PORT|STRING>

TABLE 77 IronWare OS VLAN – VLAN Creation

Feature	Description	CLI Commands
VLAN	To create a VLAN.	vlan $<VLAN_ID|INTEGER>

TABLE 78 IronWare OS VLAN – VLAN Deletion

Feature	Description	CLI Commands
VLAN	To delete a VLAN.	no vlan $<VLAN_ID|INTEGER>

TABLE 79 IronWare OS VLAN – Assign interfaces to VLAN as tagged

Feature	Description	CLI Commands
VLAN	To assign interfaces to the VLAN as tagged.	vlan $<VLAN_ID|INTEGER> tagged ethernet $<STACKID_SLOT_PORT|STRING>

TABLE 80 IronWare OS VLAN – Remove interfaces from VLAN as tagged

Feature	Description	CLI Commands
VLAN	To remove interfaces from the VLAN as tagged.	vlan $<VLAN_ID|INTEGER> no tagged ethernet $<STACKID_SLOT_PORT|STRING>

TABLE 81 IronWare OS VLAN – Assign interfaces to VLAN as untagged

Feature	Description	CLI Commands
VLAN	To assign interfaces to the VLAN as untagged.	vlan $<VLAN_ID|INTEGER> untagged ethernet $<STACKID_SLOT_PORT|STRING>

TABLE 82 IronWare OS VLAN – Configure virtual routing interface

Feature	Description	CLI Commands
VLAN	To configure a virtual routing interface on a VLAN.	vlan $<VLAN_ID|INTEGER> router-interface ve $<STACKID_SLOT_PORT|STRING>

TABLE 83 IronWare OS VLAN – Enable Spanning Tree Protocol on IOS VLAN

Feature	Description	CLI Commands
VLAN	To enable spanning tree protocol on VLAN.	vlan $<VLAN_ID|INTEGER> spanning-tree

TABLE 84 IronWare OS VLAN – Disable Spanning Tree Protocol on IOS VLAN

Feature	Description	CLI Commands
VLAN	To disable spanning tree protocol on VLAN.	vlan $<VLAN_ID|INTEGER> no spanning-tree

TABLE 85 Network OS VLAN – VLAN Interface Creation

Feature	Description	CLI Commands
VLAN	To create a VLAN Interface.	interface vlan $<VLAN_ID|INTEGER>

TABLE 86 Network OS VLAN – VLAN Interface Deletion

Feature	Description	CLI Commands
VLAN	To delete a VLAN Interface.	no interface vlan $<VLAN_ID|INTEGER>

TABLE 87 Network OS VLAN – Layer2 Switch Port Configuration

Feature	Description	CLI Commands
VLAN	To confiure an interface port as a Layer 2 switch port.	interface tengigabitethernet $<INTERFACE_NUM|SLOT_PORT> switchport

TABLE 88 Network OS VLAN – Trunk Interface Configuration with allowed VLAN list

Feature	Description	CLI Commands
VLAN	To configure the interface as a trunk interface and Specify whether all, one, or none of the VLAN interfaces are allowed to transmit and receive through the DCB interface.	interface tengigabitethernet $<INTERFACE_NUM|SLOT_PORT> switchport switchport mode trunk switchport trunk allowed vlan all switchport trunk allowed vlan none switchport trunk allowed vlan add $<VLAN_ID|INTEGER> switchport trunk allowed vlan remove $<VLAN_ID|INTEGER> switchport trunk allowed vlan except $<VLAN_ID|INTEGER>

TABLE 89 Network OS VLAN – Configure Layer2 Interface as an Interface Port

Feature	Description	CLI Commands
VLAN	To configure Layer2 interface as an interface port.	interface tengigabitethernet $<INTERFACE_NUM|SLOT_PORT> no switchport

TABLE 90 Network OS VLAN – Native VLAN Configuration

Feature	Description	CLI Commands
VLAN	To confiure the trunk interface as a native VLAN.	interface tengigabitethernet $<INTERFACE_NUM|SLOT_PORT> switchport switchport mode trunk switchport trunk native-vlan $<VLAN_ID|INTEGER>

TABLE 91 Network OS VLAN – Disable Native VLAN Configuration

Feature	Description	CLI Commands
VLAN	To disable native VLAN from a trunk interface.	interface tengigabitethernet $<INTERFACE_NUM|SLOT_PORT> no switchport trunk native-vlan $<VLAN_ID|INTEGER>

TABLE 92 Network OS VLAN – Access Interface Configuration

Feature	Description	CLI Commands
VLAN	To configure the interface as an access interface.	interface tengigabitethernet $<INTERFACE_NUM|SLOT_PORT> switchport switchport mode access switchport access vlan $<VLAN_ID|INTEGER>

TABLE 93 Network OS VLAN – Disable Access Interface Configuration

Feature	Description	CLI Commands
VLAN	To disable the access interface.	interface tengigabitethernet $<INTERFACE_NUM|SLOT_PORT> no switchport access vlan $<VLAN_ID|INTEGER>

TABLE 94 Network OS VLAN – Enable Spanning Tree Protocol on NOS VLAN

Feature	Description	CLI Commands
VLAN	To enable spanning tree protocol on VLAN for Network OS 4.0.	interface vlan $<VLAN_ID|INTEGER> no spanning-tree shutdown ! To enable spanning tree protocol on VLAN for NOS 3.0. interface vlan $<VLAN_ID|INTEGER> no shutdown

TABLE 95 Network OS VLAN – Disable Spanning Tree Protocol on Network OS VLAN

Feature	Description	CLI Commands
VLAN	To disable spanning tree protocol on VLAN for Network OS version 4.0 and later.	interface vlan $<VLAN_ID|INTEGER> spanning-tree shutdown
	To disable spanning tree protocol on VLAN for Network OS greater than or equal to (>=) version 3.0 and less than (<) version 4.0 .	interface vlan $<VLAN_ID|INTEGER> shutdown

Appendix

Troubleshooting

H

In this chapter

Application Configuration Wizard troubleshooting

The following section states a possible issue and the recommended solution for Management application Configuration Wizard errors.

Problem	Resolution
Unable to launch the Management application Configuration Wizard on a Windows Vista, Windows 7,or Windows 2008 R2 system	The Windows Vista, Windows 7,or Windows 2008 R2 system enables the User Access Control (UAC) option by default. When the UAC option is enabled, the Configuration Wizard cannot launch. If the Configuration Wizard does not launch, use one of the following options to disable the UAC option: The following are the various ways we can disable UAC in vista: **Disable using msconfig by completing the following steps.** 1 Select **Start > Run**. 2 Type msconfig on the **Run** dialog box and click **OK**. 3 Click the **Tools** tab on the **System Configuration Utility**. 4 Scroll down to and select the **Disable UAC** tool name. 5 Click **Launch**. A command window displays and runs the disable UAC command. When the command is complete, close the window. 6 Close the **System Configuration Utility**. 7 Restart the computer to apply changes. **NOTE:** You can re-enable UAC using the above procedure and selecting the **Enable UAC** tool name in step 4. **Disable using regedit by completing the following steps.** **NOTE:** Before making changes to the registry, make sure you have a valid backup. In cases where you're supposed to delete or modify keys or values from the registry it is possible to first export that key or value(s) to a .REG file before performing the changes. 1 Select **Start > Run**. 2 Type regedit on the **Run** dialog box and click **OK**. 3 Navigate to the following registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System 4 Right-click the **EnableLUA** value and select Modify. 5 Change the **Value data** field to 0 on the **Edit DWORD Value** dialog box and click **OK**. 6 Close the **Registry Editor**. 7 Restart the computer to apply changes. **NOTE:** You can re-enable UAC using the above procedure and changing the **Value data** field to 1 in step 5.

Browser troubleshooting

The following section states a possible issue and the recommended solution for browser errors.

Problem	Resolution
The **Cancel** button does not work on the **Report via E-mail** dialog box when you use the Mozilla Firefox browser.	Mozilla Firefox Browser does not support window close script. Click the browser Close button to cancel. **NOTE:** The **Cancel** button still displays on all **Report via E-mail** dialog boxes.

Client browser troubleshooting

The following section states a possible issue and the recommended solution for client browser errors.

Problem	Resolution
Downloading Client from a Internet Explorer Browser over HTTPS	If the JNLP file does not launch automatically, use one of the following options: • Complete the following steps. 1 Save the JNLP file to the local host. 2 Launch the JNLP file manually. • In Internet Explorer 7, complete the following steps. 1 Select **Tools > Internet Options**. 2 Click the **Advanced** tab. 3 Clear the **Do not save encrypted pages to disk** check box. If the browser warns you about the security certificate, use the fully qualified hostname to launch the web page.

Configuration backup and restore troubleshooting

The following section states a possible issue and the recommended solution for configuration backup and restore errors.

Problem	Resolution

Configuration backup and restore (Network OS devices only) using SCP/SFTP does not work because of one of the following issues:
• For internal SCP/SFTP server, the application was uninstalled and reinstalled without migration
• For external SCP/SFTP server, the SSH handshake keypair is changed
- manually
- due to an external server reinstall
- due to the SCP/SFTP server preference (Options dialog box) being changed from built-in to external (installed on same machine) or vice versa
	Clear the SSH (SCP/SFTP) server IP address or hostname from the known_hosts table of the device.
	• For Network OS devices running firmware version 3.0 and later, use the following command:
	`sw0# clear ssh-key SSH_server_IP_address`
	where *SSH_server_IP_address* is the IP address of the SSH server you want to delete.
	• For Network OS devices running firmware version 2.1.1b, use the following command:
	`sw0# execute-script sshdeleteknownhost`
	`IP Address/Hostname to be deleted: SSH_server_IP_address`
	where *SSH_server_IP_address* is the IP address of the SSH server you want to delete.

Configuration backup and restore (Network OS devices only) using an external SCP server does not work after reinstalling the application or the external SCP server on the Host machine.	Clear the SCP server IP address or hostname from the known_hosts table of the device using the following command: `sw0# FID10:root> ssh-keygen -R Host_Name` where *Host_Name* is the IP address or host name of the external SCP server.

Element Manager troubleshooting

The following section states a possible issue and the recommended solution for Element Manager errors.

Problem	Resolution
Unable to launch Element Manager from the Management application.	To launch Element Manager from the Management application, your local system's browser must run the Java Web Start application. To turn on Java content in the browser, complete the following steps. 1 Launch **Java Control Panel**. **For Windows**: Refer to http://java.com/en/download/help/win_controlpanel.xml. **For Linux:** Follow the steps listed. a Open the Terminal window. b Go to the Java installation directory: *cd /java/jre1.7.0_45/bin* (change the name of the directory to where you have installed Java). c Type **./ControlPanel** to open the **Java Control Panel**. 2 In the **Java Control Panel**, click the **Security** tab. 3 Select the **Enable Java content in the browser** check box. 4 Click **Apply**. When the **Windows User Account Control** (UAC) dialog box displays, allow permissions to make the changes. 5 Click **OK** in the Java Plug-in confirmation window. 6 Launch Element Manager.

Firmware download troubleshooting

The following section states a possible issue and the recommended solution for firmware download errors.

Problem	Resolution
If you configured an internal FTP server and the Management application server is running IPv6, firmware download is not supported.	Choose from one of the following options: • If the Management application is running IPv6 only, configure an external FTP server. • If the Management application is running IPv4 and IPv6, configure IPv4 to be the preferred address.

Problem	Resolution
Firmware download using SCP/SFTP does not work because of one of the following issues: • For internal SCP/SFTP server, the application was uninstalled and reinstalled without migration • For external SCP/SFTP server, the SSH handshake keypair is changed - manually - due to an external server reinstall - due to the SCP/SFTP server preference (Options dialog box) being changed from built-in to external (installed on same machine) or vice versa	Clear the SSH (SCP/SFTP) server IP address or hostname from the known_hosts table of the device. • For Fabric OS devices, use the following command: `sw0:FID128:admin>` **`sshutil delknownhost`** `IP Address/Hostname to be deleted:` *`SSH_server_IP_address`* where *`SSH_server_IP_address`* is the IP address of the SSH server you want to delete. • For Network OS devices running firmware version 3.0 and later, use the following command: `sw0#` **`clear ssh-key`** *`SSH_server_IP_address`* where *`SSH_server_IP_address`* is the IP address of the SSH server you want to delete. • For Network OS devices running firmware version 2.1.1b, use the following command: `sw0#` **`execute-script sshdeleteknownhost`** `IP Address/Hostname to be deleted:` *`SSH_server_IP_address`* where *`SSH_server_IP_address`* is the IP address of the SSH server you want to delete.
Firmware download using an external SCP server does not work after reinstalling the application or the external SCP server on the Host machine.	Clear the SCP server IP address or hostname from the known_hosts table of the device using the following command: `sw0# FID10:root> ssh-keygen –R` *`Host_Name`* where *`Host_Name`* is the IP address or host name of the external SCP server.

Launch Client troubleshooting

The following section states a possible issue and the recommended solution if you are unable to launch the remote client.

Problem	Resolution
Remote client does not upgrade from versions prior to 11.0.	The remote client does not automatically upgrade when you select the remote client shortcut of client versions earlier than 11.0. To clear the old client and launch the new remote client version, complete the following steps. 1 Clear the previous version from the Java cache,. a Select **Start > Settings > Control Panel > Java**. The **Java Control Panel** dialog box displays. b Click **View** on the **General** tab. The **Java Cache Viewer** dialog box displays. c Right-click the application and select **Delete**. d Click **Close** on the **Java Cache Viewer** dialog box. e Click **OK** on the **Java Control Panel** dialog box. 2 Launch the remote client. a Open a web browser and enter the IP address of the Management application server in the **Address** bar. If the web server port number does not use the default (443 if is SSL Enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address. For example, *IP_Address*:*Port_Number*. The Management application web start screen displays. b Click the Management application web start link. The **Log In** dialog box displays. c Enter your user name and password. The defaults are **Administrator** and **password**, respectively. **NOTE:** Do not enter *Domain**User_Name* in the **User ID** field for LDAP server authentication. d Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in. e Click **Login**. f Click **OK** on the **Login Banner** dialog box. The Management application displays. **NOTE:**

Problem	Resolution
Unable to log into the Client (the application does not launch when you use a valid user name and password and exceptions are thrown in the client side).	Use one the following procedures to configure the IP address in the host file. **Windows operating systems** 1 Log in using the 'Administrator' privilege. 2 Select **Start > Run**. 3 Type drivers in the **Open** field and press **Enter**. 4 Go to the ‘etc’ folder and open the ‘hosts’ file using a text editor. 5 Add the IP address and host name of the client in the following format: *IP_Address Host_Name*. For example, 127.0.0.1 localhost 6 Save and exit the file. **Unix operating systems** 1 Log in using the 'root' privilege. 2 Open the ‘/etc/hosts’ file using a text editor. 3 Add the IP address and host name of the client in the following format: *IP_Address Host_Name*. For example, 127.0.0.1 localhost 4 Save and exit the file.
Unable to launch the remote client (the SSL setting, web server port number, or server starting point number changed during the server upgrade).	To remove the old link and launch the correct remote client version, complete the following steps. 1 Clear the previous version from the Java cache,. a Select **Start > Settings > Control Panel > Java**. The **Java Control Panel** dialog box displays. b Click **View** on the **General** tab. The **Java Cache Viewer** dialog box displays. c Right-click the application and select **Delete**. d Click **Close** on the **Java Cache Viewer** dialog box. e Click **OK** on the **Java Control Panel** dialog box. 2 Log into the remote client from the browser. a Open a web browser and enter the IP address of the Management application server in the **Address** bar. If the web server port number does not use the default (443 if is SSL Enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address. For example, *IP_Address*:*Web_Server_Port_Number*. The Management application web start screen displays. b Click the Management application web start link. The **Log In** dialog box displays. c Enter your user name and password. The defaults are **Administrator** and **password**, respectively. **NOTE:** Do not enter *Domain\User_Name* in the **User ID** field for LDAP server authentication. d Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in. e Click **Login**. f Click **OK** on the **Login Banner** dialog box. The Management application displays. **NOTE:**

Master Log and Switch Console troubleshooting

The following section states a possible issue and the recommended solution for switch console errors.

Problem	Resolution
Too many login and log messages received on switch console and and Master Log due to lazy polling.	**NOTE:** This setting cannot be disabled for DCB switches. To disable lazy polling, complete the following steps. 1 Select **Discover > IP Products**. The **Discover Setup - IP** dialog box displays. 2 Click the **Global Settings** tab. 3 Click the **Preferences** tab. 4 Clear the **Enable lazy polling** check box. 5 Click **Apply** to save your work. 6 Click **Close** to close the **Discover Setup - IP** dialog box. 7 Click **Yes** on the confirmation message.

Patch troubleshooting

The following section states a possible issue and the recommended solution for patch errors.

Problem	Resolution
Unable to launch the SMC on a Windows Vista,Windows 7,or Windows 2008 R2 system	The Windows Vista,Windows 7,or Windows 2008 R2 system enables the User Access Control (UAC) option by default. When the UAC option is enabled, the SMC cannot launch. If the SMC does not launch, use one of the following options to disable the UAC option: The following are the various ways we can disable UAC in vista: **Disable using msconfig by completing the following steps.** 1 Select **Start > Run**. 2 Type msconfig on the **Run** dialog box and click **OK**. 3 Click the **Tools** tab on the **System Configuration Utility**. 4 Scroll down to and select the **Disable UAC** tool name. 5 Click **Launch**. A command window displays and runs the disable UAC command. When the command is complete, close the window. 6 Close the **System Configuration Utility**. 7 Restart the computer to apply changes. **NOTE:** You can re-enable UAC using the above procedure and selecting the **Enable UAC** tool name in step 4. **Disable using regedit by completing the following steps.** **NOTE:** Before making changes to the registry, make sure you have a valid backup. In cases where you're supposed to delete or modify keys or values from the registry it is possible to first export that key or value(s) to a .REG file before performing the changes. 1 Select **Start > Run**. 2 Type regedit on the **Run** dialog box and click **OK**. 3 Navigate to the following registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System 4 Right-click the **EnableLUA** value and select Modify. 5 Change the **Value data** field to 0 on the **Edit DWORD Value** dialog box and click **OK**. 6 Close the **Registry Editor**. 7 Restart the computer to apply changes. **NOTE:** You can re-enable UAC using the above procedure and changing the **Value data** field to 1 in step 5.

Professional edition login troubleshooting

The following section states a possible issue and the recommended solution for Professional edition login errors.

TABLE 96 Professional edition login troubleshooting

Problem	Resolution
Login Failed. Only one client allowed. One client session is active or has not yet timed out.	If you closed the client using Windows Task Manager (End Task or Process) or using Unix process ID (kill command), successful relaunch of the application may take up to 2 minutes.

Server troubleshooting

The following section states a possible issue and the recommended solution for server errors.

Problem	Resolution
Management server exits unexpectedly on Red hat Linux 6.1	A possible cause is low swap space configured on the system. As per the standard recommendation, swap should equal 2 times physical RAM for up to 2 GB of physical RAM, and then an additional 1 times physical RAM for any amount above 2 GB, but never less than 32 MB. Therefore, if M = Amount of RAM in GB and S = Amount of swap in GB, then If M < 2 S = M *2 Else S = M + 2

Server Management Console troubleshooting

The following section states a possible issue and the recommended solution for server management console errors.

Problem	Resolution
Unable to launch the SMC on a Windows Vista,Windows 7 , or Windows 2008 R2 system	The Windows Vista,Windows 7,or Windows 2008 R2 system enables the User Access Control (UAC) option by default. When the UAC option is enabled, the SMC cannot launch. If the SMC does not launch, use one of the following options to disable the UAC option: The following are the various ways we can disable UAC in vista: **Disable using msconfig by completing the following steps.** 1 Select **Start > Run**. 2 Type msconfig on the **Run** dialog box and click **OK**. 3 Click the **Tools** tab on the **System Configuration Utility**. 4 Scroll down to and select the **Disable UAC** tool name. 5 Click **Launch**. A command window displays and runs the disable UAC command. When the command is complete, close the window. 6 Close the **System Configuration Utility**. 7 Restart the computer to apply changes. **NOTE:** You can re-enable UAC using the above procedure and selecting the **Enable UAC** tool name in step 4. **Disable using regedit by completing the following steps.** **NOTE:** Before making changes to the registry, make sure you have a valid backup. In cases where you're supposed to delete or modify keys or values from the registry it is possible to first export that key or value(s) to a .REG file before performing the changes. 1 Select **Start > Run**. 2 Type regedit on the **Run** dialog box and click **OK**. 3 Navigate to the following registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System 4 Right-click the **EnableLUA** value and select Modify. 5 Change the **Value data** field to 0 on the **Edit DWORD Value** dialog box and click **OK**. 6 Close the **Registry Editor**. 7 Restart the computer to apply changes. **NOTE:** You can re-enable UAC using the above procedure and changing the **Value data** field to 1 in step 5.

Problem	Resolution
Unable to launch the SMC on a Windows Vista or Windows 7 system continued	**Disable using the Group Policy by completing the following steps.** You can perform this procedure on you local machine using Local Group Policy editor or for many computers at the same time using the Active Directory-based Group Policy Object (GPO) editor. To disable using the Local Group Policy editor, complete the following steps. 1 On your local Vista computer, select **Start > Run**. 2 Type gpedit.msc on the **Run** dialog box and click **OK**. 3 Browse to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options** in the Group Policy editor. 4 In the right pane scroll to the User Access Control policies (at the bottom of the pane). 5 Right-click the **Behavior of the elevation prompt for Administrators in Admin Approval Mode** policy and select Properties. 6 Select the **No Prompt** option and click **OK**. 7 Right-click the **Detect application installations and prompt for elevation** policy and select **Properties**. 8 Select the **Disabled** option and click **OK**. 9 Right-click the **Run all administrators in Admin Approval Mode** policy and select **Properties**. 10 Select the **Disabled** option and click **OK**. 11 Close the Group Policy editor. 12 Restart the computer to apply changes. To disable using the Active Directory-based GPO editor, complete the following steps. 1 On a Vista computer that is a member of a domain, select **Start > Run**. 2 Type gpedit.msc on the **Run** dialog box and click **OK**. 3 Browse to the required GPO that is linked to the OU or domain where the Vista computers are located, then edit it 4 Browse to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options** in the Group Policy editor. 5 In the right pane scroll to the User Access Control policies (at the bottom of the pane). 6 Right-click the **Behavior of the elevation prompt for Administrators in Admin Approval Mode** policy and select **Properties**. 7 Select the **No Prompt** option and click **OK**. 8 Right-click the **Detect application installations and prompt for elevation** policy and select **Properties**. 9 Select the **Disabled** option and click **OK**. 10 Right-click the **Run all administrators in Admin Approval Mode** policy and select **Properties**. 11 Select the **Disabled** option and click **OK**. 12 Close the Group Policy editor. 13. Restart the computer to apply changes.

Supportsave troubleshooting

The following section states a possible issue and the recommended solution for supportsave errors.

Problem	Resolution
Cannot capture support save information.	Capture support show by running the batch file from the *Install_Home*/bin/supportshow.bat from Windows and UNIX systems. 1 *Open Install_Home*\bin\supportsave.bat. 2 Edit file `supportsave dbuser dbpasswd [tareget-dir] [pause-option]`. **NOTE:** Unreachable switches increase the time needed to collect supportSave data.

Technical support data collection troubleshooting

The following section states a possible issue and the recommended solution for technical support data collection errors.

Problem	Resolution
Technical support data collection using SCP/SFTP does not work because of one of the following issues: • For internal SCP/SFTP server, the application was uninstalled and reinstalled without migration • For external SCP/SFTP server, the SSH handshake keypair is changed - manually - due to an external server reinstall - due to the SCP/SFTP server preference (Options dialog box) being changed from built-in to external (installed on same machine) or vice versa	Clear the SSH (SCP/SFTP) server IP address or hostname from the known_hosts table of the device. • For Fabric OS devices, use the following command: `sw0:FID128:admin>` **`sshutil delknownhost`** `IP Address/Hostname to be deleted:` *`SSH_server_IP_address`* where *`SSH_server_IP_address`* is the IP address of the SSH server you want to delete. • For Network OS devices running firmware version 3.0 and later, use the following command: `sw0#` **`clear ssh-key`** *`SSH_server_IP_address`* where *`SSH_server_IP_address`* is the IP address of the SSH server you want to delete. • For Network OS devices running firmware version 2.1.1b, use the following command: `sw0#` **`execute-script sshdeleteknownhost`** `IP Address/Hostname to be deleted:` *`SSH_server_IP_address`* where *`SSH_server_IP_address`* is the IP address of the SSH server you want to delete.
Technical support data collection using an external SCP server does not work after reinstalling the application or the external SCP server on the Host machine.	Clear the SCP server IP address or hostname from the known_hosts table of the device using the following command: `sw0# FID10:root> ssh-keygen –R` *`Host_Name`* where *`Host_Name`* is the IP address or host name of the external SCP server.

Wireless troubleshooting

After discovery, the Management application inspects the trap listener and syslog recipient configuration on wireless controllers. If there is a problem with the registration, the Management application changes the “registration success” master log event to a warning event with additional message text. The following section states the possible issues and the associated Master Log message that displays:

TABLE 97 Wireless troubleshooting

Problem	Master log warning message
The Management application successfully registers itself as SNMP trap recipient on the wireless controller; however, trap generation is disabled on the device.	Server <address> is successfully registered as SNMP Trap recipient to the switch <device_address>; but trap generation is disabled on switch.
The Management application successfully registers itself as syslog recipient on the wireless controller; however, logging is disabled on the device.	Server <address> is successfully registered as Syslog recipient to the switch <device_address>; but logging is disabled on switch.

TABLE 97 Wireless troubleshooting

Problem	Master log warning message
The Management application successfully registers itself as syslog recipient on the wireless controller as the secondary or ternary recipient (primary slot is already occupied). The wireless controller sends syslog messages to secondary or ternary recipients only if primary recipient is not reachable. Therefore, even though the Management application is registered as a syslog recipient it may not receive any messages.	Server <address> is successfully registered as Syslog recipient to the switch <device_address>; but <address> is not the primary syslog recipient.
The Management application successfully registers itself as syslog recipient on the wireless controller; however, it is non-primary recipient and logging is disabled on device.	Server <address> is successfully registered as Syslog recipient to the switch <device_address>; but logging is disabled on switch and <address> is not the primary syslog recipient.

Zoning troubleshooting

The following section states some possible issues and recommended solutions for zoning errors.

Problem	Resolution
Cannot perform zoning on a new switch.	You must use telnet (or the **Product Type and Access** tab in the **Add Properties** dialog box) to change the default password on the new switch before you can use the Management application to perform zoning.
When configuring a large zone configuration a switch displays offline during discovery.	If a large zone configuration is configured in a fabric, switches may temporarily display as being offline during discovery. Wait for the next discovery cycle and click the **Refresh** button on the toolbar.
When activating a large zone configuration on a two-switch fabric on UNIX platforms, an error message displays stating “Failed to perform the requested zoning action: Failed to zone due to exception.”	Although the error message states that the requested zoning action failed, the zone configuration will be correctly activated. Wait for the next zoning polling to occur. This issue only occurs on UNIX systems.
Zoning activation message displays for a long time, but zone configuration is not activated.	Telnet zoning can take a long time. To improve speed, open the **Discover Setup** dialog box (**Discover > Setup**) and add the IP address for the device to the **Selected Individual Addresses** list.
Out of memory error caused by running a zoning report for a large zone configuration (1 MB) in a medium-sized SAN due to a third party tool.	You must increase the client memory allocation by completing “Configuring memory allocation settings” on page 166.

H Zoning troubleshooting

Appendix

Database Fields

In this appendix

Database tables and fields

NOTE
The primary keys are marked by an asterisk (*)

TABLE 16 ACH_CALL_CENTER

Field	Definition	Format	Size
ID *	Unique generated database identifier.	int	
NAME	Name of the Call Center.	varchar	256

TABLE 17 ACH_CALL_CENTER_CONFIG

Field	Definition	Format	Size
KEY_ *	Key to identify the specific configuration of the Call Center.	varchar	256
CALL_CENTER_ID *	ID of the Call Center.	int	
VALUE	Value of specific configuration identified by Key of the Call Center.	varchar	256

TABLE 18 ACH_EVENT

Field	Definition	Format	Size
ID *	Unique generated database identifier.	int	
REASON_CODE	Reason code of the event.	varchar	256
FRU_CODE	FRU code of the event.	varchar	256
DESCRIPTION	Description of the event.	varchar	256
SEVERITY	Severity of the event.	int	

TABLE 18 ACH_EVENT (Continued)

Field	Definition	Format	Size
TYPE	Type of the event.	varchar	256
CONTRIBUTOR_PATTERN	Indicates the Contributor pattern to be used for searching the event contributor in event description. In some cases, FOS uses same message id for different events (e.g MAPS events). To increase the filtering capability of Call Home events, this contributor pattern string is used along with message id. If the event has unique message id, then contributor pattern string will be empty.	varchar	64

TABLE 19 ACH_EVENT_FILTER_MAP

Field	Definition	Format	Size
FILTER_ID *	ID of the event filter.	int	
EVENT_ID *	Event ID which needs to be associated with the filter.	int	

TABLE 20 ACH_FILTER

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
NAME	Name of the event filter.	varchar	256
DESCRIPTION	Description of the event filter.	varchar	256

TABLE 21 ACH_INFO

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
SWITCH_WWN	WWN of the switch.	varchar	23
FILTER_ID	If an event filter is assigned to the switch - the filter ID if no filter is assigned - null.	int	
CALL_CENTER_ID	ID of the call center to which the switch is assigned.	int	
SUPPORT_SAVE	1 = Support save is enabled for the switch. 0 = Support save is disabled for the switch.	smallint	
MANAGED_ELEMENT_ID	Managed element Id for the device. Default value is -1.	int	

TABLE 22 AD_GROUP

Field	Definition	Format	Size
ID *	Unique generated database identifier.	int	
NAME	Name of the active directory group.	varchar	256
EMAIL	Active Directory Group Email Address.	varchar	1024
SOURCE_SERVER_NETWORK_ADDRESS	The LDAP Server Network Address from which the Active directory group is fetched	varchar	255

TABLE 23 ADAPTER_DRIVER_FILE_DETAILS

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
FILE_NAME	Name of the driver file	varchar	64
MAJOR_VERSION	Major version of the driver file	smallint	
MINOR_VERSION	Minor version of the driver file	smallint	
MAINTENANCE	Maintenance version of the driver file	smallint	
PATCH	Patch details of the driver file	varchar	32
SUPPORTED_OS	Holds multiple flavors of the OS	varchar	1024
OS_ARCHITECTURE	Supported OS architecture	varchar	32
IMPORTED DATE	Imported date of the driver file	timestamp with time zone	
RELEASE DATE	Release date of the driver file	timestamp with time zone	
LOCATION	Location of the adapter driver file in the repository	varchar	1024

TABLE 24 ADAPTER_PORT_CONFIG_DETAILS

Field	Definition	Format	Size
CONFIG_ID	Configuration ID	int	
PROPERTY_ID	Adapter port property ID	int	
VALUE	User configured adapter port property value	varchar	256

TABLE 25 ADAPTER_PORT_CONFIG_PROPERTY

Field	Definition	Format	Size
ID	Adapter port property ID	int	
NAME	Holds the name of the adapter port property	varchar	64
VALUE_LIST	Holds possible values for each adapter port property	varchar	2048
DEFAULT_VALUE	Holds the default value of the port property	varchar	256
DATA_TYPE		int	
GROUP_NAME	Holds thegroup name of the port property.	varchar	256

TABLE 26 AOR_DEVICE_GROUP_MAP

Field	Definition	Format	Size
AOR_ID	ID of the AOR.	int	
DEVICE_GROUP_ID	The Product Group which is in the AOR.	int	

TABLE 27 AOR_DEVICE_MAP

Field	Definition	Format	Size
AOR_ID	ID of AOR	int	
DEVICE_ID	The DEVICE ID can be IP Product or ServerIron ID which is in the AOR	int	

TABLE 28 AOR_FABRIC_MAP

Field	Definition	Format	Size
AOR_ID	ID of AOR	int	
FABRIC_ID	FABRIC ID which is in the AOR	int	

TABLE 29 AOR_HOST_MAP

Field	Definition	Format	Size
AOR_ID	ID of AOR	int	
HOST_ID	HOST ID which is in the AOR	int	

TABLE 30 AOR_INM_PORT_GROUP_MAP

Field	Definition	Format	Size
AOR_ID	ID of AOR	int	
PORT_GROUP_ID	IP of port group	int	

TABLE 31 AOR_VIP_SERVER_MAP

Field	Definition	Format	Size
AOR_ID	The column holds ID of an AOR. It is Foreign Key and refers to ID column of AOR table	int	
VIP_SERVER_ID	The column holds ID of VIP Server. It is Foreign Key and refers to ID column of VIP_SERVER table	int	

TABLE 32 AUTO_TRACE_DUMP

Field	Definition	Format	Size
CORE_SWITCH_ID		int	
ENABLED	The enabled or disabled state of automatic trace dump transfer on the switch	smallint	
PROTOCOL	The protocol Unknown(0)/FTP(1)/SCP(2) to be used for transfer	smallint	
IP_ADDRESS	The IP address of the host	varchar	64
USER_NAME	User name	varchar	64
LOCATION	Location of the directory where trace dump files are to be saved	varchar	1024
PASSWORD	User password	varchar	64

TABLE 33 AVAILABLE_FLYOVER_PROPERTY

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
NAME	Name of the available property to be included in the flyover display.	varchar	40
TYPE	Indicates the flyover property type. Product property is 0, Connection property is 1, User Defined property is 2, Cee Product property is 3, Cee Connection property is 4, Host property is 5.	smallint	
DEFAULT_SELECTION	Value 1 in the column indicates default selected product/connection property and 0 indicates not included in the default list.	smallint	

TABLE 34 BIRTREPORT_PARAMETER

Field	Definition	Format	Size
ID	The primary key of the table.	int	
RUN_ID	References the ID column in the BIRTREPORT_RUN_TEMPLATE table.	int	
PARAMETER-TYPE	Control type of the parameter. • 1 - Text Box • 2 - List Box • 3 - Radio Button	int	
PARAMETER_NAME	Name of the parameter in the report template design.	varchar	128
PROMPT_TEXT	Text Label for the parameter. This value will be displayed on the GUI.	varchar	256
DATA_TYPE	Data type of the parameter. Possible values are: • 1 - String • 2 - Float • 3 - Decimal • 4 - Date and Time • 5 - Boolean • 6 - Integer • 7 - Date • 8 - Time	int	
PARAMETER_VALUE	Value of the Parameter.	varchar	256

TABLE 35 BIRTREPORT_RUN_TEMPLATE

Field	Definition	Format	Size
ID	The primary key of the table.	int	
SCHEDULE_ID	References the ID column in the BIRTREPORT_SCHEDULE_CONFIG table.	int	

TABLE 35 BIRTREPORT_RUN_TEMPLATE (Continued)

Field	Definition	Format	Size
REPORT_TEMPLATE_TITLE	Report Template title. This name is the same as the title name in the REPORT_TEMPLATE table. There is no foreign key relation here as the user may delete and add a template but the schedule should still hold good if looked up by title. Also title is unique in the REPORT_TEMPLATE table.	varchar	256
NAME	Name of the generated report file.	varchar	256

TABLE 36 BIRTREPORT_SCHEDULE_CONFIG

Field	Definition	Format	Size
ID	The primary key of the table.	int	
DEPLOYMENT_ID	References the ID column in the DEPLOYMENT_CONFIGURATION table.	int	
NAME	Name of the schedule.	varchar	128
REPORT_STORE_LOCATION	Path to the location where the generated report files are stored.	varchar	256
OVERWRITE	0 and 1 are allowed values.1 indicates overwrite is true. I.e., every run of the schedule will overwrite the previous output.0 indicates archive. I.e., every run of the schedule will create a new folder in the store location with timestamp to ensure that output of all the runs will be archived.	int	
FORMAT_TYPE	Possible values are 0, 1, and 2. • 0 indicates output will be in HTML • 1 indicates PDF • 2 indicates CSV	int	

TABLE 37 BOOT_IMAGE_DRIVER_MAP

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
MAJOR_VERSION	Major Version bit from Boot Image file	smallint	
MINOR_VERSION	Minor Version bit from Boot Image file	smallint	
MAINTENANCE	Maintenance Version bit from Boot Image file	smallint	
PATCH	Patch Version bit from Boot Image file	varchar	32
MD5_HASH	MD5 hash value for Boot Image file	varchar	64
SUPPORTED_DRIVERS	Compatible HCM Drivers delimited by comma	varchar	256

TABLE 38 BOOT_IMAGE_FILE_DETAILS_

Field	Definition	Format	Size
ID		int	
DRIVER_MAPPING_ID		int	
BOOT_IMAGE_NAME	Name of Boot Image file	varchar	64

TABLE 38 BOOT_IMAGE_FILE_DETAILS_ (Continued)

Field	Definition	Format	Size
MAJOR_VERSION	Major Version bit from Boot Image file	smallint	
MINOR_VERSION	Minor Version bit from Boot Image file	smallint	
MAINTENANCE	Maintenance Version bit from Boot Image file	smallint	
PATCH	Patch Version bit from Boot Image file	varchar	32
IMPORTED_DATE	Imported date of Boot Image file	timestamp	
RELEASE_DATE	Release date of Boot Image file	timestamp	
RELEASE_NOTES_LOCATION	Release notes location in Management application Repository	varchar	1024
LOCATION	Boot Image file location in Management application Repository	varchar	1024

TABLE 39 BOOT_LUN_SEQUENCE

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
NAME	Name of the Boot LUN Sequence	varchar	64
FABRIC_ID	PK of the owning fabric	INT	

TABLE 40 BOOT_LUN_SEQUENCE_DETAIL

Field	Definition	Format	Size
ID *	Unique generated database identifier.	int	
BOOT_LUN_SEQ_ID	PK of the owning Boot LUN Sequence	char	23
PORT_WWN	WWN of the port in the Boot LUN Sequenc	int	
LUN_NUM	LUN number of the port in the Boot LUN Sequence	int	
SEQUENCE_NUM	Sequence number of the port in the Boot LUN Sequence		

TABLE 41 CAPABILITY_

Field	Definition	Format	Size
NAME *	Name of the capability.	varchar	256
DESCRIPTION	Optional detailed description about the capability.	varchar	512

TABLE 42 CARD

Field	Definition	Format	Size
ID *	Unique generated database identifier.	int	
CORE_SWITCH_ID *	Core switch DB ID.	int	
SLOT_NUMBER	The number of the physical slot in the chassis where the blade is plugged in. For fixed blades, SlotNumber is zero.	smallint	
TYPE	ID of the blade to identify the type.	smallint	

TABLE 42 CARD (Continued)

Field	Definition	Format	Size
EQUIPMENT_TYPE	The type of the blade. It is either SW BLADE or CP BLADE.	varchar	32
STATE	State of the blade, such as ENABLED or DISABLED.	varchar	32
POWER_STATE	State of power supply to the blade.	varchar	16
ATTN_STATE		varchar	32
SERIAL_NUMBER	Factory serial number of the blade.	varchar	32
PART_NUMBER	The part number assigned by the organization responsible for producing or manufacturing the blade.	varchar	32
TRUNKING_SUPPORTED	1 = trunking is supported on this blade.	smallint	
FICON_DISABLED	1 = FICON is disabled on this blade.	smallint	
IP_ADDRESS	IP address of first Ethernet management port for a given slot with intelligent blade.	char	64
SUBNET_MASK	Mask of first Ethernet man.agement port for a given slot with intelligent blade.	varchar	64
DEFAULT_GATEWAY	Gateway IP address Ethernet management for a given slot with intelligent blade.	varchar	64
PRIMARY_FW_VERSION	Primary firmware version of applications on this blade. Applicable only for AP_BLADE.	varchar	48
SECONDARY_FW_VERSION	Secondary firmware version applications on this blade. Applicable only for AP_BLADE.	varchar	48
FCIP_CIRCUIT_CAPABLE	The blade is capable of creating FCIP Circuits. • 1 = true. • 0 = false. • Default value is 0.	smallint	
FCIP_LICENSED	FCIP Advanced Extension Licensing is available. • 1 = available. • 0 = not licensed. • -1 = not supported. • Default value is -1.	smallint	
MAX_FCIP_TUNNELS	The maximum number of tunnels that can be created in this slot. • -1 = not supported. • Default value is -1.	int	
MAX_FCIP_CIRCUITS	Describes the maximum number of circuits that can be created in this slot. • -1 = not supported. • Default value is -1.	int	
CP_BLADE_INDEX	CP blade index. Default value is -1.	smallint	
CP_HA_STATE	CP's HA state information like Active/Stand by.	varchar	128
ETHERNET_IPV6_ADDRESS	IPV6 address of Ethernet management port for the blade.	varchar	64

TABLE 42 CARD (Continued)

Field	Definition	Format	Size
ETHERNET_IPV6_GATEWAY	IPV6 Gateway address of Ethernet management port for the blade.	varchar	64
NUMBER_OF_PORTS		int	
HEADER_VERSION	The OEM or vendor-assigned version number.	int	
GIGE_MODE	Determines the port operating mode for GE ports. • 0 - 1G • 1 - 10G • 2 - Dual mode • 3 - Failover mode Default value -1 means it is not applicable.	smallint	

TABLE 43 CARD_CAPABILITY

Field	Definition	Format	Size
CARD_ID *	DB ID of the card.	int	
CAPABILITY_ *	Name of the capability detected on the card.	varchar	256
ENABLED	1 = the capability is enabled on the card. Default value is 0.	int	

TABLE 44 CED_APPLICATION

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
NAME	Name of the application. Application represents a collection of active zones in a fabric.	varchar	24
FABRIC_ID	ID of the fabric for which the application is created.	int	

TABLE 45 CED_APPLICATION_MEMBER

Field	Definition	Format	Size
APPLICATION_ID*	Auto-generated DB CED_Application table ID.	int	
ZONE_ID*	Auto-generated DB Zone table ID which joins as a member of the application.	int	

TABLE 46 CED_USER_PREFERENCE

Field	Definition	Format	Size
USER_NAME*	User Name carried from _USER table.	varchar	128
FABRIC_ID*	Fabric ID carried from Fabric table.	int	
APPLICATION_ID	CED application ID representing the group of end devices to be displayed in the fabric.	int	

TABLE 47 CEE_PORT

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
GIGE_PORT_ID	FK to GIGE_PORT	int	
VIRTUAL_SWITCH_ID	FK to owning VIRTUAL_SWITCH	int	
IF_INDEX	Interface index	int	
IF_NAME	Interface name	varchar	256
IF_MODE	Gige port mode (L2, L3, none)	varchar	8
L2_MODE	L2 mode (hybrid, trunk, access)	varchar	32
VLAN_ID	List of VLAN this port belongs to	text	
LAG_ID	LAG ID this port belongs to	int	
IP_ADDRESS	Port"s configured IP address	varchar	128
MAC_ADDRESS	Port"s MAC address	varchar	64
PORT_SPEED	Speed in Gb/sec. The default value is 0.	int	
ENABLED	State. The default value is 0.	smallint	
OCCUPIED	The default value is 0.	smallint	
LAST_UPDATE		bigint	
MAC_ACL_POLICY	stores the MAC ACL policy information of the port	varchar	64
NET_MASK	Netmask of the IPAddress of the port	varchar	128
PROTOCOL_DOWN_REASON	Reason for the port"s operational state being down	varchar	512
QOS_TYPE	QoS Type (Cee-Map, TrafficClass Map, FCoE map)	varchar	32
QOS_NAME	Name of the QoS Map set on the port	varchar	64
DOT1X_ENABLED	Indicate if 802.1x authentication is enabled on this port. The default value is 0.	smallint	
PORT_ROLE	Thisfield is used to store the port role value. The value will be populated by the NosSwitchAssetCollector. This field valid values include ISL or Edge. Default value is empty string.	varchar	32

TABLE 48 CFG_BACKUP_ARCHIVE

Field	Definition	Format	Size
CFG_BACKUP_ARCHIVE_ID		int	
DEVICE_ID	IP Product DB ID from which the configuration has been retrieved.	int	
USER_ID	Unique DB ID of user who initiated this config upoload.	int	
PRODUCT_TYPE	Indicates the type of product from which the config is retrieved for example NetIron XMR/MLX.	varchar	32
VERSION	Version of the configs downloaded for each product.	num	(8,0)
LOCATION		varchar	255

TABLE 48 CFG_BACKUP_ARCHIVE (Continued)

Field	Definition	Format	Size
DATE_TIME	The date and time at which the configuration has been backedup. The date and time will be saved in the following format "Mon May 10 17:59:13 PDT 2010".	varchar	64
FILE_NAME		varchar	64
IS_BASELINE	Indicates if the configuration file is selected by user as baselined configuration or not.	num	(1,0)
DESCRIPTION	Brief comments and description about this configuration.	varchar	1024
IMAGE_VERSION	The firmware version on the product while the config is retrieved.	varchar	64
CLI_TEMPLATE_REPORT_EXECUTION_ID	DB ID of the cli template report execution.	int	
CLI_TEMPLATE_REPORT_EXECUTION	Result of the cli template execution.	int	
CONFIG_DATA	The actual configuration data of the IP or DCB product.	txt	
CONFIG_TYPE	Configuration Type DCB_RUNNING=1, DCB_STARTUP=2, IP_STARTUP=3, IP_RUNNING=4	smallint	
DRIFT_STATUS	Indicates whether this config backup is deviated or not with respect to the active baseline at at the time of adding this config backup to the repository or not. If there is no baseline for the product, this column will be set to NO_BASELINE(-1). The possible values NO_DEVIATION=0, DEVIATED=1, NO_BASELINE=-1	int	

TABLE 49 CHANGELOG

Field	Definition	Format	Size
ID *	Unique generated database identifier.	int	
APPLIED_AT		varchar	25
DESCRIPTION		varchar	255

TABLE 50 CLI_TEMPLATE

Field	Definition	Format	Size
CLI_TEMPLATE_ID		int	
USER_ID		int	
NAME		varchar	256
TYPE	The template type. Product Monitoring: 2, Global configuration: 1 in CLI Configuration.	num	(2,0)
CLI_CMD		varchar	
DESCRIPTION		varchar	512
DEVICE_USERNAME		varchar	256

TABLE 50 CLI_TEMPLATE (Continued)

Field	Definition	Format	Size
DEVICE_PASSWORD		varchar	256
DATE_TIME		varchar	64
DEVICE_ENABLE_USERNAME		varchar	256
DEVICE_ENABLE_PASSWORD		varchar	256
CLI_FILTER		varchar	
HAS_PARAMETERS		num	(1,0)
PROMPT_ADDITIONAL_TARGET	The flag to indicate whether or not to prompt for additional targets during deployment. 1 = Prompt for additional targets. 0 =Do not prompt for additional target.	smallint	
PARAMETERS	Stores Parameter name and values in XML Format.	text	
PARAMETER_MODE	The flag to indicate whether the same parameter has to be applied for all targets or different values to be applied for each target. 0 - Same value for all targets. 1 - Different values for each targets.	smallint	
IS_EXAMPLE	The flag to indicate whether or not if the template is example template. 0 - User Defined (not example) template. 1 - Example Template.	smallint	
VALIDATE_CLI_RESPONSE	The flag to indicate whether or not if the CLI responses for each of the CLI commands are to be validated for this template. 0 - Dont validate CLI Responses. 1 - Validate CLI Responses.	smallint	
PROMPT_ADDITIONAL_PARAMETERS	The flag to indicate whether or not to prompt Parameter tab during manual deployment for changes. 0 - Dont prompt Parameter tab. 1 - Prompt Parameter tab.	smallint	
SCHEDULE_ENABLED	The flag to indicate whether or not the CLI Template is scheduled. 0 - Scheduled deployment is turned OFF. 1 - Scheduled Deployment is turned ON.	smallint	
MODULE	Stores the module or feature name of the CLI commands. This is used for example CLI templates.	varchar	256

TABLE 51 CLIENT_VIEW

Field	Definition	Format	Size
ID *	Unique generated database identifier.	int	
USER_NAME	The Management application user name.	varchar	128
NAME	Client view name.	varchar	255
DESCRIPTION	Client View description.	varchar	255

TABLE 52 CLIENT_VIEW_COLUMN

Field	Definition	Format	Size
ID *	Unique generated database identifier.	int	
NAME	Name of the column. It is used as column header in product list and property name in property sheet(SAN and IP)	varchar	255
ENTITY_CATEGORY	Holds the type of the entity to whom the column name belongs to like Port, Fabric, IPProduct, VCSInterface, etc'	varchar	128
COLUMN_INDEX	Used to differentiate user defined columns and static columns. For static it is 0 and for user defined columns it is 1,2,3.	small int	
DESCRIPTION	Holds description of the column.	varchar	255
ICON_ID	Holds Icon Id for the column. Currently it is unused.	int	
VISIBLE	Indicates whether the columns are visible. 0 - Not Visible, 1 - Visible	smallint	
EDITABLE	Indicates whether the columns are editable. 0 - Not Editable, 1 - Editable.	smallint	

TABLE 53 CLIENT_VIEW_MEMBER

Field	Definition	Format	Size
CLIENT_VIEW_ID *	Foreign key to CLIENT_VIEW table.	int	
FABRIC_ID *	Foreign key to FABRIC table.	int	

TABLE 54 CLIENT_VIEW_MEMBER_HOST

Field	Definition	Format	Size
CLIENT_VIEW_ID	Primary key of CLIENT_VIEW table	int	
HOST_ID	Primary key of DEVICE_ENCLOSURE table	int	

TABLE 55 CLUSTER

Field	Definition	Format	Size
ID *	Arbitrary integer to identify the cluster.	int	
NAME	User-assigned name to identify the cluster. Names should be unique to avoid user confusion, but the database does not enforce uniqueness.	varchar	64
IP_ADDRESS	The primary hostname or IP address for managing the cluster as a single entity. The definition of primary depends on the clustering technology.	varchar	64

TABLE 56 CLUSTER_MEMBER

Field	Definition	Format	Size
CLUSTER_ID	Identifies the cluster containing a member.	int	
DEVICE_ENCLOSURE_ID	Identifies a member of the cluster.	int	32

TABLE 57 CNA_ETH_PORT

Field	Definition	Format	Size
ID	ID of the Eth port	int	
ETH_DEV	Ethernet device	varchar	64
ETH_LOG_LEVEL	Log level for the Ethernet device. Possible values are 0 - Log Invalid 1 - Log Critical 2 - Log Error 3 - Log Warning 4 - Log Info	int	
NAME	Name of the port	varchar	256
MAC_ADDRESS	MAC Address	varchar	64
IOC_ID	IO controller ID. The default value is 0.	varchar	64
HARDWARE_PATH	Hardware path of the port	varchar	256
STATUS	Status of the Eth port. The default value is -1.	varchar	64
CNA_PORT_ID	ID of the parent port	int	
CREATION_TIME	CNA Eth port record creation time. This tells when the port was first discovered.	timestamp	
CURRENT_MAC_ADDRESS	User definable Mac address which is by default same as built in Mac address	varchar	64
MAX_BANDWIDTH	Maximum bandwidth	varchar	64
PCIF_INDEX	Pci function Iidex	varchar	64
MAX_PCIF	Maximum number of Pci functions.	smallint	
MIN_BANDWIDTH	Minimum guaranteed bandwidth. Value will be in Gbps (0 to 10).	int	
MTU	Maximum transmission unit in bytes	int	

TABLE 58 CNA_PRODUCT_CONNECTIVITY

Field	Definition	Format	Size
CNA_PORT_ID	CNA Port identifier.	int	
INTERFACE_ID	Interface Identifier.	int	

TABLE 59 CNA_ETH_PORT_CONFIG

Field	Definition	Format	Size
ID	Unique autogenerated db id.	int	
CNA_PORT_ID	Foreign key, related cna eth port config with the CNA port.	int	
CNA_ETH_PORT_ID	Nullable foreign key, related cna eth port config with the CNA eth port.	int	
PCIF_INDEX	PCI Function Index eg 2/1/1(adapter number/physical port number/port index).	varchar	64
CURRENT_MAC_ADDRESS	Current MAC address of the port.	varchar	64

TABLE 59 CNA_ETH_PORT_CONFIG (Continued)

Field	Definition	Format	Size
MAX_BANDWIDTH	Maximum guaranteed bandwidth. Value will be in Gbps (1 to 10).	varchar	64
MIN_BANDWIDTH	Minimum guaranteed bandwidth. Value will be in Gbps (0 to 10).	int	
PORT_NUMBER	Physical port number of adapter.	int	
PORT_TYPE	Type of this port. For example, ETH.	varchar	64
CREATION_TIME	Creation time of this DB record.	timestamp	
CONFIGURATION_STATUS	Indicates current configuration status of the port. Possible values are: -1 is Invalid 0 is Added 1 is deleted	int	

TABLE 60 CNA_PORT

Field	Definition	Format	Size
ID	Primary key autogenerated ID	int	
PORT_NUMBER	Port number of the CNA port	int	
PORT_WWN	Port WWN of the port	char	23
NODE_WWN	Node WWN of the port	char	23
PHYSICAL_PORT_TYPE	Port type CNA/FC	varchar	32
NAME	Name of the port	varchar	256
MAC_ADDRESS	MAC address of the port.	varchar	64
MEDIA	Media of the port	varchar	64
CEE_STATE	State of the port.	varchar	64
HBA_ID	ID of the port.	int	
CREATION_TIME	CNA port record creation time. This tells when this port was first discovered.	timestamp	
FACTORY_PORT_WWN	Factory configured Port WWN defined for the CNA port in HCM	varchar	23
FACTORY_NODE_WWN	Factory configured Node WWN defined for the CNA port in HC	varchar	23
PREBOOT_CREATED	Flag to identify vports created during preboot and will accept string values True/false/empty	varchar	23

TABLE 61 COLLECTOR

Field	Definition	Format	Size
NAME *	Name of the collector registered with the collection framework.	varchar	256
CLASS_NAME	Java class name which serves as the collector.	varchar	256
DESCRIPTION	Collector description, usually not used.	varchar	512

TABLE 62 COLLECTOR_MIB_OBJECT_ENTRY

Field	Definition	Format	Size
COLLECTOR_MIB_OBJECT_ENTRY_ID	Primary key autogenerated ID.	int	
COLLECTOR_ID	ID of the PERF_COLLECTOR.	int	
MIB_OBJECT_ID	MIB_OBJECT table DB ID.	int	

TABLE 63 COLLECTOR_SNMP_EXPRESSION_ENTRY

Field	Definition	Format	Size
COLLECTOR_SNMP_EXPRESSION_ENTRY_ID	Primary key autogenerated ID.	int	
COLLECTOR_ID	ID of the PERF_COLLECTOR.	int	
EXPRESSION_ID	Id of the SNMP_EXPRESSION.	int	

TABLE 64 COLLECTOR_TARGET_ENTRY

Field	Definition	Format	Size
COLLECTOR_TARGET_ENTRY_ID	Primary key autogenerated ID.	int	
COLLECTOR_ID	ID of the PERF_COLLECTOR.	int	
TARGET_ID	Target ID of the SNMP collector data. For device level collector it will use deviceId, and for port level it will use interfaceId.	int	
PROP_STR	Property string of the PERF_COLLECTOR.	varchar	8192
COLLECTOR_TARGET_ENTRY_TYPE	Target type of the SNMP collector data. for device level collector the target type is 0, for port level it is 1.	int	

TABLE 65 CONFIG_BLOCK

Field	Definition	Format	Size
ID	ID of the block.	int	
NAME	Name of the block.	varchar	255
DESCRIPTION	Description of the block.	varchar	1024
USE_REGEX	Indicates whether the block start is built with regular expression or not. 0 = Does not contain Regular expression 1 = Contains regular expression	smallint	
BLOCK_START	Block start string to match one or more block starts in the device config. Can be built with regular expression to match more than one block.	varchar	1024
BLOCK_END	Block end string. Used the first match to form config block from start to end.	varchar	1024
CATEGORY	Category of the Block. 0 = User defined 1 = Predefined.	smallint	

TABLE 66 CONFIG_CONDITION

Field	Definition	Format	Size
ID	Condition ID.	int	
NAME	Name of the condition.	varchar	255
DESCRIPTION	Description of the condition.	varchar	1024
REMEDIATION	Remediation details for failed conditions.	text	
USE_REGEX	Indicates whether the condition lines are built with regular expression or not. 0 = Does not contain Regular expression 1 = Contains regular expression	smallint	
MATCH	The device config should Match or Not match with condition. 0 = Not Match 1 = Match.	smallint	
CONDITION_STR	The condition string to match the device config. Unlimited length. Each line in configuration will be matched in the whole config or a block if the order_lines is 0. Else all lines will be matched together.	text	
ORDER_LINES	Indicates whether the condition_str lines order should be matched in the config or block. 0 = Lines order check is not required. 1 = Lines order should be matched.	smallint	
CATEGORY	Category of the Condition. 0 = User defined, 1 = Predefined.	smallint	

TABLE 67 CORE_SWITCH

Field	Definition	Format	Size
ID*	Auto generated ID for this table.	int	
IP_ADDRESS	IP Address of the switch that is represented by this record. Could be either IPV4 or IPV6 address.	varchar	128
WWN	WWN of the core switch.	char	23
NAME	Switch name if available otherwise stores the wwn of the switch.	varchar	64
TYPE	Stores the switch type, the sw_bd_type of the switch.	smallint	
MODEL	Holds the switch model, whether its Brocade, Mcdata or unknown . Value 2 is for Brocade and 3 is for McData	smallint	
FIRMWARE_VERSION	Firmware version of the switch.	varchar	128
VENDOR	Vendor information for the switch.	varchar	256
MAX_VIRTUAL_SWITCHES	Maximum number of virtual switches supported.	smallint	
NUM_VIRTUAL_SWITCHES	Total number of virtual switch present.	smallint	
REACHABLE	Determines whether the switch is reachable from the Management application. 1 is reachable and 0 is unreachable	smallint	

TABLE 67 CORE_SWITCH (Continued)

Field	Definition	Format	Size
UNREACHABLE_TIME	Time when the switch becomes unreachable.	timestamp	
OPERATIONAL_STATUS	Chassis operational status like FRU, Power Supply etc..	varchar	128
CREATION_TIME	Core switch record creation time. This tells us when the intial discovery has happened.	timestamp	
LAST_SCAN_TIME	Last scan time tells the time when the last time the switch was polled.	timestamp	
LAST_UPDATE_TIME	Last update time tells the time when the last update to the database record happened.	timestamp	
SYSLOG_REGISTERED	Determies whether the switch is registered for sending syslog traps. • 1 is registered • 0 is not registered.	smallint	
CALL_HOME_ENABLED	Determines whether the call home feature is enabled..	smallint	
SNMP_REGISTERED	Determines whether the switch is registered for sending SNMP traps . • 1 is registered • 0 is not registered.	smallint	
USER_IP_ADDRESS	Only for McData switches, this column is used to store the IP address which user provides for those M-model switches for which seed switch is unable to return IP address.	varchar	128
NIC_PROFILE_ID	Nic Profile ID refers to the entry in the NIcProfile table that has IP Address of the Management application which is used as Syslog or SNMP reciepients.	int	
MANAGING_SERVER_IP_ADDRESS	IP address(v4/v6) of the Management application server which is currently managing the M-model switch. Used for M-EOS switch only. It does not apply to Fabric OS switches.	varchar	128
VF_ENABLED	Determines whether Virtual Fabric is enabled on the switch. • 1 is enabled • 0 is disabled	smallint	
VF_SUPPORTED	Determines whether virtual fabric is supported on the switch. • 1 is supported • 0 is unsupported	smallint	
MANAGED_ELEMENT_ID	A unique managed element ID for this physical switch. Also a foreign key reference to the MANAGED_ELEMENT table.	int	

TABLE 67 CORE_SWITCH (Continued)

Field	Definition	Format	Size
NAT_PRIVATE_IP_ADDRESS	NAT private IP Address. Feature available from NMS DC Eureka release onwards. During a successful NAT translation the Private IP that gets translated will be stored in this field. The new translated IP Address will be stored in the existing IP_ADDRESS field. All the NAT look up will be done using the NAT Private IP Address.	varchar	128
ALTERNATE_IP_ADDRESS	Alternate IP address of the switch. Feature available from Eureka release onwards. During fabric discovery the column will be populated based on the values in the fabricinfo.html. If Management application server is IPV6 capable, then we store the switchetherIP NVP else we store the switchetherIPV6. So could be either IPV4 or IPV6 address. If there exists any NAT translation, translated IP will be used.	varchar	128
MAC_ADDRESS	Stores the VCS Mac Address. The value will be populated by the FabricCollector. Default value is empty string. The management interface Mac Address will be stored here.	varchar	64

TABLE 68 CORE_SWITCH_CAPABILITY

Field	Definition	Format	Size
CORE_SWITCH_ID *	DB ID.	int	
CAPABILITY_ *	Name of the capability detected on the core switch.	varchar	256
ENABLED	1 = the capability is enabled on the core switch. Default value is 0.	int	

TABLE 69 CORE_SWITCH_CHECKSUM

Field	Definition	Format	Size
CORE_SWITCH_ID *	DB ID.	int	
CHECKSUM_KEY *	Checksum type.	varchar	32
CHECKSUM	Checksum value.	varchar	16

TABLE 70 CORE_SWITCH_COLLECTION

Field	Definition	Format	Size
CORE_SWITCH_ID *	Core switch ID.	int	
COLLECTION_NAME *	Collector name.	varchar	256
LAST_CORE_SW_ MODIFICATION	Last core switch modification time.	timestamp	

TABLE 71 CORE_SWITCH_DETAILS

Field	Definition	Format	Size
CORE_SWITCH_ID*	Primary key for the table.	int	
ETHERNET_MASK	Ethernet mask of the core switch IP address.	char	64

TABLE 71 CORE_SWITCH_DETAILS (Continued)

Field	Definition	Format	Size
FC_MASK	FC IP Address ethernet mask.	char	64
FC_IP	Fibre Channel IP address.	char	64
FC_CERTIFICATE	FC IP Address.	smallint	
SW_LICENSE_ID	License ID of the chassis.	char	23
SUPPLIER_SERIAL_NUMBER	Supplier serial number for the switch.	varchar	32
PART_NUMBER	Partnumber of the switch	varchar	32
CHECK_BEACON	Denotes if Switch Beacon is enabled or not on the switch. 1 = beacon is turned on; otherwise, 0.	smallint	
TIMEZONE	Timezone of the switch.	varchar	32
MAX_PORT	Number of maximum ports physically allowed on the switch.	smallint	
CHASSIS_SERVICE_TAG	Chassis service tag for the switch.	varchar	32
BAY_ID	Bay ID of the switch.	varchar	32
TYPE_NUMBER	Type number is more of details for the type, Ex: SLKWRM.	varchar	32
MODEL_NUMBER	Model number is the same as the model number like Brocade 8000, Brocade VDX 6710.	varchar	256
MANUFACTURER	Manufacturer for the switch.	varchar	32
PLANT_OF_MANUFACTURER	Plant of the manufacturer for the switch.	varchar	32
SWITCH_SERIAL_NUMBER	This is the factory serial number.	varchar	32
ACT_CP_PRI_FW_VERSION	Stores Active CP primary firmware version.	varchar	128
ACT_CP_SEC_FW_VERSION	Stores Active CP secondary firmware version.	varchar	128
STBY_CP_PRI_FW_VERSION	Standby CP primary firmware version.	varchar	128
STBY_CP_SEC_FW_VERSION	Standby CP secondary firmware version.	varchar	128
TYPE	Type of the switch, basically the sw bd type stored in the core switch.	smallint	
EGM_CAPABLE	EGM license supported or not. • 1 is supported • 0 is not supported.	smallint	
SUB_TYPE	Sub Type of the switch. DCX+ and DCX-4S+ has values as 1, otherwise 0.	varchar	32
PARTITION	Partitions supported in the switch.	smallint	
MAX_NUM_OF_BLADES	Required by SMIA to populate Brocade_Chassis.MaxNumOfBlades property. It indicates the max no of blades that can be present in a chassis.	smallint	

TABLE 71 CORE_SWITCH_DETAILS (Continued)

Field	Definition	Format	Size
VENDOR_VERSION	Required by integrated SMI agent to populate Brocade_Product.Version property.	varchar	32
VENDOR_PART_NUMBER	Required by integrated SMI agent to populate Brocade_Product.SKUNumber property.	varchar	32
SNMP_INFORMS_ENABLED	Flag to denote whether SNMP informs option in the switch is enabled or disabled. Default value is 0.	smallint	
RNID_SEQUENCE_NUMBER	RNID sequence number for the switch.	varchar	32
CONTACT	Contact details of the switch. Syscontact from the RFC 1213 Mib.	varchar	256
LOCATION	Location details for the switch. Syslocation from RFC 1213.	varchar	256
DESCRIPTION	Description about the switch. Sysdescr from RFC 1213	varchar	256
FIRMWARE_VERSION	Firmware version of the switch.	varchar	128
CHASSIS_PACKAGE_TYPE	A value indicating the type of chassis.	int	
DOMAIN_NAME	Denotes the domain name configured in switch.	varchar	64
IP_ADDRESS_PREFIX	Required to populate the prefix of IPv6 address. Applicable only for IPv6 address.		
DOMAIN_NAME	Denotes the domain name configured in switch.		
FRAME_LOG_SIZE	The number of entries in the framelog.	int	
FRAME_LOG_ENABLED	Indicates if framelog is enabled on the switch. 0 = disabled, 1 = enabled.	smallint	
MAPS_ENABLED	Boolean flag to indicate if the switch is MAPS enabled or not. Enabled: 1, Disabled: 0.	smallint	

TABLE 72 CRYPTO_HOST

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
CRYPTO_TARGET_CONTAINER_ID	Foreign key reference to the CRYPTO_TARGET_CONTAINER that contains this host.	int	
VI_NODE_WWN	Node WWN of Virtual Initiator that represents this host.	char	23
VI_PORT_WWN	Port WWN of Virtual Initiator that represents this host.	char	23
HOST_PORT_WWN	Physical (real) host''s Port WWN	char	23
HOST_NODE_WWN	Physical (real) host''s Node WWN	char	23

TABLE 73 CRYPTO_LUN

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
CRYPTO_TARGET_CONTAINER_ID	Foreign key reference to the CRYPTO_TARGET_CONTAINER that contains the host for which these LUNs are configured.	int	
SERIAL_NUMBER	The LUN serial number, used to identify the physical LUN.	varchar	256
ENCRYPTION_STATE	Boolean. • True (1) if LUN is being encrypted. • False (0) if cleartext. The default value is 0.	smallint	
STATUS	Not currently used but left in for possible future use. Replaced by LUN_STATE. The default value is 0.	smallint	
REKEY_INTERVAL	The number of days that data encryption keys should be used before automatically generated a new key. 0 = infinite, i.e., no re-keying.	int	
VOLUME_LABEL_PREFIX	A user-configured string used to construct the Brocade-specific volume label on encrypted tapes. Ignored for disk LUNs.	varchar	256
LAST_REKEY_DATE	The last time a data encryption key was generated for this LUN. REKEY_INTERVAL days after this date, a new key will be generated.	timestamp	
LAST_REKEY_STATUS	The success or failure of the most recent re-keying operation, if any. This field is not currently used, but is left in the hope that FOS will support it in the future. Only valid for disk LUNs. The default value is 0.	smallint	
LAST_REKEY_PROGRESS	Indicates whether a re-key operation is in progress. • 0 = no re-keying in progress. • > 0 = percentage done of re-keying operation in progress. Only valid for disk LUNs. The default value is 0.	smallint	
CURRENT_VOLUME_LABEL	If a tape session is in progress, this is the volume label for the currently mounted tape. Only valid for tape LUNs.	varchar	2048
PRIOR_ENCRYPTION_STATE	Not used. When configuring a new disk LUN, this field indicates whether the LUN is already encrypted (1) or cleartext (0). This information does not need to be persisted. Only valid for disk LUNs.	smallint	
ENCRYPTION_FORMAT	If ENCRYPTION_STATE is true, ENCRYPTION_FORMAT indicates the type of encryption. • 0 = cleartext • 1 = DF-compatible • 2 = native	smallint	
ENCRYPT_EXISTING_DATA	Not used. When configuring a disk LUN that was previously cleartext and is to be encrypted, this property tells the switch whether or not to start a re-keying operation to encrypt the existing LUN data. This property does not need to be persisted.	smallint	

TABLE 73 CRYPTO_LUN (Continued)

Field	Definition	Format	Size
DECRYPT_EXISTING_DATA	Not used. When configuring disk LUN that was previously encrypted and is to become cleartext, this property tells the switch whether or not to start a re-keying operation to decrypt the existing LUN data. This property does not need to be persisted. This feature is no longer supported in FOS.	smallint	
KEY_ID	Hex-encoded binary key vault ID for the current data encryption key for this LUN. This ID may be used to locate the data encryption key in the key vault.	varchar	64
CRYPTO_HOST_ID	Foreign key reference to the CRYPTO_HOST that uses this LUN.	int	
LUN_NUMBER	The Logical Unit Number of the LUN, as seen by the LUNs host. This may be an integer (0 - 65565) or a WWN-format 8-byte hex number.	varchar	64
BLOCK_SIZE	The LUN"s Logical Block Size, in bytes. Only valid for disk LUNs.	int	
TOTAL_BLOCKS	The total number of logical blocks in the LUN. Multiplying BLOCK_SIZE by TOTAL_BLOCKS gives the LUN size in bytes.	int	
LUN_STATE	LUN operational status, such as OK or disabled for various reasons. For possible values see the enum definition in CryptoClientConstants. The default value is 0.	int	
LUN_FLAGS	Bitmap of LUN options. The only option currently used is bit 0 (least significant) which indicates that the LUN must be manually enabled because it has been disabled due to inconsistent metadata detected. The default value is 0.	bigint	
ENCRYPTION_ALGORITHM	Stores the Encryption Algorithm used to encrypt/decrypt data on the LUN	varchar	512
KEY_ID_STATE	State of the Key ID retrieval from Key Vault. The default value is 0.	smallint	
REKEY_SESSION_NUMBER	Unique Rekey session number. The default value is 0.	int	
PERCENTAGE_COMPLETE	Percentage of rekey completion. The default value is 0.	int	
REKEY_ROLE	Rekey Role definition. The default value is 0.	smallint	
CURRENT_LBA	Current Logical Block address for the rekey session in progress. The default value is 0.	int	
LUN_STATE_STRING	Lun state string.	varchar	2048
NEW_LUN	This field specifies that when a LUN is added to its container, indicate that it"s a new LUN to be used in SRDF Configuration. Feature available only from 6.4 release onwards and for RSA key vaults. CryptoLun collector and CryptoLunBean fills in this value. The default value is -1.	smallint	

TABLE 73 CRYPTO_LUN (Continued)

Field	Definition	Format	Size
NEW_LUN_TYPE	This field indicates the role of the LUN configured in the SRDF mode. The values could be R1, R2 or UNKNOWN. Feature available only from 6.4 release onwards and for RSA key vaults. CryptoLuncollector fills in this value.	varchar	64
DISABLE_WRITE_EARLY_ACK	This variable indicates whether write early acknowledgement is enabled (if value is 0) or disabled (if value is 1). The value of this variable is considered only for tape LUNs. This value is applicable only for the FOS 6.3.2 version and above.	smallint	
DISABLE_READ_AHEAD	This variable indicates whether read ahead is enabled (if value is 0) or disabled (if value is 1). The value of this variable is considered only for tape LUNs. This value is applicable only for the FOS 6.3.2 version and above.	smallint	
TIME_LEFT_FOR_AUTO_REKEY	The time left until next auto rekey, starts from the time last key for LUN was generated. This field is not updated every minute in DB. Its value is same as last_rekey_date + re_key_interval. As per current CAL implementation, will get only last_rekey_date when rekey is in progress. Otherwise it will be 0. CAL is providing "time left for auto rekey" attribute, and this value is stored in DB.	bigint	
THIN_PROVISION_LUN	Indicates whether the LUN is a Thin Provisioning LUN or not. The different Thin Provisioning values are 0(Unknown), 1(No), 2(Yes).	int	

TABLE 74 CRYPTO_SWITCH

Field	Definition	Format	Size
SWITCH_ID*	Primary key. The value is the same as the primary key of a record in the VIRTUAL_SWITCH table	int	
ENCRYPTION_GROUP_ID	Foreign key to the ENCRYPTION_GROUP table. Identifies the Encryption Group that this switch belongs to. Null indicates the switch is not part of an Encryption Group.	int	
GROUP_LEADER_POSITION	No longer used. Previously indicated whether this switch is the group leader. Use GROUP_LEADER_ID in the ENCRYPTION_GROUP table instead.	smallint	
TAPE_ENCRYPTION	No longer used. Previously enabled or disabled tape encryption at the switch level. This feature has been removed from Fabric OS. Default value is 0.	smallint	
TAPE_KEY_POLICY	No longer used. Previously used to configure a separate data encryption key per volume or per group. This feature has been removed from Fabric OS. Default value is 0.	smallint	

TABLE 74 CRYPTO_SWITCH (Continued)

Field	Definition	Format	Size
PRIMARY_VAULT_LINK_ STATUS	The status of the link key for the primary key vault. Link keys are used only for NetApp LKM key vaults. For possible values, see the enum definition in the DTO class. Default value is 0.	smallint	
BACKUP_VAULT_LINK_ STATUS	The status of the link key for the backup key vault. Link keys are used only for NetApp LKM key vaults. For possible values, see the enum definition in the DTO class. Default value is 0.	smallint	
CP_CERTIFICATE	The public key certificate, in PEM format, of the switch's Control Processor module. This certificate is exchanged with other switches to establish secure communication between switches in an Encryption Group.	varchar	4096
KAC_CERTIFICATE	The public key certificate, in PEM format, of the switch"s Key Archive Client module. This certificate is installed on key vaults to establish secure communication between this switch and the key vault. For firmware versions below 7.1.0 it will be in PEM format (encoded) and for firmware versions 7.1.0 and above it will be in p12 format (encoded).	varchar	8192
PRIMARY_VAULT_ CONNECTIVITY_STATUS	The status of the network connection between this switch and the primary key vault. For possible values, see the enum definition in the DTO class. Default value is 0.	smallint	
BACKUP_VAULT_ CONNECTIVITY_STATUS	The status of the network connection between this switch and the backup key vault. For possible values, see the enum definition in the DTO class. Default value is 0.	smallint	
UN_ERASE_ENABLED	This variable indicates whether LUN Erase feature is enabled or not on the switch. The value 1 means LUN Erase is enabled on the switch.The Value 0 means LUN Erase is not enabled on the switch.	smallint	

TABLE 75 CRYPTO_TARGET_CONTAINER

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
ENCRYPTION_ENGINE_ID	Foreign key reference to the ENCRYPTION_ENGINE that owns this container.	int	
NAME	A user-supplied name for the container.	varchar	64
VT_NODE_WWN	The Node WWN of the Virtual Target that represents the real physical target device.	char	23
VT_PORT_WWN	The Port WWN of the Virtual Target that represents the real physical target device.	char	23

TABLE 75 CRYPTO_TARGET_CONTAINER (Continued)

Field	Definition	Format	Size
FAILOVER_STATUS	Indicates whether this container''s target is being encrypted by the encryption engine on which the container is configured (value 0) or by another encryption engine in the HA Cluster (value 1). Default value is 0..	smallint	
FAILOVER_STATUS_2	Failover status from the HA Cluster peer.	smallint	
DEVICE_STATUS	The physical target storage device operational status when the virtual initiator last attempted to access the target. For possible values, see the enum definition in the DTO class. Default value is 0.	smallint	
DEVICE_TYPE	Indicates whether the target storage device is a disk (0) or tape (1) device. Default value is 0.	smallint	
TARGET_PORT_WWN	The Port WWN of the physical target storage device associated with this container.	char	23
TARGET_NODE_WWN	The Node WWN of the physical target storage device associated with this container.	char	23
CONTAINER_FIELD_DATA	Container metadata information	varchar	256
CONFIGURATION_STATUS	Configuration status. Default value is 0.	smallint	
FRONT_END_N_PORT_NUMBER	Indicates N_Port number where CISCO Fabric will be connected when BES is in AG Mode. Default value is -1.	smallint	

TABLE 76 CUSTOM_FAVORITES_OBJECT_LIST

Field	Definition	Format	Size
FAVORITE_ID	Represents the ID in FAVORITES table	int	
OBJECT_ID	Represents the member's ID of the custom favorites. It can be port/tunnel/EE monitor ID.	int	

TABLE 77 DASHBOARD

Field	Definition	Format	Size
ID	Dashboard ID.	int	
NAME	Name of the dashboard.	varchar	128
DESCRIPTION	Description of the dashboard.	varchar	256
CREATED_BY	References the ID column of the USER_ table. Foreign Key USER_(ID) who created the dashboard. For out of dashboards the column will be 2 to indicate system user.	int	

TABLE 77 DASHBOARD (Continued)

Field	Definition	Format	Size
CREATION_TIME	Time when dashboard was created.	timestamp	
LAST_OPENED_TIME	Time when dashboard was last opened.	timestamp	

TABLE 78 DASHBOARD_CANVAS

Field	Definition	Format	Size
ID	Dashboard Canvas ID.	int	
NAME	Name of the Dashboard canvas.	varchar	128
DESCRIPTION	Description of the dashboard canvas.	varchar	512

TABLE 79 DASHBOARD_CANVAS_PREFERENCE

Field	Definition	Format	Size
ID	Dashboard preferences like user ID, Scope ID etc are stored per dashboard.	int	
USER_ID	FK USER_.ID. ID of the user who own the dashboard.	int	
SCOPE_ID	FK USERDEFINED_NETWORK_SCOPE.ID. This value will be populated when user selects the predefined scope.	int	
SCOPE_TYPE	FK SCOPE_TYPE.ID. This value will be populated when user select user defined network scope.	int	
DASHBOARD_ID	FK DASHBOARD.ID. The ID of the dashboard to which the preference is applied.	int	
DASHBOARD_CANVAS_ID	FK DASHBOARD_CANVAS.ID. The ID of the Canvas in which the dashboard is shown	int	
VISIBLE	Visibility of the dashboard. 0 - Not Visible 1 - Visible.	smallint	
TIME_SCOPE	Time Scope of the Dashboard.	int	

TABLE 80 DASHBOARD_PROVIDER

Field	Definition	Format	Size
CLASS_NAME	The fully defined class name of the Provider class. This is stored per widget Provider class.	varchar	128
REFRESH_INTERVAL	Refresh Interval of the Widget in seconds. Default is 5 seconds.	int	

TABLE 80 DASHBOARD_PROVIDER

Field	Definition	Format	Size
PROVIDER_GROUP	The Group to which the Provider belong to. Similar providers will have same group name.	varchar	128
PROVIDER_ORDER	The order of execution passed to the Job Executor framework. Provider belong to same group will have different order number. Default: 0	int	

TABLE 81 DASHBOARD_WIDGET

Field	Definition	Format	Size
ID	ID of the dashboard widget. Auto incremented.	int	
TITLE	Name of the dashboard widget.	varchar	255
DESCRIPTION	Description of the dashboard widget.	varchar	512
EDITABLE	Indicates whether the widget attributes are editable. 0 - Not Editable, 1 - Editable.	smalint	
CATEGORY	Dashboard widget category. Used for categorizing the widgets based on the type. Possible values are 1 - General, 2 - Performance, 3 - Starlifter (future).	int	
PROVIDER_CLASS_NAME	Provides the mapping between widget and the summary provider. Fully qualified class name of the summary provider implementation for the widget. The class should implement SummaryProvider interface.	varchar	128
UI_PANEL_CLASS_NAME	Provides the mapping between widget and UI panel. Fully qualified class name of the dashboard widget user interface class. The class should extend from AbstractGadget.	varchar	128
SUMMARY_CLASS_NAME	Provides the mapping between widget and the summary. Fully qualified class name of the summary implementation for the widget. The class should implement Summary interface.	varchar	128
time_scope_supported	References the ID column of the DASHBOARD_PROVIDER table. Provides the mapping between widget and the summary provider. Fully qualified class name of the summary provider implementation for the widget. The class should implement SummaryProvider interface.	int	
network_scope_supported	Indicates whether the widget supports Time Scope. 0 - Not Supported 1 - Supported 2 - Partial'	int	

TABLE 81 DASHBOARD_WIDGET (Continued)

Field	Definition	Format	Size
installation_type	Indicates the widgets is SAN Only (0) / IP Only (1) / SAN_IP (2)'	int	
shared_provider	Can the provider be shared? 0 - Not Shared 1 - Shared.	int	

TABLE 82 DASHBOARD_WIDGET_PREFERENCE

Field	Definition	Format	Size
ID	Auto incremented widget preference ID.	int	
WIDGET_ID	Foreign Key to DASHBOARD_WIDGET(ID).	int	
USER_ID	Foreign Key to USER_ (ID).	int	
DASHBOARD_ID	Foreign Key to DASHBOARD(ID).	int	
VISIBLE	Indicates whether the widget is visible for the user in the dashboard. 0 - Not Visible, 1 - Visible.	smallint	
STATE	State of the widget. Possible values are 0 - Normal, 1 - Maximized, 2 - Collapsed.	int	
WIDTH	Width of the widget.	int	
HEIGHT	Height of the widget.	int	
ROW_INDEX	Row position of the widget. -1 for an out-of-box widget defined but not shown.	int	
COLUMN_INDEX	Column position of the widget. -1 for an out-of-box widget defined but not shown.	int	
CANVAS_ID	Foreign Key to DASHBOARD_CANVAS.ID	int	

TABLE 83 DEFAULT_FAVORITES

Field	Definition	Format	Size
ID	Name of the favorite.	int	
NAME	The topnumber of ports (5,10,15,20).	varchar	64
TOP_N	Types of ports (FC/FCIP/GE) and -End Monitors.	varchar	40
SELECTION_FILTER	The time interval in which the graph is shown.	varchar	40
FROM_TIME	Always null. The default favorite is not customized.	varchar	40
CUSTOM_LAST_VALUE	Always null. The default favorite is not customized.	int	
CUSTOM_TIME_UNIT	Always null. The default favorite is not customized.	varchar	40
CUSTOM_FROM	Always null. The default favorite is not customized.	timestamp	
CUSTOM_TO	The default five minutes granularity.	timestamp	
GRANULARITY	Always null.	varchar	40
THRESHOLD	The measure Tx MBps or Rx MBps based on DEFAULT_FAVORITES.NAME	int	

TABLE 83 DEFAULT_FAVORITES (Continued)

Field	Definition	Format	Size
MAIN_MEASURE	The Additional measures based on the FAVORITE.MAIN_MEASURE	varchar	40
ADDITIONAL_MEASURE	The Additional measures based on the FAVORITE.MAIN_MEASURE	int	

TABLE 84 DEFAULT_WIDGET_PREFERENCE

Field	Definition	Format	Size
ID	Auto incremented Dashboard Widget Preference ID.	int	
dashboard_id	Foreign Key to DASHBOARD(ID).	int	
widget_id	Foreign Key to DASHBOARD_WIDGET(ID).	int	
installation_type	Indicates the widgets is SAN Only (0) / IP Only (1) / SAN_IP (2).	int	
visible	Indicates whether the widget is visible for the user in the dashboard. 0 - Not Visible, 1 - Visible.	int	
“state”	State of the widget. Possible values are 0 - Normal, 1 - Maximized, 2 - Collapsed.	int	
width	Width of the widget.	int	
height	Height of the widget.	int	
row_index	Row position of the widget. -1 for an out-of-box widget defined but not shown.	int	
column_index	Column position of the widget. -1 for an out-of-box widget defined but not shown.	int	

TABLE 85 DEPLOYMENT_CONFIGURATION

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
NAME	Name of the configuration	varchar	255
CONFIGURATION_TYPE	Indentifies the save configuration type. • 1 - Not applicable • 1 - Running • 2 - Startup • 3 - Running & Startup	smallint	
DEPLOY_OPTION	Identifies the deployment options. • 1-Deploy Now • 2-Save & Deploy • 3-Save deployment only • 4-Scheduled	smallint	
DEPLOYMENT_HANDLER_ID	Foreign Key references DEPLOYMENT_HANDLER (ID). Identifies the handler to use for the configuration	int	
SCHEDULE_ENABLED	1 indicates that the schedule is applied to the configuration	smallint	

TABLE 85 DEPLOYMENT_CONFIGURATION (Continued)

Field	Definition	Format	Size
SNAPSHOT_ENABLED	1 indicates that snapshot is applied to the configuration	smallint	
CLI_TEMPLATE_ID	Identifies the CLI template details. -1 if SNAPSHOT_ENABLED is False	int	
SNAPSHOT_SETTING	Identifies the setting type • 1-Presnapshot • 2-Postsnapshot • 3-Pre & Post snapshot • -1 if SNAPSHOT_ENABLED is False	smallint	
POST_DEPLOYMENT_DELAY	Post deployment delay in seconds	int	
CREATED_BY	User who created the configuration	varchar	255
LAST_MODIFIED_BY	User who last modified the configuration. When the configuration is first created	varchar	255
MANAGEMENT_FLAG	True if deployment should be managed by Deployment Manager Module and this will be displayed in Deployment Manager UI	smallint	
DESCRIPTION	Used to describe the deployment configuration	varchar	255

TABLE 86 DEPLOYMENT_HANDLER

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
MODULE	Identifies the unique deployment module	varchar	64
SUB_MODULE	Identifies sub-module	varchar	64
MODULE_DISPLAYNAME	Display text for module name.	varchar	128
HANDLER_CLASS	Fully qualifies name of handler class for the module. This class has to implement <DeploymentHandler> interface	varchar	255
CLIENT_ACTION_HANDLER_CLASS	Fully qualifies module-specific client class which implements <DeploymentDelegateActionsHandler> interface. Framework will delegate edit, duplicate, delete actions to this class	varchar	255
PRIVILEGE_ID	Comma separated privilege IDs	varchar	64

TABLE 87 DEPLOYMENT_PRODUCT_STATUS

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
DEPLOYMENT_STATUS_ID	Foreign Key references DEPLOYMENT_STATUS (id). Identifies the execution cycle for the deployment.	int	
DEPLOYMENT_TIME	Time when this product deployment occurred.	timestamp	

TABLE 87 DEPLOYMENT_PRODUCT_STATUS (Continued)

Field	Definition	Format	Size
PRODUCT_ID	This record will be per product. Hence this will have the id of the product.	int	
PRODUCT_TYPE_ID	Foreign Key references TARGET_TYPE(id). This identifies the PRODUCT_ID. (Whether it is switch, device, etc).	int	
STATUS	Indicated the product deployment status 1-Aborted 2-Succesful 3-Partial Failure 4-Failed	smallint	
MESSAGE	Message to be displayed in the report.	txt	
ERROR_CODE	Error code, can be used for i18n	int	

TABLE 88 DEPLOYMENT_REPORT_TEMPLATE

Field	Definition	Format	Size
DEPLOYMENT_HANDLER_ID	Foreign Key references DEPLOYMENT_HANDLER(id).	int	
HEADER	Stores header content of deployment report. This could be plain text or HTML or XML	text	
FOOTER	Stores the footer content of deployment report. This could be plain text or HTML or XML.	text	

TABLE 89 DEPLOYMENT_STATUS

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
DEPLOYMENT_CONFIGURATION_ID	Foreign Key References DEPLOYMENT_CONFIGURATION(id). Identifies the deployment configuration	int	
DEPLOYMENT_TIME	Start Time of the deployment (UTC)	timestamp with time zone	
STATUS	Overall status of the deployment. 1-In Progress 2-Success 3-Failure 4-Partially failed	smallint	
DEPLOYED_BY	User who deployed the configuration	varchar	255
STATUS_MESSAGE	Overall Success/Failure status description	txt	
TRIGGER_SOURCE	Maintains the source from which this deployment was triggered such as Event Action <Event policy name>, Manual and Scheduled etc.	varchar	128

TABLE 90 DEPLOYMENT_TARGET_MAP

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
DEPLOYMENT_CONFIGURATION_ID	Foreign Key References DEPLOYMENT_CONFIGURATION (id) Identifies the deployment configuration this row is applied	int	
TARGET_ID	Identifies the target. It will NOT have mapping to any product table like device, etc	varchar	255
TARGET_TYPE_ID	Foreign Key references TARGET_TYPE (id) Identifies the target type	int	
TARGET_PARENT_ID	Identifies the parent of the target. If, switch, device, port group, device group it will be same as target id. If it is port/interfaces the parent id will be the switch id	int	

TABLE 91 DEVICE

Field	Definition	Format	Size
DEVICE_ID	Primary key for this table.	int	
IP_ADDRESS	IP address of this device.	varchar	255
ALIAS_NAME	Device alias name.	varchar	512
HOST_NAME	Best matching host name obtained through the device IP address.	varchar	512
SYS_NAME	An administratively-assigned name for this device.	varchar	255
SYS_CONTACT	The textual identification of the contact person for this device, together with information on how to contact this person.	varchar	255
DESCRIPTION	A textual description of the device.	varchar	512
SYS_LOCATION	The physical location of this device.	varchar	255
COMMUNITY_STR_GET	SNMP GET community string to query the device.	varchar	512
COMMUNITY_STR_SET	SNMP SET community string of this device.	varchar	512
SYS_OID	The vendor's authoritative identification of this device ie., System Object Identifier.	varchar	255
SUPER_USER_PASSWORD	Super user password configured in the device.	varchar	512
TABLE_SUBTYPE	Device table subtype defined by INM BizObject framework.	varchar	32
LOCAL_USER_NAME	Local user name configured in the device for CLI access.	varchar	512
LOCAL_PASSWORD	Password to access the telnet interface.	varchar	512
TELNET_PASSWORD	Password to access the Telnet interface.	varchar	512
RADIUS_USER_NAME	User name for RADIUS access.	varchar	512
RADIUS_PASSWORD	Password for RADIUS access.	varchar	512

TABLE 91 DEVICE (Continued)

Field	Definition	Format	Size
TAC_USER_NAME	User name for TACACS access.	varchar	512
TAC_PASSWORD	Password for TACACS access.	varchar	512
TACPLUS_USER_NAME	User name for TACACS+ access.	varchar	512
TACPLUS_PASSWORD	Password for TACACS+ access.	varchar	512
IS_ROUTER	Flag to identify whether the device is router or not.	num	(1,0)
IS_SLB	Flag to identify whether the device supports server load balancing or not.	num	(1,0)
FIRST_SEEN_TIME		varchar	64
LAST_SEEN_TIME	Time when the device is getting discovered by recent collection.	varchar	64
LAST_PROBE_TIME		varchar	64
LAST_PROBE_STATUS		varchar	64
IS_SFLOW_CAPABLE	Flag to identify whether the device is SFlow capable or not.	num	(1,0)
SNMPV3_RO_AUTH_TYPE	SNMP V3 read only authentication type.	varchar	1
SNMPV3_RO_AUTH_USERNAME	SNMP V3 read only authentication user name.	varchar	512
SNMPV3_RO_AUTH_PASSWORD	SNMP V3 read only authentication password.	varchar	512
SNMPV3_RO_PRIV_PROTOCOL	SNMP V3 read only privacy protocol.	varchar	1
SNMPV3_RO_PRIV_PASSWORD	SNMP V3 read only privacy password.	varchar	512
SNMPV3_RW_AUTH_TYPE	SNMP V3 read write authentication type.	varchar	1
SNMPV3_RW_AUTH_USERNAME	SNMP V3 read write authentication user name.	varchar	512
SNMPV3_RW_AUTH_PASSWORD	SNMP V3 read write authentication password.	varchar	512
SNMPV3_RW_PRIV_PROTOCOL	SNMP V3 read write privacy protocol.	varchar	1
SNMPV3_RW_PRIV_PASSWORD	SNMP V3 read write privacy password.	varchar	512
LOCAL_USERNAME_PORT_CFG	Agent user name configured in device used for port configuration.	varchar	512
LOCAL_PASSWORD_PORT_CFG	Agent password configured in device used for port configuration.	varchar	512
LOCAL_USERNAME_READ_ONLY	Local user name for read only access.	varchar	512
LOCAL_PASSWORD_READ_ONLY	Local password for read only access.	varchar	512
RADIUS_USERNAME_PORT_CFG	RADIUS user name configured in device used for port configuration.	varchar	512
RADIUS_PASSWORD_PORT_CFG	RADIUS password configured in device used for port configuration.	varchar	512
RADIUS_USERNAME_READ_ONLY	RADIUS user name configured in device used for read only access.	varchar	512
RADIUS_PASSWORD_READ_ONLY	RADIUS password configured in device used for read only access.	varchar	512

TABLE 91 DEVICE (Continued)

Field	Definition	Format	Size
TAC_USERNAME_PORT_CFG	TACACS username for port configuration.	varchar	512
TAC_PASSWORD_PORT_CFG	TACACS password for port configuration.	varchar	512
TAC_USERNAME_READ_ONLY	TACACS username for read only access.	varchar	512
TAC_PASSWORD_READ_ONLY	TACACS password for read only access.	varchar	512
TACPLUS_USERNAME_PORT_CFG	TACACS+ username for port configuration.	varchar	512
TACPLUS_PASSWORD_PORT_CFG	TACACS+ password for port configuration.	varchar	512
TACPLUS_USERNAME_READ_ONLY	TACACS+ username for read only access.	varchar	512
TACPLUS_PASSWORD_READ_ONLY	TACACS+ password for read only access.	varchar	512
ENABLE_PASSWORD_PORT_CFG	Enable password configured in device used for port configuration.	varchar	512
ENABLE_PASSWORD_READ_ONLY	Enable password for read only access.	varchar	512
ADMIN_STATUS	Device admin status.	smallint	
ADMIN_STATUS_DURATION	Time duration of the admin status without any change.	int	
ADMIN_STATUS_LAST_UPDATED	Time when the admin status updated last.	bigint	
MEMO_LAST_UPDATED	Time when the memo got updated last.	bigint	
MEMO	Memo updated by the user for this device.	varchar	4096
TACPLUS_ENABLE_USERNAME	TACACS+ enable user name.	varchar	512
TACPLUS_ENABLE_PASSWORD	TACACS+ enable password.	varchar	512
OPER_STATUS	Device operational status.	smallint	
OPER_STATUS_LAST_UPDATED	Time when the device operational status got updated recently.	bigint	
LLDP_CHASSIS_ID_SUBTYPE	Chassis ID subtype returned by lldp MIB.	smallint	
LLDP_CHASSIS_ID	Chassis ID returned by lldp MIB.	bytea	
IS_FDP_ENABLED	Flag to identify whether Foundry Discovery Protocol is enabled or not.	num	(1,0)
IS_CDP_ENABLED	Flag to identify whether Cisco Discovery Protocol is enabled or not.	num	(1,0)
VENDOR	Vendor of this device.	varchar	64
IS_FOUNDRY	Flag to identify whether the device is Foundry product or not.	num	(1,0)
MANAGED_ELEMENT_ID	A unique managed element ID for this IP switch. Also a foreign key reference to the MANAGED_ELEMENT table.	int	
NODE_WWN	The managed element node WWN if one exists, or null/empty otherwise.	varchar	23

TABLE 91 DEVICE (Continued)

Field	Definition	Format	Size
SYSLOG_REGISTERED	This flag is to indicate whether the device is registered DCM as its syslog destination server. • 0 indicates not registered. • 1 indicates registered.	num	1
TRAP_REGISTERED	This flag is to indicate whether the device is registered DCM as its SNMP trap destination server. • 0 indicates not registered. • 1 indicates registered.	num	1
PORT_COUNT	Record the number of presented physical ports on the device.	int	
SERIAL_NUMBER	Record the serial number of the device. If there is no serial number, an empty string will be stored.	varchar	32
CATEGORY	This flag is to classify the device category • 0 is for unknown • 1 is for fixed configuration device • 2 is for chassis device • 3 is for stack device (logical)	int	
MPLS_MANAGE_STATE	This flag is to classify the device mpls managing state • 0 indicates unknown state for catching all • 1 indicates not applicable; if the IP Product is not XMR/MLX, it will be set to this value. • 2 indicates MPLS unmanaged state; in PP or PPE edition, XMR/MLX product will be set to this value. • 3 indicates MPLS managed state; only XMR/MLX product in EE edition will be set to this value.	int	
LICENSE_PORT_COUNT	It records the number of the ports that presented in the device.	int	
SUB_CATEGORY	This column is used to classify device sub category for DCB switches. Column helps to identify whether the DCB switch is an Elara/Frisco or DCX with Europa blade etc. Value 0 indicates that this is a pure IP device and hence that is the default value. Value 1 indicates that this is an Elara DCB device. The values will be populated by the DCB collector during the discovery of the DCB switch.	int	
LICENSED_FEATURES	This column is used to persist the feature based software licenses existing on the device. This represents bitmask as an integer value, where each bit represents a unique feature.	int	

TABLE 91 DEVICE (Continued)

Field	Definition	Format	Size
IS_DCB_SWITCH	This column is used to flag whether the device is a DCB Switch or not. Value 0 indicates that this is not a DCB switch device and hence that is the default value and value 1 indicates that this is a DCB device. The values will be populated by the DCB collector during the discovery of the DCB switch.	num	(1,0)
PRODUCT_FAMILY	Record the product family as "BI", "EI", "FGS/FLS/STK". Make it string field to accommodate dynamic group database search.	varchar	32
NETCONF_TRANSPORT	The transport protocol used to connect to this device through Netconf. Possible values are: • 0=Netconf not supported by this device • 1=SSH • 2=HTTPS • 3=HTTP • 4=WING_HTTPS • 5=WING_HTTP	smallint	
POE_CAPABLE	The POE capability of device. Possible values are: • 0 = POE is not supported by this device • 1 = POE is supported with IEEE 802.3af standard by this device • 2 = POE plus is supported with IEEE 802.3at standard by this device	smallint	
CLUSTER_MODE	This column is used to determine whether VCS Cluster is in Standalone mode or Cluster mode. The values will be populated by the VCS collector during the discovery of the VCS switch. The default value of -1 means that its a non VCS device. Following Enum will be defined as NON_VCS(-1), STANDALONE(0), CLUSTER(1).	smallint	
CLUSTER_TYPE	This column is used to determine whether VCS is in Fabric Cluster or Logical Chassis. The values are populated by the VCS collector during the discovery of the VCS switch. The default value -1 means that its a non-VCS device. Following are the values and their types: • 0 - Unknown • 1 - Standalone • 2 - Fabric Cluster • 3 - Logical Chassis	smallint	
IS_VCS_CAPABLE	This column is used to determine whether the device is a VCS device. The default value 0 means that the device is not VCS capable and value 1 means that the device is VCS capable.	smallint	
TRACKING	This column helps to identify that whether the device is left/joined the cluster membership. The value will be a bit mask value where 2^1 will be treated as left, 2^2 treated as joined. The default value will be -1.	smallint	

TABLE 91 DEVICE (Continued)

Field	Definition	Format	Size
VCS_ID	This column is used to store the VCS ID of the device. The value will be populated by the NosSwitchAssetCollector during the discovery of the VCS Cluster. The non zero value will be stored as VCS ID. Default value is -1.	smallint	
VCS_LICENSED	Indicates whether the cluster device has VCS license or not. Possible values are 0 for not applicable, 1 for licensed, 2 for not licensed. 0 is default. Clusters with 2 or less nodes will have value of 0 as all those clusters are automatically licensed. Clusters with 3 or more nodes will have values 1 or 2 depending on whether the license was acquired or not.		
RBRIDGE_ID	This column is used to store the Rbridge ID of the device. The value will be populated by the NosSwitchAssetCollector during the discovery of the VCS member. The non zero value will be stored as Rbridge ID. Default value is -1.	smallint	
IS_PRINCIPAL_SWITCH	This column is used to determine whether VCS member is a Principal switch or not. Value 1 indicates that this is a principal switch and 0 indicates that this not a Principal switch. The values will be populated by the VCS collector during the discovery of the VCS switch. The default value of 0 means that its a principal switch.	smallint	
IS_NETCONF_REACHABLE	This column is used to determine whether the device is netconf reachable. The value will be populated by the NosSwitchAssetCollector. The value of 0 means not reachable, 1 means reachable port and -1 means unknown status. Default value is -1	smallint	
FABRIC_WATCH_STATUS	Switch status based on components.	smallint	
FABRIC_WATCH_STATUS_REASON	Component reason for switch status.	varchar	1028
MAC_ADDRESS	The mac address to identify the wireless controller or AP. This will be empty string for all other devices.	varchar	64
MANAGED_AP_COUNT	Its the number of APs that the controller managed.	int	
CONTROLLER_CLUSTER_MODE	Cluster mode of the controller: Active, Standby and None. -1 : NA, 0 : None, 1 : Active, 2 : Standby.	int	
CONTROLLER_CLUSTER_NAME	This is controller cluster name.	varchar	65
CONTROLLER_CLUSTER_PEER_IP	IP addresses of the controller cluster peer.	varchar	128
WIRELESS_TYPE	To filter the APs from the product. 0 : NonAP, 1 : managed Brocade branded AP, 2 : standalone Brocade branded AP.	int	
BRIEF_PRODUCT_FAMILY	Shorter name for the product family.	varchar	32

TABLE 91 DEVICE (Continued)

Field	Definition	Format	Size
USER_DEFINED_VALUE_1	User defined value used for product.	varchar	256
USER_DEFINED_VALUE_2	User defined value used for product.	varchar	256
USER_DEFINED_VALUE_3	User defined value used for product.	varchar	256
CLUSTER_MEMBER_STATE	Indicates the state of the member in Fabric Cluster and logical chassis. States can be Online, Offline, Rejoining etc.. For all other devices this column will be empty.	varchar	64
MODE	Denotes the mode of the device. 1 denotes it is in non-AG mode and 2 denotes that the device is in AG mode.-1 denotes not applicable and will be set to all non NOS devices.	int	

TABLE 92 DEVICE_CONNECTION

Field	Definition	Format	Size
ID	The primary key.	int	
FABRIC_ID	ID of the fabric which the device port is connected to. It refers the ID column of FABRIC table.	int	
DEVICE_PORT_ID	ID of end device port. It refers ID field of DEVICE_PORT table.	int	
SWITCH_PORT_ID	ID of switch port which end device port is connected. In case device port is connected through AG, this port refer the switch port which AG is connected. It refers to the ID field of SWITCH_PORT table.	int	
AG_PORT_ID	In case of AG, this would refer to F Port of the AG which end device port is connected. If the device port is directly connected to switch port or NPIV connection then it would be -1. It refers to the ID field of SWITCH_PORT table for the access gateway switches.	int	
CREATION_TIME	Time at which the device connection record is created.	timestamp	
LAST_UPDATED_TIME	Time at which connection properties are modified for this record.	timestamp	
MISSING	Indicates if the device connection is missing or not.	int	
MISSING_TIME	Time from which the device connection has been missing.	timestamp	
TRUSTED	Indicates if the device connection is trusted or not.	int	

TABLE 93 DEVICE_ENCLOSURE

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
NAME	Name of the Device enclosure.	varchar	256
TYPE	Type of Device enclosure - Storage Array/Server.	varchar	32

TABLE 93 DEVICE_ENCLOSURE (Continued)

Field	Definition	Format	Size
ICON	Type of Icon.	int	
OS	Operating System.	varchar	256
APPLICATIONS	Application which created device enclosure.	varchar	256
DEPARTMENT	Department using this device enclosure.	varchar	256
CONTACT	Contact person details.	varchar	256
LOCATION	Location of physical setup.	varchar	256
DESCRIPTION	Description if any.	varchar	256
COMMENT_	Comments if any.	varchar	256
IP_ADDRESS	IP Address if assigned by user.	varchar	128
VENDOR	Vendor name.	varchar	256
MODEL	Device enclosure Model.	varchar	256
SERIAL_NUMBER	Serial Number given for the entity.	varchar	256
FIRMWARE	Firmware running on the device which is not applicable for device enclosure logical entity.	varchar	256
USER_DEFINED_VALUE1	User-defined custom value.	varchar	256
USER_DEFINED_VALUE2	User-defined custom value.	varchar	256
USER_DEFINED_VALUE3	User-defined custom value.	varchar	256
HCM_AGENT_VERSION	Version of the HCM agent running on the host	varchar	32
OS_VERSION	Operating system version for the enclosure	varchar	256
CREATED_BY	Module which created this enclosure: 0->Manual, 1->HBA 2->VM. Default value is 0.	int	
TRACK_CHANGES	Flag to enable/disable tracking. Default value is 0.	smallint	
LAST_UPDATE_TIME	Last time at which the host information was updated.	timestamp	
LAST_UPDATE_MODULE	Module which updated the host information.	smallint	
TRUSTED	Flag to mark the enclosure trusted. Default value is 0.	smallint	
CREATION_TIME	Time when enclosure was created. Default is 'now()'.	timestamp	
MISSING	Flag to indicate missing enclosure. Default value is 0.	smallint	
MISSING_TIME	Time when the enclosure is found to be missing.	timestamp	
HOST_NAME	Host Name corresponding to the Device Enclsoure.	varchar	256
SYSLOG_REGISTERED	SysLog flag that indicates if syslog has been enabled or not.	smallint	

TABLE 93 DEVICE_ENCLOSURE (Continued)

Field	Definition	Format	Size
VIRTUALIZATION	If this enclosure is a host, this column indicates whether the host is running a virtualization hypervisor. 0 = unknown 1 = no supported hypervisor present 2 = VMware ESX 3 = Microsoft Hyper-V. Default value is 0.	smallint	
MANAGED_ELEMENT_ID	A unique managed element ID for a managed host.If the device enclosure is manually created (does not represent a managed host) then the field is null. Also a foreign key reference to the MANAGED_ELEMENT table.	int	
MANAGED_BY	1 - Manual - (user created not managed condition) - Default. 2 - Host Adapter 3 - VMM 4.Both Host Adapter and VMM';	smallint	
QUEUE_DEPTH	Queue Depth can be used to control FCP exchange resource allocation. Queue depth can range from 0 to 254 and default value is 32.	int	

TABLE 94 DEVICE_ENCLOSURE_MEMBER

Field	Definition	Format	Size
ENCLOSURE_ID*	DEVICE_ENCLOSURE table ID.	int	
DEVICE_PORT_WWN*	WWN Of Device Port.	char	23
DEVICE_PORT_ID	Device_Port table ID.	int	

TABLE 95 DEVICE_FDMI_DETAILS

Field	Definition	Format	Size
DEVICE_NODE_ID	Device node id for the FDMI device node. This column refers to the device_node tables primary key	int	
SERIAL_NUMBER	Holds the serial number of the device available via FDMI	varchar	128
FIRMWARE_VERSION	Holds the firmware version of the device available via FDMI ex: 2.1.0.2	varchar	64
DRIVER_VERSION	Holds the driver version of the device available via FDMI, ex: 2.1.0.2	varchar	64
MANUFACTURER	Holds the manufacturer of the device available via FDMI, ex : Brocade	varchar	64
MODEL	Holds the model of the device available via FDMI, ex : Brocade-825	varchar	64
HARDWARE_VERSION	Holds the hardware version of the device available via FDMI, ex: Rev-C	varchar	64

TABLE 95 DEVICE_FDMI_DETAILS (Continued)

Field	Definition	Format	Size
MODEL_DESCRIPTION	Holds the model description of the device available via FDMI, ex : Brocade-825	varchar	64
NODE_NAME	Holds the node name of the device available via FDMI, ex : 20:00:00:05:1e:7c:64:94	varchar	64

TABLE 96 DEVICE_GROUP

Field	Definition	Format	Size
DEVICE_GROUP_ID	Primary key for this table.	int	
NAME	Name of this device group.	varchar	128
USER_ID	User ID corresponds to the user who created the device.	int	
DESCRIPTION	Device group description.	varchar	255
IS_PUBLIC	Flag to identify whether this group is shared across users.	num	(1,0)
IS_INTERNAL	Flag to identify this group is internal.	num	(1,0)
TABLE_SUBTYPE	Table subtype defined by BizObject framework	varchar	32
IS_AP_GROUP	Flag to identify whether this group is access point device group.	num	(1,0)
IS_SENSOR_GROUP	Flag to identify whether this group is sensor device group.	num	(1,0)
VIEW_MASK	Flag to decide whether to show the device group in topology or not.	num	(1,0)
GROUP_TYPE	This flag is to classify the device group type: • 0 is the default and reserved for internal temporary group • 1 is for System Device Group • 2 is for MPLS System Device Group • 3 is for User Defined Device Group	int	

TABLE 97 DEVICE_GROUP_ENTRY

Field	Definition	Format	Size
DEVICE_GROUP_ID	Database ID of the DEVICE_GROUP instance which the device is member of.	int	
DEVICE_GROUP_ENTRY_ID	Unique database auto generated identifier.	int	
DEVICE_ID	Database ID of the member DEVICE.	int	

TABLE 98 DEVICE_GROUP

Field	Definition	Format	Size
DEVICE_GROUP_ID	Primary key for this table.	int	
NAME	Name of this device group.	varchar	128
USER_ID	User ID corresponds to the user who created the device.	int	

TABLE 98 DEVICE_GROUP (Continued)

Field	Definition	Format	Size
DESCRIPTION	Device group description.	varchar	255
IS_PUBLIC	Flag to identify whether this group is shared across users.	num	(1,0)
IS_INTERNAL	Flag to identify this group is internal.	num	(1,0)
TABLE_SUBTYPE	Table subtype defined by BizObject framework	varchar	32
IS_AP_GROUP	Flag to identify whether this group is access point device group.	num	(1,0)
IS_SENSOR_GROUP	Flag to identify whether this group is sensor device group.	num	(1,0)
VIEW_MASK	Flag to decide whether to show the device group in topology or not.	num	(1,0)
GROUP_TYPE	This flag is to classify the device group type: • 0 is the default and reserved for internal temporary group • 1 is for System Device Group • 2 is for MPLS System Device Group • 3 is for User Defined Device Group	int	

TABLE 99 DEVICE_MAC_GROUP_MAPPING

Field	Definition	Format	Size
MAC_GROUP_DB_ID	Foreign Key Reference to the MAC_GROUP table. Part of Primary key.	int	
DEVICE_ID	Foreign Key reference to DEVICE table. Part of Primary key;	int	

TABLE 100 DEVICE_NODE

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
FABRIC_ID	Fabric DB ID to which this device node belongs.	int	
WWN	Device node WWN.	char	23
TYPE	Initiator or target or both or unknown. The possible values are Initiator, Target, Initiator+Target, Unknown(Initiator or Target)	varchar	32
DEVICE_TYPE	0 = physical 1 = virtual 2 = NPV 3 = iSCSI 4 = both physical & virtual	smallint	
SYMBOLIC_NAME	Device node symbolic name.	varchar	256
FDMI_HOST_NAME	Device node FDMI host name.	varchar	128
VENDOR	Device node vendor.	varchar	64
CAPABILITY_		varchar	16

TABLE 100 DEVICE_NODE (Continued)

Field	Definition	Format	Size
TRUSTED	1 = the node is trusted for "fabric tracking. Default value is 0.	smallint	
CREATION_TIME	Timestamp when the record is created by the Management application server.	timestamp	
MISSING	1 = the device node is missing from the fabric. Default value is 0.	smallint	
MISSING_TIME	Time when the device node missed.	timestamp	
PROXY_DEVICE	One of the device ports of this device node has translated domain. That device port is set as the Proxy Device and this Device Node is treated as virtual by assigning a value of 1 to this field. Default value is 0.	smallint	
AG	1 = the device node is actually an AG connected to a switch in the fabric. Default value is 0.	smallint	
PREVIOUS_MISSING_STATE	Default value is 0.	smallint	

TABLE 101 DEVICE_PORT

Field	Definition	Format	Size
NODE_ID	Reference to the ID of the Device Node of which this device port is a part of.	int	
DOMAIN_ID	Stores the Domain ID of the switch to which this device port is connected to.	int	
WWN	Stores the Device Port WWN	char	23
SWITCH_PORT_WWN	Stores the switch port wwn to which this device port is physically connected to. However If the device is connected to an AG, this will contain the switch port WWN till the AG impact is applied by the application. If AG impact fails to be applied this will continue to have the switch port wwn instead of the AG port wwn.	char	23
NUMBER	Stores the port number of this device port.	smallint	
PORT_ID	Stores the FDMI host name.	varchar	6
TYPE	Stores the Vendor of this device.	varchar	32
SYMBOLIC NAME	Stores the Symbolic Name.	varchar	256
FC4_TYPE		varchar	64
COS	Stores the Class of Service.	varchar	16
IP_PORT		varchar	63
HARDWARE_ADDRESS	Stores the Hardware Address.	varchar	32
TRUSTED	Denotes if the device port is trusted or not.	smallint	
CREATION_TIME	The creation time of this record.	timestamp	

TABLE 101 DEVICE_PORT

Field	Definition	Format	Size
MISSING	Denotes if this device port is missing or not.	smallint	
MISSING_TIME	Denotes the time from which the device port is missing. Applicable only if the device is missing.	timestamp	
NPV_PHYSICAL	Denotes if this is physical device port or a logical NPIV port.	smallint	
EDGE_SWITCH_PORT_WWN	EDGE_SWITCH_PORT_WWN will be the same as the SWITCH_PORT_WWN except in the case of devices behind the AG. This field will be updated by the name server info collector, added for the feature support of AG WWN N port mapping. This is a null able field. It is used to determine which mapping is used by the AG.	char	23
LOGGED_TO_AG	Indicates if the device is connected with an AG. Not null field and default value is 0, device not connected to AG	smallint	
AG_NODE_WWN	If the device is connected with an AG, the AG switch WWN will be populated. Not null field and default value is empty	char	23
AG_N_PORT_WWN	If the device is connected with an AG, N-Port WWN of AG which is connected to switch will be populated from the N2F and N2WWN map	char	23
MISSING_REASON	The device missing reason.	varchar	1024

TABLE 102 DEVICE_PORT_GIGE_PORT_LINK

Field	Definition	Format	Size
DEVICE_PORT_ID	The primary key of the DevicePort	int	
GIGE_PORT_ID	The primary key of the GigEPort.	int	
DIRECT_ATTACH	Indicates whether the device port is directly attached to the CEE 10G TE port.	smallint	
VIRTUAL_FCOE_PORT_ID	The value of virtual_fcoe_port_id in the Device_Port_Gige_Port_Link table is applicable only for NOS devices. For FOS devices, the virtual_fcoe_port_id value, will be null, as currently in the Management application that mapping data is not collected. Hence the default value is null.	int	
LAG_ID	LAG interface ID which associates port channel with end device. This will be null if device port is associated with physical gige port.	int	

TABLE 103 DEVICE_PORT_MAC_ADDRESS_MAP

Field	Definition	Format	Size
DEVICE_PORT_ID	The primary key of the device port	int	
MAC_ADDRESS	Mac address of the device	varchar	64

TABLE 104 DISK_USAGE

Field	Definition	Format	Size
ID	Primary key of the table. Autogenerated.	int	
TIME_THRESHOLD_CROSSED	Holds the timestamp at which the disk space was analyzed and found to have crossed the threshold (both low to high and vice versa).	timestamp	
MEMORY_UTILIZATION	Holds the disk usage as a percentage. Value varies from 0 to 100.	double precision	
THRESHOLD_TYPE	Denotes whether disk space usage crosses above or below threshold limit. 1 if it is goes above threshold, 0 if it goes below threshold (in previous instance it was above threshold).	smallint	
FREE_SPACE	Holds the free disk space at the particular time in bytes.	bigint	
TOTAL_SPACE	Holds the total disk space at the particular time in bytes.	bigint	

TABLE 105 ENCRYPTION_ENGINE

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
SWITCH_ID	Foreign key reference to both the VIRTUAL_SWITCH table and the CRYPTO_SWITCH table (both switch tables use the same primary key values). Identifies the switch that contains this encryption engine.	int	
SLOT_NUMBER	For chassis switches, the slot or blade that contains the encryption engine. Always 0 for pizza-box switches with a single embedded encryption engine.	smallint	
STATUS	Not used. Previously used to indicate the engine''s operational status. Replaced by EE_STATE. The default value is 0.	smallint	
HA_CLUSTER_ID	Foreign key reference to an HA_CLUSTER record. Identifies the HA Cluster that this engine belongs to. Null if this engine does not belong to an HA Cluster.	int	
SYSTEM_CARD_STATUS	Indicates whether a System Card is currently inserted in the Encryption Engine, and whether the card is valid or not. This feature is not yet supported. The default value is ‘disabled’.	varchar	256
WWN_POOLS_AVAILABLE	Not used. Previously used to indicate the number of WWN pools remaining for allocation on this encryption engine. This feature is no longer supported.	int	
STATE	Administrative state for this engine. 0 = disabled, 1 = enabled. The default value is 0.	smallint	

TABLE 105 ENCRYPTION_ENGINE (Continued)

Field	Definition	Format	Size
SP_CERTIFICATE	The public key certificate, in PEM format, for the Security Processor within the Encryption Engine. Used to create link keys for Decru LKM key vaults.	varchar	4096
EE_STATE	The operational status of this Encryption Engine. For possible values, see the enum defintion in the DTO class The default value is 0.	int	
HA_CLUSTER_STATUS	Stores the status of the HA Cluster to which the engine is a pair participant The default value is 0.	smallint	
ROUTING_MODE		smallint	
MEDIA_TYPE		char	50
LINK_IP_ADDRESS	Local EE - BP Link IP Address, If there are no links the IP Address could be 0.0.0.0	varchar	64
LINK_NET_MASK	Local EE - BP Link IP new mask	varchar	64
LINK_GW_IP_ADDRESS	Local EE- BP Gateway Address	varchar	64
LINK_MAC_ADDRESS	Local EE Link MAC Address	varchar	64
INK_MTU	Local EE Link MTU. The default value is -1.	int	
LINK_STATE	Local EE State says whether link is down or up	varchar	256
REBALANCE_REQUIRED	This field indicates whether a rebalance operation is required on the Encryption Engine. It can take two values, One(1) indicating that rebalance is required on the Encryption Engine and zero(0) indicating that no rebalance is required on the Encryption Engine. Encryption Engine is said to be unbalanced when the disk and Tape containers are not evenly balanced on the hosting engine. The default value is 0.	smallint	

TABLE 106 ENCRYPTION_GROUP

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
NAME	User-assigned name for this encryption group.	varchar	64
LEADER_SWITCH_ID	'Foreign key reference to both the VIRTUAL_SWITCH table and the CRYPTO_SWITCH table (both switch tables use the same primary key values). Identifies the switch that currently provides central configuration and reporting capabilities for the encryption group. This column may be null if the group leader is not in a discovered fabric.	int	
LEADER_SWITCH_WWN	The Node WWN of the current group leader switch. Each encryption group has one group leader switch.	char	23

TABLE 106 ENCRYPTION_GROUP (Continued)

Field	Definition	Format	Size
DEPLOYMENT_MODE	Indicates Transparent (0) or NonTransparent (1) deployment mode. Only Transparent mode is currently supported. All switches in the Encryption Group share the same deployment mode. Transparent mode uses re-direction zones to preserve existing zoning of physical hosts and targets. Non-transparent mode requires zoning changes to zone physical hosts with Virtual Targets and to zone Virtual Initiators with physical targets. The default value is 0.	smallint	
FAILBACK_MODE	Indicates Automatic (0) or Manual (1) failback. Failback occurs when a previously unavailable Encryption Engine comes back online. In Auto mode, the restored Encryption Engine resumes encrypting all traffic for target containers configured on the Encryption Engine. In manual mode, encryption continues running on the backup encryption engines until manually changed. The default value is 0.	smallint	
SYSTEM_CARD_REQUIRED	Boolean value that indicates whether a System Card (smart card) must be inserted in the Encryption Engine to enable the engine after power-up. This feature is not yet supported. The default value is 0.	smallint	
ACTIVE_MASTER_KEY_ STATUS	The operational status of the "master key" or "Key Encryption Key (KEK)" used to encrypt Data Encryption Keys in a key vault. Not used for Decru LKM key vaults. 0 = not used, 1 = required but not present, 2 = present but not backed up, 3 = okay. The default value is 0.	smallint	
ALT_MASTER_KEY_STATUS	The operational status of an alternate "master key" used to access older data encryption keys. Not used for Decru LKM key vaults. 0 = not used, 1 = not present, 3 = okay. The default value is 0.	smallint	
QUORUM_SIZE	The number of authentication cards required to approve certain secure operations. This feature is not yet supported. The default value is 0.	smallint	
RECOVERY_SET_SIZE	No longer used. Previously used to indicate the number of smart cards used to back up a Master Key. The number of cards is now specified when the backup is created, and not persisted in the database. The default value is 0.	smallint	
KEY_VAULT_TYPE	Indicates the type of key vault used by switches in this Encryption Group. 0 = Decru Lifetime Key Manager (LKM), 1 = RSA Key Manager (RKM), 2 = Brocade internal key storage (for demo use only). The default value is 0.	smallint	

TABLE 106 ENCRYPTION_GROUP (Continued)

Field	Definition	Format	Size
PRIMARY_KEY_VAULT_ID	Foreign key reference to the KEY_VAULT record that describes the primary key vault for this Encryption Group. Null if no primary key vault is configured.	int	
BACKUP_KEY_VAULT_ID	Foreign key reference to the KEY_VAULT record that describes the backup key vault for this Encryption Group. Null if no backup key vault is configured.	int	
GROUP_LEADER_STATUS	Stores the status of the Group leader node	int	
SRDF_MODE	This field denotes whether the SRDF support is enabled or not. Feature available only from 6.4 release onwards and for RSA key vaults. EncryptionGroup collector and EncryptionGroupBean fills in this value. The default value is -1.	smallint	

TABLE 107 ENCRYPTION_GROUP_MEMBER

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
ENCRYPTION_GROUP_ID	Foreign key reference to the ENCRYPTION_GROUP record that identifies the encryption group that this member switch belongs to	int	
MEMBER_IP_ADDRESS	The management IP address (IPv4, IPv6, or hostname) of the member switch	varchar	128
MEMBER_WWN	the node WWN of the member switch	char	23
MEMBER_STATUS	The reachability status of the member switch as seen by the group leader switch. For possible values see the enum definition in the DTO class	smallint	

TABLE 108 ENCRYPTION_KMIP_PARAMETERS

Field	Definition	Format	Size
ENCRYPTION_GROUP_ID	Foreign key reference to the ENCRYPTION_GROUP record that describes the group ID of this Encryption Group.	int	
HA_MODE	Indicates the configured High Availability mode for the encryption group. Possible values are noHA, opaque, transparent, and NA.	varchar	32
AUTHENTICATION_MODE	Indicates the configured User Authentication mode for the encryption group. Possible values are None, Username, UserPass, and NA.	varchar	32
CERTIFICATE_TYPE	Indicates the configured Certificate Type for the encryption group. Possible values are self, CASign, and NA.	varchar	32

TABLE 109 ENCRYPTION_TAPE_POOL

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
SWITCH_ID	No longer used. Tape pools used to belong to specific switches, but are now shared by all switches in an encryption group	int	
ENCRYPTION_ENGINE_ID	No longer used. Tape pools used to belong to specific encryption engines, but are now shared by all encryption engines in an encryption group	int	
ENCRYPTION_GROUP_ID	Foreign key reference to the ENCRYPTION_GROUP record that describes which encryption group this tape pool belongs to	int	
TAPE_POOL_NAME	User-supplied name or number for the tape pool. This is the same name or number specified in the tape backup application. Numbers are stored in hex	varchar	64
TAPE_POOL_OPERATION_MODE	Specifies which type of encryption should be used by tape volumes in this tape pool. 0 = Native, 1 = DF-compatible	smallint	
TAPE_POOL_POLICY	Specifies whether tape volumes in this tape pool should be encrypted. 0 = encrypted, 1 = cleartext	smallint	
KEY_EXPIRATION	Number of days each data encryption key for this tape pool should be used. After the configured number of days, a new data encryption key is automatically generated for any further tape volumes in this pool. 0 = no expiration	int	
TAPE_POOL_LABEL_TYPE	Indicates whether the TAPE_POOL_NAME field is a name or a number. 0 = name, 1 = number	smallint	

TABLE 110 ETHERNET_CLOUD

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
SWITCH_ID	The unique id of the switch this cloud is associated to.	int	

TABLE 111 ETHERNET_ISL

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
SOURCE_PORT_ID	The unique id of the source port.	int	
DEST_PORT_ID	The unique id of the destination port.	int	
MISSING	Flag to identify whether the ethernet isl link is missing from the switch.	smallint,	
MISSING_TIME	Time when the ethernet isl link is missing from the switch.	timestamp	

TABLE 111 ETHERNET_ISL (Continued)

Field	Definition	Format	Size
TRUSTED	Is this ethernet isl link is trusted.	smallint,	
CREATION_TIME	Time when the ethernet isl link record is created.	timestamp	

TABLE 112 EVENT

Field	Definition	Format	Size
ID*	Unique generated database identifier for an event.	int	
ME_ID	Unique managed element ID used to refer the product that is associated with the event.	int	
SEVERITY	Indicates the severity of the event. Possible values : Emergency- 0, Alert- 1, Critical- 2, Error- 3,Warning- 4,Notice- 5, Info- 6,Debug- 7,Unknown- 8.	int	
AREA	Indicates the Area from which the event has occurred. Possible values : Unknown- 0, SAN- 1, IP- 2, Application Events -3, SAN+IP- 4.	smallint	
ACKNOWLEDGED	Indicates whether the user has acknowledged the event or not. Possible values: Unacknowledged-0 , Acknowledged-1.	smallint	
SOURCE_NAME	This field indicates the name of the source that triggered the event. This could be the name of the source switch or name of the Management application server in the case of application events.	varchar	255
SOURCE_ADDR	'Indicates the IP Address of the source that triggered the event. This could be the IP address of the source switch or IP address of the Management application server in the case of application events.	varchar	50
EVENT_ORIGIN_ID	Database ID of the event origin such as Trap, Syclog etc referring to EVENT_ORIGIN metadata.	int	
EVENT_CATEGORY_ID	Database ID of the event category referring to EVENT_CATEGORY metadata.	int	
EVENT_MODULE_ID	Database ID of the event module referring to EVENT_MODULE metadata.	int	
EVENT_DESCRIPTION_ID	Indicates the identifier of the event description in the EVENT_DESCRIPTION table.	int	
LAST_OCCURRENCE_HOST_TIME	Indicates the the Management application server timestamp when this event occurred last.	timestamp	
EVENT_COUNT	Indicates the number of occurrences of the event. Count indicates the number of times the same event occurred in a given ten minute window.	int	
RESOLVED	This field indicates whether an event is resolved due to another matching event or based on user action. Possible values: Unresolved – 0, Resolved – 1.	smallint	
ACKED_TIME	Indicates the timestamp when the event was acknowledged.	Timestamp	
FIRST_OCCURRENCE_HOST_TIME	Indicates the the Management application server timestamp when the event occurred for the first time.	timestamp	10

TABLE 112 EVENT (Continued)

Field	Definition	Format	Size
EVENT_AUDIT	'Indicates whether this is an audit event or not.	varchar	255
EVENT_KEY	Unique key for the event. This is a string message key represents message ID from events originated from switch or the predefined message Id for application events in the Management application.	varchar	
EVENT_ACTION_ID	Reference to the ID in the EVENT_POLICY table. Represents the event action policy that was responsible for generating this event.	int	
DEVICE_GROUP_ID	Reference to the DEVICE_GROUP_ID in the DEVICE_GROUP table.	int	
PORT_GROUP_ID	Reference to the ID in the PORT_GROUP table.	int	
SPECIAL_EVENT	'Indicates whether the event is marked as special event or not. Not a Special event-0, Special event-1.	smallint	

TABLE 113 EVENT_CALL_HOME

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
EVENT_ID	Database ID of the EVENT instance.	int	
EVENT_NUMBER	Indicates the Event Number for the event from the Events.html of the associated product .	int	
FRU_CODE	Indicates the Field Replaceable Unit code of the Call Home event.	int	
REASON_CODE	Indicates the reason code of the Call Home event.	int	
FRU_POSITION	Indicates the FRU position of the Call Home event.	int	

TABLE 114 EVENT_CATEGORY

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
DESCRIPTION	Holds the event categories. Possible values : Unknown- 0, Product Event- 1, Link Incident Event- 2 , Product Audit Event- 3, Product Status Event- 4, Security Event- 5 , User Action Event- 6, Management Server Event- 7.	varchar	50

TABLE 115 EVENT_DESCRIPTION

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
DESCRIPTION	Holds the description of the Event.	varchar	1024

TABLE 116 EVENT_DETAILS

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
EVENT_ID	Database ID of the EVENT instance.	int	
FIRST_OCCURRENCE_SWITCH_TIME	Indicates the first occurrence switch timestamp of the event.	timestamp	
LAST_OCCURRENCE_SWITCH_TIME	Indicates the last occurrence switch timestamp of the event.	timestamp	
CONTRIBUTORS	Indicates the contributing factor for the event resulted due to a status change of the switch.	varchar	512
OPERATIONAL_STATUS	Indicates the operational Status of the product associated with the event.	varchar	255
NODE_WWN	Unique World Wide Number for the product.	varchar	23
PORT_WWN	Unique World Wide Number for the port for which the event was generated.	varchar	23
OID	Indicates the Object ID of the Trap or Syslog.	varchar	50
VIRTUAL_FABRIC_ID	Indicates the Virtual Fabric id of the switch which triggered the event.	smallint	
UNIT	Indicates the Unit number of the Chassis from which the event was triggered.	smallint	
SLOT	Indicates the blade or the slot number in which the port is present.	int	
PORT	indicates the switch port number for which the event was generated.	int	
PRODUCT_ADDRESS	Indicates the IP Address of the Product from which the event is originated.	varchar	
RAS_LOG_ID	Indicates the RASLOG Id of the RASLOG event.	varchar	20
INTERFACE_TYPE	Indicates the type of the interface – Possible Values: Ethernet Port-0, FC Port-1.	smallint	
USER_NAME	Captures the user information from audit Syslog messages.	Varchar	512
PORT_NAME	Shows the PortName for the corresponding port.	Varchar	255
MAC_ADDRESS	'Indicates the MAC address of the Access Point from which this event is received. If the event is received from the wireless controller or any other products, this will be empty.';	varchar	64

TABLE 117 EVENT_FWD_FILTER

Field	Definition	Format	Size
ID		int	
NAME	Filter Name	varchar	32
DESCRIPTION		varchar	256
TYPE	Filter Type (SNMP/ SYSLOG)	smallint	
APPLICATION_ENABLED	If Application Events enabled	smallint	

TABLE 117 EVENT_FWD_FILTER (Continued)

Field	Definition	Format	Size
SNORT_ENABLED	If Snort Messages enabled	smallint	
PSUDO_ENABLED	If Pseudo Events enabled	smallint	
REGULAR_EXP	Common filtering message for Syslog Forwarding	varchar	512
SEVERITY	Emergency(0), Alert(1), Critical(2), Error(3), Warning(4), Notice(5), Info(6), Debug (7). Traps with selected severity and those with higher severity will be forwarded.	smallint	

TABLE 118 EVENT_INSTANCE

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
EVENT_POLICY_ID	Foreign Key to Event_Policy Table	int	
EVENT_KEY	A String Key string which identifies a specific instance of an Event.	varchar	64
STRING_PATTERN	A Regular expression pattern string which can be used to match an Event instance.	varchar	1024
CATEGORY	A small integer which identifies the Category of an Event instance. 0 - Unknown 1 - Product Event 2- Link Incident Event 3 - Product Audit Event 4- Product Status Event 5 - Security Event 6- User Action Event 7- Management Server Event. The default value is 0.	smallint	
SEVERITY	The Severity of the Event that is logged per Event Policy 0- Unknown 1- Emergency 2- Alert 3- Critical 4- Error 5- Warning 6- Notice 7- Info 8- Debug. The default value is 0.	smallint	
SEQUENCE_NUMBER	The sequence number of an event instance that''s specific to the policy. The default value is 0.	smallint	
MSG_IDS	Stores the Message ID(s) configured for Custom Event Type	varchar	512

TABLE 119 EVENT_MODULE

Field	Definition	Format	Size
ID	The default value is 0.	int	
DESCRIPTION		varchar	256

TABLE 120 EVENT_NOTIFICATION

Field	Definition	Format	Size
ID*		int	
STATUS	Status of Event Notification. value will be 0 if disabled, 1 otherwise. Default value is 0.	smallint	
SERVER_NAME	E-mail (SMTP) server name.	varchar	256
REPLY_ADDRESS	Reply E-mail address.	varchar	50
SEND_ADDRESS	E-mail address for which a Test E-mail notification is to be sent.	varchar	512
SMTP_PORT	SMTP Port number. Default value is 25.	int	
USER_NAME	User name for authentication.	varchar	256
PASSWORD	Password for authentication.	varchar	256
NOTIFICATION_INTERVAL	Time interval between successive event notifications.	int	
NOTIFICATION_UNIT	Time interval Unit: 0 = Seconds 1 = Minutes 2 = Hours Default value is 0.	smallint	
TEST_OPTION	Time interval Unit: 0 = Send test to configured e-mail address. 1 = Send test to all enabled users. Default value is 0.	smallint	
SSL_ENABLED	Default value is 0.	smallint	

TABLE 121 EVENT_ORIGIN

Field	Definition	Format	Size
ID	0 - Unknown 1 - Trap 2 - Syslog 3 - Snort 4 - Pseudoevent 5 - Application Events 6 - Others	int	
DESCRIPTION		varchar	50

TABLE 122 EVENT_POLICY

Field	Definition	Format	Size
ID		int	
TYPE	Even Policy Type 0 - Pseudo Event 1 - Event Action	smallint	
NAME	The Name of the Event Policy	varchar	256
DESCRIPTION	The Description of the Event Policy	varchar	1024

TABLE 122 EVENT_POLICY (Continued)

Field	Definition	Format	Size
STATUS	Administrative status of the Event Policy 0 - disabled 1- enabled	smallint	
LAST_MODIFIED_TIME	The Severity of the Event that is logged per Event Policy 0- Unknown 1- Emergency 2- Alert 3- Critical 4- Error 5- Warning 6- Notice 7- Info 8- Debug';	timestamp	
SEVERITY	The Event Policy Sub Type Escalation (0), Resolving (1), Flapping (2),Repeating (3). The default value is 0.	smallint	
MESSAGE		varchar	256
SUB_TYPE	The Event Policy Sub Type Escalation (0), Resolving (1), Flapping (2),Repeating (3)	smallint	
EVENT_ORIGIN	0- SNMP Trap 1- Application Event 2- Pseudo Event 3- Snort 4- Pseudo Event 5- Custom Event	smallint	
PROPERTIES	The property string which is used to define various parameters that are associated with an Event Policy such as flapping time and durations etc	varchar	2048

TABLE 123 EVENT_POLICY_SOURCE_ENTRY

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
EVENT_POLICY_ID	Foreign Key to Event_Policy Table	int	
MANAGEMENT_ELEMENT_ID	A soft reference key to the Management Element ID. Do not maintain it as a foreign key constraints. The default value is 0.	int	
INTERFACE_ID	A soft reference key to the Interface ID. Do not maintain it as a foreign key constraints. The default value is 0.	int	
DEVICE_GROUP_ID	A reference key to the Device Group Do not maintain it as a foreign key constraints. The default value is 0.	int	
PORT_GROUP_ID	A reference key to the Port Group Do not maintain it as a foreign key constraints. The default value is 0.	int	
SOURCE_SELECTION_TYPE	Option selected to give Source Information • 0- IPAddress/Node wwn/Name provided • 1- Source selected from available list of sources. The default value is 0.	smallint	
IP_ADDRESS	IP address of source	varchar	1024

TABLE 123 EVENT_POLICY_SOURCE_ENTRY (Continued)

Field	Definition	Format	Size
WWN	Node WWN of source	varchar	1024
SOURCE_NAME	Source Name	varchar	1024

TABLE 124 EVENT_PROCESSOR_MAP

Field	Definition	Format	Size
PROCESSOR_CLASS_NAME	The fully qualified processor class name which will be invoked for the corresponding event id in this table. Column added as part of the Event Processing Framework	varchar	1024
EVENT_ID	The Event Id is the Trap OID on which the corresponding processor needs to act up on . Column added as part of the Event Processing Framework	varchar	1024

TABLE 125 EVENT_RULE

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
NAME	Name of the Event Rule.	varchar	255
TYPE	Event Rule Type: • 0 = Port Offline • 1 = PM Threshold crossed • 2 = Security Violation • 4 = Event	int	
DESCRIPTION	Description about the Event Rule.	varchar	512
OPERATOR1	AND operator used to append the rule.	varchar	12
EVENT_TYPE_ID	The Selected Event type ID from the Event type combo box.	int	
OPERATOR2	AND operator used to append the rule.	varchar	12
MESSAGE_ID	Message ID provided by the user.	varchar	20
OPERATOR3	AND operator used to append the rule.	varchar	12
IP_ADDRESS	Source IP Address.	varchar	1024
OPERATOR4	AND operator used to append the rule.	varchar	12
WWN	Source WWN.	varchar	1024
OPERATOR5	AND operator used to append the rule.	varchar	12
COUNT	Count of the specified event.	int	
OPERATOR6	AND operator used to append the rule.	varchar	12
DURATION	Duration of the specified event.	bigint	
STATE	State of the rule: • 0 = Disabled • 1 = Enabled	smallint	
SEVERITY_LEVEL	Event severity level. Default value is 4.	int	

TABLE 125 EVENT_RULE (Continued)

Field	Definition	Format	Size
SOURCE_NAME	Name of the source.	varchar	1024
DESCRIPTION_CONTAINS	Description pattern about the rule.	varchar	255
LAST_MODIFIED_TIME	Rules last edited time.	timestamp	
SELECTED_TIME_UNIT	Timestamp unit of the selected rule: • 0 = second • 1 = Minutes • 2 = Hours Default value is 1.	smallint	

TABLE 126 EVENT_RULE_ACTION

Field	Definition	Format	Size
ID*		int	
RULE_ID	The rule ID present in the Event_Rule Table.	int	
NAME	Name of the Event Rule Action: • Launch Script = for launch script • Send E-mail = for send e-mail • Raise Event = for broadcast message	varchar	255
TYPE	Name of the action: • script = for Launch Script • e-mail = for E-mail • message = for Broadcast message	varchar	30
FIELD1	Data for the selected action.	varchar	512
FIELD2	Data for the selected action.	varchar	512
FIELD3	Data for the selected action.	varchar	512
FIELD4	Data for the selected action.	varchar	512
STATE	State of the Action: • 0 = Action Disabled • 1 = Action Enabled Default value is 0.	smallint	

TABLE 127 FABRIC

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
SAN_ID	Foreign key to SAN table; usually 1 since there is only one SAN.	int	
SEED_SWITCH_WWN	WWN of the virtual switch used as seed switch to discover the fabric.	char	23
NAME	User-assigned fabric name.	varchar	256
CONTACT	User-assigned "contact" for the fabric.	varchar	256
LOCATION	User-assigned "location" for the fabric.	varchar	256
DESCRIPTION	User-assigned fabric description.	varchar	256

TABLE 127 FABRIC (Continued)

Field	Definition	Format	Size
TYPE	Denotes the type of Fabric. 0 = legacy fabric, 1 = base fabric, 2 = logical fabric, 3 = partial fabric, 4 = ethernet fabric. Default value is 0.	smallint	
SECURE	1 = it is a secured fabric. Default value is 0.	smallint	
AD_ENVIRONMENT	1 = there are user-defined ADs in this fabric. Default value is 0.	smallint	
MANAGED	1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric. Default value is 1.	smallint	
MANAGEMENT_STATE	Bit map to indicate various management indications for the fabric. Default value is 0.	smallint	
TRACK_CHANGES	1 = changes (member switches, ISL and devices) in the fabric are tracked. Default value is 0.	smallint	
STATS_COLLECTION	1 = statistics collection is enabled on the fabric. Default value is 0.	smallint	
CREATION_TIME	When the fabric record is inserted, i.e., created. Default value is 'now()'.	timestamp	
LAST_FABRIC_CHANGED	Time when fabric last changed.	timestamp	
LAST_SCAN_TIME	Last Scan time for the fabric i.e. when the switch was scanned for changes.	timestamp	
LAST_UPDATE_TIME	Time when fabric was last updated. Default value is 'now()'.	timestamp	
ACTIVE_ZONESET_NAME	Name of the zone configuration which is effective / active in that fabric.	varchar	256
USER_DEFINED_VALUE_1	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_2	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_3	User-defined custom value.	varchar	256
PRINCIPAL_SWITCH_WWN	WWN of the principal switch of the fabric	char	23
ZONE_TRANSACTION_TIMEOUT	Number of seconds that a ZONE_TRANSACTION can be idle Default value is 180.	int	
FABRIC_MODEL	Default value is 1.	smallint	
LAST_FAILURE_TIMESTAMP	Denotes the last failure timestamp.	timestamp	
LAST_SUCCESSFUL_TIMESTAMP	Dentoes the last successful timestamp.	timestamp	
ENHANCED_TI_ZONE_SUPPORT	Holds the value if the fabric has enhanced TI Zone support or not. Default: 0 Values: 0|1.	smallint	

TABLE 127 FABRIC (Continued)

Field	Definition	Format	Size
FABRIC	The fabric name persisted on switches running FOS 7.0 and later. Not to be confused with NAME, which is store on Network Advisor only.	varchar	128
STATUS	Overall operational status of the fabric. 0 is unknown, 1 is healthy, 2 is marginal, 3 is down, 5 is Reachable, 6 is unreachable, 7 is Degraded link.	int	
TRACKING_STATUS	This represents bitmask as an integer value which represents missing or untrusted state of fabric members, ISLs, SANConnections, device Nodes and device ports. 1 is missing switch/ISL in fabric, 2 is untrusted switch or ISL in fabric, 4 is missing initiator or port in fabric, 8 is untrusted initiator or port in fabric, 16 is missing target or port in fabric, 32 is untrusted target or port in fabric.	int	
BOTTLENECK_STATUS	Holds bottleneck status of fabric. Default is 0, Values are 0 or 1.	int	
VCS_LICENSED	Indicates whether the fabric has VCS license or not. Possible values are 0 for not applicable, 1 for licensed, 2 for not licensed. 0 is default. Fabrics representing clusters with 2 or less nodes will have value of 0 as all those are automatically licensed. Fabrics representing clusters with 3 or more nodes will have values 1 or 2 depending on whether the license was acquired or not.	int	
HAS_NOS_AG	Denotes whether fabric has NOS AG connected to it or not. 0 denotes that the fabric has no NOS AG connected to it and 1 denotes a NOS AG is connected to the fabric. -1 denotes that it is not applicable and will be set to NOS clusters.	int	

TABLE 128 FABRIC_CHECKSUM

Field	Definition	Format	Size
FABRIC_ID *	Fabric ID, foreign key to the FABRIC table.	int	
CHECKSUM_KEY *	Type of checksum, e.g. device data or zone data.	varchar	32
CHECKSUM	Actual checksum value.	varchar	16

TABLE 129 FABRIC_COLLECTION

Field	Definition	Format	Size
FABRIC_ID *	Fabric ID, foreign key to the FABRIC table.	int	
COLLECTOR_NAME *	Name of the collector, e.g., NameServerInfoCollector, TopologyCollector, ZoneInfoCollector, ActiveZoneInfoCollector.	varchar	256

TABLE 129 FABRIC_COLLECTION (Continued)

Field	Definition	Format	Size
SEED_SWITCH_IP	IP address of the switch which serves as the seed switch. This is the switch from which above mentioned fabric level collectors get their information.	varchar	128
LAST_SEED_SW_ MODIFICATION	Timestamp of the seed switch, when the particular HTML page was changed last. Note that this is not when the last time collection was done.	timestamp	

TABLE 130 FABRIC_DISCOVERY_POLICY

Field	Definition	Format	Size
FABRIC_ID	The database ID of the fabric that the policy belongs to.	int	
DISCOVER_ALL_MEMBERS	This column indicates if all the members of the fabric can be discovered. 1 means discover all members and 0 means do not discover all members. In the case of 0, the filtering rules comes from FabricDiscoveryPolicyRule table.	smallint	
CREATION_TIME		timestamp	
LAST_UPDATE_TIME		timestamp	

TABLE 131 FABRIC_DISCOVERY_POLICY_RULE

Field	Definition	Format	Size
ID		serial	
FABRIC_ID	The database ID of the fabric that the policy belongs to.	int	
FILTER	Filter to be applied for this fabric. This could be IP Address or WWN or SwitchType. The Type of the filter comes from the FilterType column. This can be either in included list or excluded list depending on the EXCLUDED column value.	varchar	128
FILTER_TYPE	This column indicates type of the filter. It could take values like 0 for IP Address, 1 for WWN and 2 for SwitchType. Default is IP address type.	smallint	
EXCLUDED	This column indicates if the Filter in the record should be included or excluded. 1 means exclude and 0 means include. Default is to include.	smallint	
CREATION_TIME		timestamp	
LAST_UPDATE_TIME		timestamp	

TABLE 132 FABRIC_MEMBER

Field	Definition	Format	Size
FABRIC_ID*	Fabric ID, foreign key to FABRIC table.	int	
VIRTUAL_SWITCH_ID*	ID of the virtual switch which is a member of this fabric, foreign key to VIRTUAL_SWITCH table.	int	

TABLE 132 FABRIC_MEMBER (Continued)

Field	Definition	Format	Size
TRUSTED	1 = the switch is a trusted member of the fabric. Either found in the initial discovery or user subsequently entrusted the switch by user action. Default Value is 0.	smallint	
CREATION_TIME	When the switch became a member. Default Value is 'now()'.	timestamp	
MISSING	1 = it is missing from the fabric. Default Value is 0.	smallint	
MISSING_TIME	When it is missed from the fabric; null if the member is entrusted.	timestamp	
LAST_UPDATE	Last Updated time for the record.	bigint	

TABLE 133 FABRIC_THRESHOLD_SETTING

Field	Definition	Format	Size
FABRIC_ID*	References the ID in FABRIC table	int	
POLICY_ID*	References the ID in THRESHOLD_POLICY table	int	

TABLE 134 FABRIC_VCS_CLUSTER_MAP

Field	Definition	Format	Size
FABRIC_ID	Foreign key to ID in fabric table.	int	
VCS_CLUSTER_ME_ID	Foreign key to ID in ManagedElement table. This is the VCS cluster entry managed_element_id reference.	int	

TABLE 135 FABRIC_ZONING_EDIT_RESTRICTION

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
FABRIC_ID	PK of the owning fabric	int	
CHANGE_COUNT	Count of the maximum changes allowed in active zone config in the fabric.The default value is 0.	int	

TABLE 136 FAVORITES

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
NAME	Name of the favorite.	varchar	64
USER_	The application user credentials.	varchar	128
TOP_N	The top number of ports(5,10,15,20).	varchar	40
SELECTION_FILTER	Types of ports (FC/FCIP/GE) and -End Monitors.	varchar	40

TABLE 136 FAVORITES (Continued)

Field	Definition	Format	Size
FROM_TIME	The time interval in which the graph is shown. Time interval can be predefined or custom. If FROM_TIME is Custom, the user can choose the number of minutes/hours/days or specify the time interval.	varchar	40
CUSTOM_LAST_VALUE	The number of minutes/hours/days. It becomes null in two cases. 1. When the value of FROM_TIME is not Custom. 2. When FROM_TIME is Custom, and user chooses the time interval (CUSTOM_FROM and CUSTOM_TO)	int	
CUSTOM_TIME_UNIT	The unit type (Minutes, Hours, Days) of the CUSTOM_LAST_VALUE.	varchar	40
CUSTOM_FROM	The starting time.	timestamp	
CUSTOM_TO	The ending time.	timestamp	
GRANULARITY	The granularity.	varchar	40
THRESHOLD	The reference line.	int	
MAIN_MEASURE	The measure of FC/FCIP/GE.	varchar	40
ADDITIONAL_MEASURE	The additional measures.	int	
CUSTOM_SELECTION_OBJECT_TYPE	Represents the selected filter type. • 0 - Default favorite • 1 - FC Ports • 2 - Device Ports • 3 - ISL Ports • 4 - 10GE Ports • 5 - FCIP Tunnels • 6 - EE Monitors Selected member identifiers are stored in CUSTOM_FAVORITES_OBJECT_LIST table if this favorite is not default.	int	
PLOT_EVENTS	Indicates whether the PM historical chart should overlay the events on the graph. 0 - No, 1 - Yes.	smallint	

TABLE 137 FCIP_CIRCUIT_PORT_MAP

Field	Definition	Format	Size
CIRCUIT_ID		int	
SWITCH_PORT_ID	SWITCH_PORT_ID of one end of the circuit	int	

TABLE 138 FCIP_PORT_TUNNEL_MAP

Field	Definition	Format	Size
SWITCHPORT_ID*	Switch Port ID.	int	
TUNNEL_ID*	FCIP Tunnel ID.	int	

TABLE 139 FCIP_TUNNEL

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
TUNNEL_ID	Tunnel ID for that GigE Port.	smallint	
VLAN_TAG	VLAN Tag on the tunnel (if present). Default value is -1.	int	
SOURCE_IP	Source IP on which the tunnel is created.	char	64
DEST_IP	Destination IP on the other end of tunnel.	char	64
LOCAL_WWN	Local port WWN for the tunnel.	char	23
REMOTE_WWN_RESTRICT	Remote Port WWN for the tunnel.	char	23
COMMUNICATION_RATE	Bandwidth specified for the tunnel.	double precision	
MIN_RETRANSMIT_TIME	FCIP Tunnel Parameter.	int	
SELECTIVE_ACK_ENABLED	FCIP Tunnel Parameter.	smallint	
KEEP_ALIVE_TIMEOUT	FCIP Tunnel Parameter.	int	
MAX_RETRANSMISSION	FCIP Tunnel Parameter.	int	
WAN_TOV_ENABLED	Is WAN TOV enabled. Default value is 0.	smallint	
TUNNEL_STATUS	Tunnel Status (Active/Inactive).	int	
DESCRIPTION	Description for the created tunnel.	varchar	64
FICON_TRB_ID_ENABLED	Whether Ficon_Tape_Read_Block is enabled on that tunnel. Default value is 0.	smallint	
FICON_TT_EMUL_ENABLED	Whether Ficon_Tin_Tir_Emulation is enabled on that tunnel. Default value is 0.	smallint	
FICON_DLA_EMUL_ENABLED	Whether Device_Level_Ack_Emulation is enabled on that tunnel. Default value is 0.	smallint	
FICON_TAPE_WRITE_MAX_PIPE	The Value for FICON_TAPE_WRITE_MAX_PIPE on the tunnel. Default value is -1.	int	
FICON_TAPE_READ_MAX_PIPE	The Value for FICON_TAPE_READ_MAX_PIPE on the tunnel. Default value is -1.	int	
FICON_TAPE_WRITE_MAX_OPS	The Value for FICON_TAPE_WRITE_MAX_OPS on the tunnel. Default value is -1.	int	
FICON_TAPE_READ_MAX_OPS	The Value for FICON_TAPE_READ_MAX_OPS on the tunnel. Default value is -1.	int	
FICON_TAPE_WRITE_TIMER	The Value for FICON_TAPE_WRITE_TIMER on the tunnel. Default value is -1.	int	

TABLE 139 FCIP_TUNNEL (Continued)

Field	Definition	Format	Size
FICON_TAPE_MAX_WRITE_CHAIN	The Value for FICON_TAPE_MAX_WRITE_CHAIN on the tunnel. Default value is -1.	int	
FICON_OXID_BASE	The Value for FICON_OXID_BASE on the tunnel. Default value is -1.	int	
FICON_XRC_EMULATION_ENABLED	Whether Xrc_Emulation is enabled on that tunnel. Default value is 0.	smallint	
FICON_TW_EMUL_ENABLED	Whether Ficon_Tape_Write_Emulation is enabled on that tunnel. Default value is 0.	smallint	
FICON_TR_EMUL_ENABLED	Whether Ficon_Tape_Read_Emulation is enabled on that tunnel. Default value is 0.	smallint	
FICON_DEBUG_FLAGS	FICON_DEBUG_FLAGS for that particular tunnel. Default value is -1.	double precision	
REMOTE_WWN	Configured WWN of the Remote Node.	char	64
CDC	CDC Flag. Default value is 0.	smallint	
ADMIN_STATUS	Admin Status of the Tunnel. Default value is 0.	smallint	
CONTROL_L2_COS	Class of service as defined by IEEE 802.1p for tunnel. Default value is -1.	int	
DSCP_CONTROL	DiffServe marking for control frame. Default value is -1.	int	
TRUNKING_ALGORITHM	Trunking Algorithm. Default value is -1.	int	
EXTENDED_TUNNEL	Indicates if the tunnel is an Extended Tunnel (i.e. new Tunnel type on the switch). Default value is 0.	smallint	
VIRTUAL_SWITCH_ID	Refers to the virtual switch to which the tunnel record belongs to.	int	
CIRCUIT_COUNT	The number of circuits configured on the tunnel. Default value is 1.	smallint	
MISMATCHED_CONFIG_DETAILS	Details of the reasons as to why the tunnel is down.	varchar	2048
LAST_UPDATE	Last update time tells the time when the last update to the database record happened.	bigint	
SLOT_NUMBER	SLOT_NUMBER on which the VE Port of the tunnel exists. Default value is 0.	int	
FICON_ENABLED	Is Ficon enabled. Default: 0, Values: 0|1. Default value is 0.	smallint	
TPERF_ENABLED	Is Tperf enabled. Default: 0, Values: 0|1. Default value is 0.	smallint	

TABLE 139 FCIP_TUNNEL (Continued)

Field	Definition	Format	Size
AUTH_KEY	This is the preshared-key to be used during IKE authentication.	varchar	128
CONNECTED_COUNT	Active connections count. Default value is 1.	smallint	
TUNNEL_STATUS_STRING	Tunnel Status string value from switch for the tunnel.	varchar	256
COMPRESSION_MODE	Compression mode value (0,1,2,3). Default value is 0.	smallint	
TURBO_WRITE_ENABLED	Whether turbo write (fast write) is enabled or not (0,1). Default value is 0.	smallint	
TAPE_ACCELERATION_ENABLED	Whether turbo write (fast write) is enabled or not (0,1). Default value is 0.	smallint	
IPSEC_ENABLED	Default value is 0.	smallint	
PRESHARED_KEY	The preshared key on tunnel.	char	32
QOS_HIGH	QoS high value.	smallint	
QOS_MEDIUM	QoS medium value.	smallint	
QOS_LOW	QoS low value.	smallint	
BACKWARD_COMPATIBLE	Whether the 10G tunnel is backward compatible with previous FOS versions.	smallint	
FICON_TERADATA_READ_ENABLED	Whether Ficon_Teradata_Read_Pipelining is enabled on that tunnel.	smallint	
FICON_TERADATA_WRITE_ENABLED	Whether Ficon_Teradata_Write_Pipelining is enabled on that tunnel.	smallint	

TABLE 140 FCIP_TUNNEL_CIRCUIT

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
TUNNEL_ID	Tunnel ID to which the circuit belongs to	int	
CIRCUIT_NUMBER	Circuit Number of the Circuit from the switch	smallint	
COMPRESSION_ ENABLED	Whether Compression is enabled on that circuit	smallint	
TURBO_WRITE_ ENABLED	Whether TurboWrite is enabled on that circuit'	smallint	
TAPE_ACCELERATION_ENABLED	Whether TapeAccelaration is enabled on that circuit	smallint	
IKE_POLICY_NUM	The IKE Policy on the circuit.The default value is -1.	int	

TABLE 140 FCIP_TUNNEL_CIRCUIT (Continued)

Field	Definition	Format	Size
IPSEC_POLICY_NUM	The IPSEC Policy on the circuit'. The default value is -1	int	
PRESHARED_KEY	The preshared Key on the circuit	char(	32
SOURCE_IP	SOURCE_IP of the circuit	varchar	64
DEST_IP	DESTINATION_IP of the circuit	varchar	64
VLAN_TAG	VLAN Tag of the circuit. The default value is -1	int	
SELECTIVE_ACK	Select acknowledgement flag.The default value is 0.	smallint	
QOS_MAPPING	QOS Mapping. The default value is 0.	smallint	
PATH_MTU_DISCOVERY	MTU Discovery Path. The default value is 0.	smallint	
MIN_COMM_RATE	Minimum communication Speed. The default value is 0.	int	
MAX_COMM_RATE	Maximum communication Speed. The default value is 0.	int	
MIN_RETRANSMIT_TIME	Minimum Retransmission Time. The default value is -1	int	
MAX_RETRANSMIT_TIME	Maximum retransmission time. The default value is -1	int	
KEEP_ALIVE_TIMEOUT	Keep Alive timeout. The default value is -1	int	
ADMIN_STATUS	Is admin status enabled. The default value is 0.	smallint	
METRIC	Circuit metric to set priority. The default value is -1	int	
DATA_L2_COS	Class of service as defined by IEEE 802.1p for circuit. The default value is -1.	int	
DSCP_DATA	DiffServe marking for Data Frame. The default value is -1	int	
MAX_RETRANSMISSIONS	Max number of Retransmission attempts on the circuit. The default value is 0.	int	
SLOT_NUMBER	Slot number of the circuit. The default value is 0.	smallint	
VE_PORT_NUMBER	VE port number of the tunnel to which the circuit belongs.	int	

TABLE 140 FCIP_TUNNEL_CIRCUIT (Continued)

Field	Definition	Format	Size
SECURITY_FLAG	Security Flag associated with the circuit. The default value is 0.	int	
DSCP_CONTROL	Diffserve marking for control frame. The default value is 0.	int	
CIRCUIT_STATUS	Status of the circuit. The default value is 0.	smallint	
ENABLED	Is circuit enabled. Default: 0, Values: 0|1. The default value is 0.	smallint	
MISMATCHED_CONFIGURATIONS	If a tunnel is down due to mismatched configurations on local and remote end, this property specifies the list of such mismatched configurations.	varchar	1024
CIRCUIT_STATUS_STRING	Circuit Status string value from switch for the tunnel	varchar	256
L2COS_F_CLASS	The default value is 0.	smallint	
L2_COS_HIGH	The default value is 0.	smallint	
L2_COS_MEDIUM	The default value is 0.	smallint	
L2_COS_LOW	The default value is 0.	smallint	
DSCP_F_CLASS	The default value is 0.	smallint	
DSCP_HIGH	The default value is 0.	smallint	
DSCP_MEDIUM	The default value is 0.	smallint	
DSCP_LOW	The default value is 0.	smallint	
FAILOVER_CIRCUIT	Whether the circuit is configured as failover or not.	smallint	
FAILOVER_GROUP_ID	Represents the failover group id for the circuit 0 - Default Failover Group. 1 - 9 Failover Group numbers for the circuits. -1 - Not supported. For the switches running less than FOS 7.2.	int	

TABLE 141 FCIP_TUNNEL_PERFORMANCE

Field	Definition	Format	Size
TUNNEL_ID	Primary key of the Switch Port	int	
SWITCH_ID	The number of octets or bytes that have been transmitted by this port. One second periodic polling of the port. This value is saved and compared with the next polled value to compute net throughput. Note, for Fibre Channel, ordered sets are not included in the count	int	
TX	'The number of octets or bytes that have been transmitted by this port. One second periodic polling of the port. This value is saved and compared with the next polled value to compute net throughput. Note, for Fibre Channel, ordered sets are not included in the count	double precision	
RX	The number of octets or bytes that have been received by this port. One second periodic polling of the port. This value is saved and compared with the next polled value to compute net throughput. Note, for Fibre Channel, ordered sets are not included in the count.	double precision	
TX_UTILIZATION	The computed value of TX based on speed of port	double precision	
RX_UTILIZATION	The computed value of RX based on speed of port	double precision	
DROPPED_PACKETS	Number of TCP packets dropped	double precision	
COMPRESSION	Compression ratio	bigint	
LATENCY	Round trip time (latency) in milliseconds	int	
LINK_RETRANSMITS	Number of segments retransmitted	double precision	
RTT_BY_TIME_OUT	Counter of retransmit packets due to timeout	double precision	
RTT_BY_DUP_ACK	Counter of retransmit packets due to duplicate acknowledgement'	double precision	
DUPLICATE_ACK	Counter of duplicate acknowledgement packets	double precision	
ROUND_TRIP_TIME	Round trip time in milliseconds	double precision	
TCP_OUT_OF_ORDER	Counter of TCP out-of-order.	double precision	
SLOW_START	Counter of slow starts	double precision	
LAST_UPDATE_TIME	'Time when this stats record was updated	timestamp	

TABLE 142 FCOE_DEVICE

Field	Definition	Format	Size
DEVICE_NODE_ID	The primary key of the DeviceNode.	int	
DIRECT_ATTACH	Indicates whether the fcoe device is directly attached to the switch"s TE port or to a cloud.	smallint	
ATTACH_ID	The primary key of the port (if direct attached) or cloud (if not direct attached).	int	
MAC_ADDRESS	Mac address of device.	varchar	64

TABLE 143 FCR_ROUTE

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
BB_FABRIC_ID	Backbone fabric DB ID.	int	
FCR_FABRIC_ID	FID assigned to edge fabric.	int	
SWITCH_WWN	WWN of the router switch.	varchar	128
NR_PORT_ID	Route parameter.	int	
FCRP_COST	Route parameter.	int	
EX_PORT_WWN	Ex_port WWN.	varchar	128

TABLE 144 FEATURE

Field	Definition	Format	Size
FEATURE_ID*	ID used to uniquely identify the feature.	int	6
NAME	Name of the feature.	varchar	256
DESCRIPTION	Description for the feature.	varchar	256

TABLE 145 FEATURE_EDITION_MAP

Field	Definition	Format	Size
FEATURE_ID*	ID used to uniquely identify the feature.	int	
EDITION_MASK	Used to associate a feature to the edition (Reserved for future).	int	

TABLE 146 FEATURES_USAGE

Field	Definition	Format	Size
CLIENT_IP	Identifies client IP.	varchar	128
USER_NAME	Identifies the feature used user name.	varchar	128
FEATURE_NAME	Identifies the unique feature(module) name.	varchar	128
SUB_FEATURE_NAME	Identifies the sub module name	varchar	128
OPERATION_NAME	Identifies the major operation or action happened in that feature.	varchar	128
LAST_UPDATED_TIME	Identifies the last updated time stamp.	timestamp	

TABLE 146 FEATURES_USAGE (Continued)

Field	Definition	Format	Size
USAGE_COUNT	Count shows how many times the feature is accessed.	int	
FIRST_UPDATED_TIME	Identifies the first updated time stamp.	timestamp	

TABLE 147 FICON_DEVICE_PORT

Field	Definition	Format	Size
DEVICE_PORT_ID*	Value for the device port to which these FICON properties are applied.	int	
TYPE_NUMBER		varchar	16
MODEL_NUMBER	Ficon device model number, such as S18.	varchar	64
MANUFACTURER	Manufacturer of the device, typically IBM.	varchar	64
MANUFACTURER_PLANT	Plant number where the device is manufactured.	varchar	64
SEQUENCE_NUMBER	Device sequence number.	varchar	32
TAG	FICON device property, e.g., 809a or 809b.	varchar	16
FLAG	FICON device property, e.g., 0x10 (hex).	varchar	8
PARAMS	FICON device property string, e.g., Valid channel port.	varchar	16

TABLE 148 FIRMWARE_FILE_DETAIL

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
FIRMWARE_NAME	Name of the firmware file.	varchar	64
MAJOR_VERSION	Major version bit from the firmware version.	smallint	
MINOR_VERSION	Minor version bit from the firmware version.	smallint	
MAINTENANCE	Maintenance bit from the firmware version.	smallint	
PATCH	Patch bit from the firmware version.	varchar	64
PHASE	Phase bit from the firmware version.	varchar	64
RELEASE_DATE	Release date of the firmware file.	timestamp	
IMPORTED_DATE	Imported date of the file to the Management application.	timestamp	
FIRMWARE_FILE_SIZE	Firmware file size.	int	
FIRMWARE_LOCATION	Firmware file location in the Management application repository.	varchar	1024
RELEASE_NOTES_ LOCATION	Release notes file location in theManagement application repository.	varchar	1024
FIRMWARE_REPOSITORY_ TYPE	Repository type to identify the FTP server: 0 = internal FTP. 1 = external FTP.	smallint	

TABLE 149 FIRMWARE_SWITCH_DETAIL

Field	Definition	Format	Size
FIRMWARE_ID*	ID for the firmware file.	int	
SWITCH_TYPE*	Switch type that supports this firmware file.	smallint	
REBOOT_REQUIRED	Reboot required flag for the switch type.	smallint	
NUMFILES	Number of files in the firmware.	int	

TABLE 150 FOUNDRY_DEVICE

Field	Definition	Format	Size
DEVICE_ID	Database ID of the DEVICE instance.	int	
IMAGE_VERSION	Firmware image version currently running in the device.	varchar	128
PRODUCT_TYPE	Product type of the device computed based on sysoid and version of main board. To get the main board version for devices, refer octet 28 of snChasMainBrdId MIB in foundry.mib.	varchar	32
FEATURE_MASK	A bit string representing the software features available in the switch/router. Each bit represent a feature and if the feature available then bit value would be 1 and 0 otherwise. Refer snAgSoftwareFeature MIB in foundry.MIB for various features supported and its corresponding details.	bytea	
IS_PORT_VLAN_ENABLED	'Port VLANs enabled for the product or not.	num	(1,0)
ARCHITECTURE_TYPE	Chassis architecture type. Refer snChasArchitectureType MIB in foundry.mib for possible values.	num	(2,0)
BUILD_LABEL	The image label of the built software.	varchar	64
SSL_SLOT	Slot number of the SSL module.	num	(4,0)

TABLE 151 FOUNDRY_MODULE

Field	Definition	Format	Size
MODULE_ID	Unique generated database identifier.	int	
SERIAL_NUM	Serial number of this module.	varchar	32
DRAM_SIZE	Dynamic RAM size in Kilo bytes. Currently it is not populated and used.	num	(4,0)
BOOT_FLASH_SIZE	Boot flash size in Kilo bytes. Currently it is not populated and used.	num	(4,0)
MODULE_TYPE	Type of this module. Refer snAgentBrdMainBrdId in foundry.mib for more details and possible values.	num	(4,0)
CODE_FLASH_SIZE	Code flash size in Kilo bytes. Currently it is not populated and used.	num	(4,0)

TABLE 151 FOUNDRY_MODULE (Continued)

Field	Definition	Format	Size
EXPANSION_MODULE_TYPE	Expansion board type. Refer snAgentBrdExpBrdId in foundry.mib for more details and possible values.	num	(4,0)
EXPANSION_MODULE_DESCRIPTION	The expansion board description string. Expansion board are those boards attaching on the main board.	varchar	128

TABLE 152 FOUNDRY_PHYSICAL_DEVICE

Field	Definition	Format	Size
PHYSICAL_DEVICE_ID	Unique generated identifier.	int	
SERIAL_NUMBER	The serial number of the chassis.	varchar	32
PRODUCT_TYPE	Product type based on sysoid or architecture type and management module main board id.	varchar	32

TABLE 153 FOUNDRY_PHYSICAL_PORT

Field	Definition	Format	Size
PHYSICAL_PORT_ID	Database ID of PHYSICAL_PORT instance.	int	
CONNECTOR_TYPE	The type of connector that the port offers. Refer snSwPortInfoConnectorType of foundry.mib for more details and possible values.	smallint	
MEDIA_TYPE	The media type for the port. Refer snSwPortInfoMediaType of foundry.mib for more details and possible values.	smallint	
GIG_TYPE		smallint	

TABLE 154 FPORT_TRUNK_GROUP

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
VIRTUAL_SWITCH_ID	Virtual switch ID where this F_Port Trunk Group is defined.	int	
MASTER_USER_PORT	User port number for the master port of this trunk.	smallint	
WWN	WWN of the trunk group.	char	23
TRUNK_AREA	User-assigned area number used to group together F_ports of the trunk.	smallint	

TABLE 155 FPORT_TRUNK_MEMBER

Field	Definition	Format	Size
GROUP_ID*	Foreign key to the PORT_TRUNK_GROUP table.	int	
PORT_NUMBER*	Member user port number.	smallint	
WWN	Member port WWN.	char	23

TABLE 156 FRU

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
CORE_SWITCH_ID		int	
TAG	provides the TAG number of FRU element, requested by SMIA and values filled in by Switch Asset Collector. Field probably contains information such as asset tag or serial number data. This value varies depending on the type of physical package	varchar	64
PART_NUMBER	provides the part number of the FRU element, requested by SMIA and values filled in by Switch Asset Collector. Field probably contains the part number assigned by the organization responsible for producing or manufacturing the physical element	varchar	64
SERIAL_NUMBER	provides the serial number of the FRU element, requested by SMIA and values filled in by Switch Asset Collector	varchar	64
VENDOR_PART_ NUMBER	provides the Vendor-assigned part number of this package, requested by SMIA and values filled in by Switch Asset Collector	varchar	64
VENDOR_SERIAL_ NUMBER	provides the Vendor-assigned serial number of this package, requested by SMIA and values filled in by Switch Asset Collector'	varchar	64
CAN_BE_FRUED	provides whether this element can be removed from the switch, requested by SMIA and values filled in by Switch Asset Collector. Maps to IsRemovable field in the html. The default value is -1.	int	
SLOT_NUMBER	provides the slot number of this FRU element , requested by SMIA and values filled in by Switch Asset Collector.The default value is -1.	int	
MANUFACTURER_DATE	provides the manufactured date of this FRU element, requested by SMIA and values filled in by Switch Asset Collector	timestamp	
UPDATE_DATE	provides the updated date of this FRU element, requested by SMIA and values filled in by Switch Asset Collector	timestamp	
VERSION		varchar	32
MANUFACTURER	provides the manufacturer of this FRU element ,requested by SMIA and values filled in by Switch Asset Collector	varchar	64
VENDOR_EQUIPMENT_T YPE	provides the vendor equipment type of the FRU element, requested by SMIA and values filled in by Switch Asset Collector	varchar	32
OPERATIONAL_STATUS	provides the operational status of the FRU element, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above. The default value is -1.	int	

TABLE 156 FRU (Continued)

Field	Definition	Format	Size
TOTAL_OUTPUT_POWER	provides the total power output of the power supply FRU element, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above. this field is applicable only for the power supply FRU element. The default value is -1.	bigint	
SPEED	provides the speed of the FAN FRU element, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above. this field is applicable only for the FAN FRU element. The default value is -1.	int	
CREATION_TIME	provides the record creation time, standard columns for Management application and values filled in by Switch Asset Collector	timestamp	
LAST_UPDATE_TIME	provides the record creation time, standard columns for Management application and values filled in by Switch Asset Collector	timestamp	
PREVIOUS_OP_STATUS	provides the previous operational status of FRU element, requested by SMIA and values filled in by Switch Asset Collector. Helps identify the operational status transitions. The default value is -1.	int	
VENDOR	This holds the vendor name information for FRU	varchar	256

TABLE 157 FTP_SERVER

Field	Definition	Format	Size
ID*		int	
TYPE	Type indicates the what type of file. Internal FTP - 0, External FTP - 1, External SCP - 2, Internal SCP/SFTP - 3, External SFTP - 4 and Technical support FTP - 100. Technical Support FTP server configuration is created by user to transfer the technical support files from the Management application repository to specified FTP server. Other server configurations can be seen in Options dialog.	smallint	
IP	FTP server IP address.	varchar	64
USER_NAME	FTP server user name.	varchar	64
PASSWORD	FTP server user password.	varchar	512
ROOT_DIRECTORY	FTP server root directory location.	varchar	1024
PORT	Port on which FTP server is configured.	int	

TABLE 158 GENERATED_REPORT

Field	Definition	Format	Size
ID*		int	
NAME	Report name.	varchar	256
TYPE_ID	Report type.	int	

TABLE 158 GENERATED_REPORT (Continued)

Field	Definition	Format	Size
EFCM_USER	Management application user who has generated this report.	varchar	128
REPORT_OBJECT	Report object BLOB.	bytea	
TIMESTAMP_	Timestamp when the report is generated.	timestamp	
FABRIC_NAME	Fabric Name.	varchar	256

TABLE 159 GIGE_PORT

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
SWITCH_PORT_ID	ID for the GigE Port in SWITCH_PORT.	int	
PORT_NUMBER	GigE Port Number(0 for ge0 and 1 for ge1).	int	
SLOT_NUMBER	Slot number on which the GigE Port is present.	int	
ENABLED	Enabled or disabled. Default value is 0.	smallint	
SPEED	Port speed details. Default value is 0.	bigint	
MAX_SPEED	Port maximum speed supported.	bigint	
MAC_ADDRESS	MAC Address of that port.	varchar	64
PORT_NAME	GigE Port Name.	varchar	64
OPERATIONAL_STATUS	LED status.	int	
LED_STATE	LED status.	smallint	
SPEED_LED_STATE	GigE Port type details.	smallint	
PORT_TYPE	Port type for the GigE Port.	varchar	64
PERSISTENTLY_DISABLED	Whether the GigE Port is persistently disabled.	smallint	
INTERFACE_TYPE		smallint	
CHECKSUM		varchar	16
FCIP_CAPABLE	1 = FCIP capable; otherwise, 0. Default value is 2.	smallint	
ISCSI_CAPABLE	1 = ISCSI capable; otherwise, 0. Default value is 2.	smallint	
REMOTE_MAC_ADDRESS	MAC address of attached port of the 10G GigE Port.	varchar	64
INBAND_MANAGEMENT_STATUS	1 = Inband Management status is enabled; otherwise, 0. Default value is 0.	smallint	
OCCUPIED	Default value is 0.	smallint	
LAST_UPDATE		bigint	

TABLE 160 GIGE_PORT_ETHERNET_CLOUD_LINK

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
CLOUD_ID		int	
SWITCH_PORT_ID	The unique id of the switch TE port that this member connects to.	int	
TRUSTED		smallint	
CREATION_TIME		timestamp	
MISSING		smallint	
MISSING_TIME		timestamp	

TABLE 161 GIGE_PORT_STATS

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
SWITCH_ID	References the ID in CORE_SWITCH table.	int	
PORT_ID	References the ID in SWITCH_PORT table.	int	
CREATION_TIME	The polling time.	timestamp	
TX	Transmit (TX) value in bytes.	double precision	
RX	Receive (RX) value in bytes.	double precision	
TX_UTILIZATION	Transmit utilization (TX%) value in percentage.	double precision	
RX_UTILIZATION	Receive utilization (RX%) value in percentage.	double precision	
DROPPED_PACKETS	Number of dropped packets.	double precision	
COMPRESSION	The compression value.	double precision	
LATENCY	The latency value.	double precision	
BANDWIDTH	The bandwidth value.	double precision	

TABLE 162 GLOBAL_VLAN

Field	Definition	Format	Size
GLOBAL_VLAN_DB_ID	Unique database generated identifier.	int	
NAME	Name for Global VLAN.	varchar	255
CONTEXT_DEVICE_ID	Database ID of the DEVICE instance which is associated with global VLAN.	int	

TABLE 163 GRE_TUNNEL_INTERFACE

Field	Definition	Format	Size
INTERFACE_ID	This column is used to store the id of the interface. The value will be populated by the discovery engine where the corresponding GRE Tunnel Interface details will be persisted in the INTERFACE table.	int	

TABLE 164 HA_CLUSTER

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
NAME	User-supplied name for the HA Cluster.	varchar	64
ENCRYPTION_GROUP_ID	Foreign key reference to the ENCRYPTION_GROUP that contains this HA Cluster.	int	
MEMBER_LIST	A comma-separated list of Encryption Engines in the HA Cluster. Each engine is identified by a switch node WWN, followed by "/", followed by the slot number. The slot number is 0 if the switch does not have removable blades.	varchar	256

TABLE 165 HBA

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
HOST_ID	ID of the Device Enclosure (Host) to which this HBA belongs to.	int	
NAME	User defined name of the HBA	varchar	128
POWER_MODE	Power mode of the HBA	varchar	256
MODEL	Model code of the HBA	varchar	256
MODEL_DESCRIPTION	Model description for the HBA	varchar	256
OPERATING_STATUS	Current operating status of the HBA: 1: Enabled/0: Disabled. The default value is 0.	smallint	
CHIP_REVISION	Revision level of the chip used in the HBA	varchar	64
HARDWARE_PATH	Hardware path for the HBA.	varchar	256
SERIAL_NUMBER	Serial number of the HBA	varchar	64
TEMPERATURE	Temperatur of HBA. Both in Celsius/Fahrenheit	varchar	16
USERNAME	User name to be used for logging into the HBA.	varchar	256
PASSWORD	Password used for logging into the HBA	varchar	256
MANAGEMENT_STATE	Management state bit mask, Managed/Auth failed etc. The default value is -1.	int	
MANAGEMENT_INTERFACE	Management interface bit mask, JSON/WMI/SMI etc . The default value is -1.	int	
DRIVER_VERSION	The version level of the host adapter driver	varchar	256
DRIVER_NAME	The name of the HBA driver	varchar	256
FIRMWARE_VERSION	The version level of the firmware	varchar	256

TABLE 165 HBA (Continued)

Field	Definition	Format	Size
BIOS_VERSION	The version level of the BIOS	varchar	256
PCI_REG_VENDOR_ID	The identifier of the PCI Register"s vendor	varchar	32
PCI_REG_DEVICE_ID	The device ID of the PCI Register	varchar	32
PCI_REG_SUBSYSTEM_ID	The ID of the PCI subsystem	varchar	32
PCI_REG_SUBSYS_VENDOR_ID	The ID of the PCI subsystem vendor.	varchar	32
PCI_REG_LANE_COUNT	The number of PCI lanes, in Gbps, each way between the PCI slot and the adapter. The default value is 8.	int	
PCI_REG_NEG_LANE_COUNT	The set number of PCI lanes that were initially negotiated. The default value is 8.	int	
PCI_REG_GENERATION	PCI generation	varchar	256
TRUSTED	Denotes whether HBA is trusted by user or not. When the host first time discovered, all the HBAs will be trusted by default. If any HBA added later, then it will be in untrusted stated. 0 denotes untrusted and 1 is for trusted.	smallint	
CREATION_TIME	HBA record creation time. This tells us when this HBA was first discovered.	timestamp	
MISSING	Denotes whether HBA is missing or not. 0 denotes present and 1 states that HBA is missing from host.	smallint	
MISSING_TIME	States the missing time of the HBA. This will be null if the HBA is available.	timestamp	
CIM_NAMESPACE	Reflects the CIM namespace used to discover the HBA	varchar	128
CARD_TYPE	FC for HBA, CNA for CNA. The default value is ‘FC’.	varchar	32
WWN	WWN of the adapter	varchar	23
HCM_AGENT_VERSION	Version of HCM agent used to managed the HBA	varchar	128
MAC_ADDRESS	Adapter mac address	varchar	64
MAX_SPEED_SUPPORTED	The maximum port speed that is supported on the port, in Gb/s. The default value is 0.	int	
VPD_PRODUCT_DESCRIPTION	Description of the product	varchar	256
VPD_PART_NUMBER	Part Number of the device	varchar	32
VPD_EC_LEVEL	EC Level of the device	varchar	32
VPD_FRU_NUMBER	FRU number of the device	varchar	256
VPD_SERIAL_NUMBER	serial number of the device	varchar	32

TABLE 165 HBA (Continued)

Field	Definition	Format	Size
VPD_PW	PW details of the device	varchar	32
VPD_EDC	EDC details of the device	varchar	32
VPD_MDC	MDC details of the device	varchar	32
VPD_FABRIC_GEOGRAPHY	FABRIC_GEOGRAPHY of the device	varchar	256
VPD_LOCATION	LOCATION of the device	varchar	256
VPD_MANUFACTURER_ID	MANUFACTURER_ID of the device	varchar	256
VPD_PCI_GEOGRAPHY	PCI_GEOGRAPHY of the device	varchar	256
VPD_VENDOR_DATA	VENDOR_DATA of the device	varchar	256
VPD_EXT_CAPABILITY	EXT_CAPABILITY of the device	varchar	256
VPD_OEM	OEM details of the device	varchar	256
VPD_OEM_INFO	OEM related information of the device	varchar	256
MAX_PCIF	Maximum number of Pci functions.	smallint	
CARD_MODE	The mode that the card is operating on.	smallint	
DRIVER_CARD_MODE	It is the same as card type but uses new values applicable for 3.0 and later driver versions. Deprecates the card type field. Possible values are: • HBA/CNA/AnyIO/Mezzanine • HBA/Mezzanine CNA/Mezzanine AnyIO	varchar	32
VENDOR	Adapter vendor name.	varchar	128

TABLE 166 HBA_NODE_MAP

Field	Definition	Format	Size
DEVICE_NODE_ID	Primary key from the Device Node table	int	
HBA_ID	Primary key from the HBA table	int	

TABLE 167 HBA_PORT

Field	Definition	Format	Size
DEVICE_PORT_ID	Primary key on the owner Device port table	int	
CONFIGURED_STATE	Indicates whether the port is enabled or disabled. The default value is 0.	smallint	
CONFIGURED_SPEED	The configured speed of the port. E.g. Auto-negotiate	varchar	64
CONFIGURED_TOPOLOGY	The topology setting. The default value is 1.	int	
MAX_SPEED_SUPPORTED	The maximum port speed that is supported on the port, in Gb/s. The default value is 0.	int	
OPERATING_STATE	Indicates whether the link is online or offline. The default value is 0.	smallint	

TABLE 167 HBA_PORT (Continued)

Field	Definition	Format	Size
OPERATING_TOPOLOGY	The topology setting at which the port is operating. The default value is 1.	int	
SUPPORTED_FC4_TYPES	List of supported FC4 types for this port.	varchar	32
SUPPORTED_COS	Supported Class of Service (COS) for this port.	varchar	32
TRUSTED	Denotes whether port is trusted or not. 0 denotes untrusted and 1 is for trusted.	smallint	
CREATION_TIME	HBA port record creation time. This tells us when this HBA port was first discovered.	timestamp	
MISSING	Denotes whether port is missing or not. 0 denotes present and 1 states that port is missing from fabric.	smallint	
MISSING_TIME	States the missing time of the this port.	timestamp	
OPERATING_SPEED	Operating speed of the hba port. The default value is 0.	varchar	64
CNA_PORT_ID	Nullable foreign key, related FC pot with the CNA port	int	
PORT_NWWN	Node WWN for the HBA port	varchar	23
PHYSICAL_PORT_WWN	Physical Ports WWN in case of V port	varchar	128
SWITCH_IP	IP of the switch, HBA port is connected to	varchar	23
PRINCIPAL_SWITCH_WWN	WWN of the principal switch of the fabric, HBA is connected to	varchar	128
HBA_ID	HBA ID of the HBA this port belongs to	int	
PORT_NUMBER	Port number of this HBA port.	smallint	
NAME	Name defined for the HBA port in HCM	varchar	
FACTORY_PORT_WWN	Factory configured Port WWN defined for the HBA port in HCM	varchar	
FACTORY_NODE_WWN	Factory configured Node WWN defined for the HBA port in HCM	varchar	
PREBOOT_CREATED	Flag to identify vports created during preboot	varchar	
MAX_BANDWIDTH	Maximum bandwidth	varchar	64
PCIF_INDEX	Pci function index	varchar	64
MAX_PCIF	Maximum number of Pci functions.	smallint	
SYNTHETIC_FC	Synthetic FC is applicable for Windows only: • 0 - Unknow • 1 - Yes • 2 - No.	int	

TABLE 168 HBA_PORT_DETAIL

Field	Definition	Format	Size
DEVICE_PORT_ID	Device port id acts as the primary key	int	
PERSISTENT_BINDING	Persistent binding value of the port. With persistent binding (on the host), one can bind a LUN to a specific device file, thus making sure devices reappear on the same device files after reboots. 0 – disable 1 – enabled	smallint	
FABRIC_NAME	Principal switch WWN of the Fabric to which the port is associated with.	varchar	64
BOOT_OVER_SAN	Flag to indicate whether boot over SAN is enabled or not.. The default value is 0.	smallint	
BOOT_OPTION	Boot option for the port. Possible values are 0 - AUTO_DISCOVERED_FROM_FABRIC , 1 - FIRST_VISIBLE_LUN, 2 - USER_CONFIGURED_LUN	smallint	
BOOT_SPEED	Boot speed for the port in Gbps. Possible values are 0 - AUTO_NEGOTIATE and 2, 4, 8, 16 Gbps. The default value is 0.	int	
BOOT_TOPOLOGY	Boot topology for the port. Possible values are 0 - Point to Point , 1 - Loop. The default value is 1.	int	
BOOTUP_DELAY	On starting system how long system needs to wait for user action. Configured value ranges 0,1,2,5 and 10 minutes. Default value is 0.	int	
BB_CREDIT	The maximum number of receive buffer. The default value is 8.	int	
FRAME_DATA_FIELD_SIZE	The default value is 512.	int	
HARDWARE_PATH	Indicates whether MPIO is enabled or disabled		
V_PORT_COUNT	Number of logical ports. The default value is 0.	int	
QUEUE_DEPTH	The number of I/O operations that can be run in parallel on a device. The default value is 0.	int	
INTERRUPT_CONTROL_COALESCE	Indicates whether interrupt control is on or off. The default value is 0.	smallint	
INTERRUPT_CONTROL_LATENCY	Sets the interrupt control latency value.. The default value is 0.	int	
INTERRUPT_CONTROL_DELAY	Sets the interrupt control delay value.. The default value is 0.	int	
BEACON_STATE	Indicates whether beaconing is on or off.. The default value is 0.	smallint	
LINK_BEACON_STATE	Indicates whether link beaconing is on or off.. The default value is 0.	smallint	

TABLE 168 HBA_PORT_DETAIL (Continued)

Field	Definition	Format	Size
MPIO_MODE_STATE	Indicates whether multipathing mode is on or off.. The default value is 0.	smallint	
PATH_TIME_OUT	The value between 0 to 60 that specifies the time out session. Note you can only enable or edit the path time out when MPIO is disabled. The default value is 0.	int	
LOGGING_LEVEL	The port logging level. Values include Log Critical, Log Error, Log Warning, and Log Info. The default value is 0.	smallint	
TARGET_RATE_LIMIT	Target rate limit of the port. Possible values are 0 -disabled, 1 - enabled. The default value is 0.	smallint	
DEFAULT_RATE_LIMIT	Default target rate limit of the port speed (1 Gbps). The default value is 0.	int	
VF_MODE	True if the port is in VF (Virtual Fabric) mode.	smallint	
RECIEVE_BUFFER_CREDIT	Receiving buffer-to-buffer credits (BB_credits) for the port.	varchar	64
TRANSMIT_BUFFER_CREDIT	Transmitting buffer-to-buffer credits (BB_credits) for the port.	varchar	64
FCSP_AUTH_STATE	Indicates whether FC-SP authentication is on or off. The default value is 0.	smallint	
FCSP_STATUS	The status of FC-SP authentication. The default value is 'Disabled'.	varchar	32
FCSP_ALGORITHM	The configured authentication algorithm. The default value is 'MD5'.	varchar	64
FCSP_GROUP	The DH Group (DH Null, group 0 is the only option). The default value is 0.	smallint	
FCSP_ERROR_STATUS	The health status of the Fibre Channel Security Protocol parameters	varchar	256
QOS_CONFIGURED_STATE	Indicates whether QoS is enabled or disabled. The default value is 0.	smallint	
QOS_OPERATING_STATE	QOS Operating state. The default value is 'Disabled'.	varchar	256
QOS_TOTAL_BB_CREDIT	The number of receive buffers. The default value is 2.	varchar	16
QOS_PRIORITY_LEVEL	QoS priority levels. Values include High, Medium, and Low	varchar	32
QOS_HIGH_BW_ALLOCATION	Percentage of bandwidth allocation for the High priority level.	varchar	32
QOS_MEDIUM_BW_ALLOCATION	Percentage of bandwidth allocation for the Medium priority level	varchar	32
QOS_LOW_BW_ALLOCATION	Percentage of bandwidth allocation for the Low priority level.	varchar	32

TABLE 168 HBA_PORT_DETAIL (Continued)

Field	Definition	Format	Size
MEDIA	media of port	varchar	64
IOC_ID	IO controller ID	int	
PREBOOT_DISABLED	Boolean value indicating if port was disabled during preboot.. The default value is 0.	smallint	
ALARM_WARNING	A bit mask indicating degrading SFP if the bit mask has any 1s in it. It bit mask is all 0s then SFP is in good state.	varchar	32
IO_EXEC_THROTTLE_MAX	Maximum value is 2000. This feature is available for driver 3.1 and later.	int	
IO_EXEC_THROTTLE_OPERATIONAL	Operation value ranges from 0 - 2000.	int	
IO_EXEC_THROTTLE_CONFIGURED	Configured value ranges from 0 - 2000.	int	
FEC_STATE	State of FEC. The FEC (Forward Error Correction) is an error recovery mechanism that allows the receiver of the corrupted frame to correct the error without referring back to the port which transmitted the frame. Supported on prowler card in FC mode. Applicable values are Online, Offline and Not Supported. Note : Not Supported on (PORT_MEDIA_MEZZANINE_CARD).	varchar	128
BB_CREDIT_RECOVERY_STATUS	Status of Buffer to Buffer Credit Recovery. Supported on FC ports. Applicable values are Online, Offline, Not Applicable, and Disable.	varchar	32
CONFIGURED_BB_SCN_COUNT	Configured value of Buffer to Buffer Credit Recovery state change notification count. Range between 1 to 15.	int	
NEGOTIATED_BB_SCN_COUNT	Buffer to Buffer Credit Recovery state change notification count value set by bcu. Range between 1 to 15.	int	

TABLE 169 HBA_PORT_DEVICE_PORT_MAP

Field	Definition	Format	Size
DEVICE_PORT_ID	ID from the device_port table.	int	
HBA_PORT_ID	DEVICE_PORT_ID from the hba_port table.	int	

TABLE 170 HBA_PORT_FCOE_DETAILS

Field	Definition	Format	Size
DEVICE_PORT_ID		int	
BANDWIDTH	The bandwidth percentage of the FCoE port eg. 10 gb for CNA.	int	
FIP_STATE	FIP (Fibre channel Initialization Protocol) state of the port 0 – disable , 1- enabled.	varchar	64
DISCOVERY_PRIORITY	Discovery priority of the port. Currently not used.	varchar	256

TABLE 170 HBA_PORT_FCOE_DETAILS (Continued)

Field	Definition	Format	Size
FCF_FCMAP	FC Map value of port. Currently not used.	varchar	256
FCF_FPMA_MAC	FPMA (fabric-provided MAC address) MAC address of port. Currently not used.	varchar	64
FCF_MAC	FCF (FCoE Forwarder) MAC value of port.	varchar	64
FCF_MODE	FCF (FCoE Forwarder) Mode of the port. Currently not used.	varchar	256
FCF_NAMEID	FCF (FCoE Forwarder) Name of the port currently Not used.	varchar	256
FCPIM_MPIO_MODE	Indicates whether multipathing I/O (MPIO) mode is turned on or off. 1- on, 0 - off	smallint	
PORT_LOG_ENABLED	True if port log is enabled.	smallint	
MAX_FRAME_SIZE	The frame size, in bytes, of the FCoE port.	int	
MTU	Maximum transmission unit in bytes of the FCoE port. Default - 2112, 0 - auto	int	
PATH_TOV	The value between 0 and 60 that specifies the time-out session. **NOTE:** You can only enable or edit the path time out when MPIO is disabled	int	
SCSI_QUEUE_DEPTH	The LUN queue depth feature determines how many concurrent IOs the adapter will accept and process per LUN (not at the adapter port level, as with the IO throttle value). Not setting the queue depth to the optimal level can result in poor performance, where outstanding IO queuing can cause bottlenecks. For optimum performance, consider both the configuration settings of the HBA and the physical limits on the storage array. If you set the queue depth too low on the HBA it could lead to under-utilization of storage resources. **NOTE:** The Queue Depth feature is supported for all adapter classes configured in FC or FCoE mode (Windows operating systems only)'	int	
STATE	The state of the FCoE port (online or offline).	varchar	64
SUPPORTED_CLASS	The classes supported on the FCoE port. For example, Class2 and Class3.	varchar	256
TRL_SPEED	TRL (Target Rate limit) speed. This will be less than max speed supported by this port.	int	
TRL_STATE	TRL (Target Rate limit) state of the port. Possible values are 0 - disable , 1 - Enable	smallint	
PG_ID	The priority group ID. Possible values are 0-7 (user-definable) and 15.0-15.7 (strict priority).	varchar	32
PRIORITIES	'Lists the available priorities (High, Medium, Low).	varchar	128
FCOE_MAC	FCOE MAC address of the port.	varchar	64
IOC_ID	The IO controller Identifier.	int	

TABLE 171 HBA_REMOTE_PORT

Field	Definition	Format	Size
ID	Autogenerate primary column.	int	
SYMBOLIC_NAME	The symbolic name associated with the remote port.	varchar	256
PORT_WWN	The world wide name of the remote device"s port.	char	23
NODE_WWN	The world wide name of the remote device	char	23
NAME	The name associated with the device	varchar	256
FC_ADDRESS	FC Address for the port in hex	varchar	6
FRAME_DATA_SIZE	The frame size, in bytes, of the device. The default value is 512.	int	
SPEED	Operating speed of the remote port.	int	
STATE	Indicates whether the device is online or offline. The default value is ‘Offline’.	varchar	64
SUPPORTED_COS	The types of classes that are supported on the remote port; for example, Class-3	varchar	32
DEVICE_TYPE	The type of the device; for example, Disk or Tape.	varchar	64
BIND_TYPE	The persistent bind type. The default value is 0.	smallint	
TARGET_ID	The identifier of the target device. The default value is 0.	int	
ROLE	The role of the device (target or initiator)	varchar	64
VENDOR	The vendor of the device	varchar	256
PRODUCT_ID	The device"s identifier.	varchar	256
PRODUCT_VERSION	Field which stores information regarging target rate limiting on the remote port	varchar	256
QOS_PRIORITY	QOS Priority on the target. The default value is 'Unknown'.	varchar	64
QOS_FLOW_ID	QOS Flow ID on the target. The default value is 0.	varchar	64
CURRENT_SPEED	Current speed of the remote port, as enforced by TRL. The default value is 0.	varchar	64
TRL_ENFORCED	True if TRL(Target Rate limit) is enforced.	varchar	16
BUS_NO	Channel number in the PCI Bus. The default value is 0.	varchar	32
FCP_IM_STATE	Indicates whether the Fibre Channel Protocol Input Method (FCP-IM) is online or offline.	varchar	128
IO_LATENCY_MIN	Minimum IO Latency value (< 79) in milliseconds and is calculated when HBA port starts SCSI (FCP) exchanges	varchar	32
IO_LATENCY_MAX	IO Latency value in milliseconds and is calculated when HBA port starts SCSI (FCP) exchanges	varchar	32
IO_LATENCY_AVERAGE	Average IO Latency value in milliseconds and is calculated when HBA port starts SCSI (FCP) exchanges	varchar	32

TABLE 171 HBA_REMOTE_PORT (Continued)

Field	Definition	Format	Size
DATA_RETRANSMISSION_SUPPORT	Field to indicate whether the remote port supports data retransmission.0 would mean unsupported and nonzero value implies supported. The default value is 0.	smallint	
REC_SUPPORT	Field to indicate whether the remote port supports the REC ELS command Channel number in the PCI Bus.Zero would mean unsupported and nonzero value implies supported. The default value is 0.	smallint	
TASK_RENTRY_IDENT_SUPPORT	The number of PRLI responses from the target to the initiator and begins when HBA Port starts FCP exchanges.Zero would mean unsupported and nonzero value implies supported. The default value is 0.	int	
CONFIRMED_COMPLETIONS_SUPPORT	The number of confirmed completions on the remote port and begins when HBA Port starts FCP exchanges.Zero would mean unsupported and nonzero value implies supported. The default value is 0.	int	

TABLE 172 HBA_REMOTE_PORT_LUN

Field	Definition	Format	size
ID	Auto generated primary key	int	
HBA_REMOTE_PORT_ID	Primary key of owner row in Remote Port	int	
FCP_LUN	The logical unit number of Fibre Channel Protocol (FCP) device. The default value is 0.	varchar	16
CAPACITY	The capacity of the logical unit. The default value is 0.	int	
BLOCK_SIZE	The block size of the logical unit, in bytes (for example, 512 Bytes). The default value is 0.	int	
VENDOR	The vendor of the device to which the logical unit is assigned	varchar	256
PRODUCT_ID	The product identifier of the device to which the logical unit is assigned	varchar	256
PRODUCT_VERSION	The revision level of the device to which the logical unit is assigned.	varchar	256
PRODUCT_SERIAL_NO	The serial number of the device to which the logical unit is assigned	varchar	256
TARGET_WWN	The world wide name of the target devic	char	23
PHYSICAL_LUN	'If there is a lun connected to a remote port, then it represents a value 1 indicating it is a physical lun otherwise it is a dummy lun with value 0. The default value is 1.	smallint	
LUN_ID	IS lun id	varchar	32

TABLE 173 HBA_TARGET

Field	Definition	Format	size
DEVICE_PORT_ID	Primary key from the Device port table	int	
HBA_REMOTE_PORT_LUN_ID	Primary key from the HBA Remote port lun table	int	
BOOT_LUN	Flag to indicate of the LUN is bootable. The default value is -1.	smallint	
TRUSTED	Denotes whether target is trusted or not. 0 denotes untrusted and 1 is for trusted.	smallint	
CREATION_TIME	Creation time of the entry	timestamp	
MISSING	Flag to indicate if the remote LUN is missing. The default value is 0.	smallint	
MISSING_TIME	Time at which the LUN is marked missing.	timestamp	
TARGET_ID	The identifier of the target device as reported by each HBA port. The default value is 0.	int	

TABLE 174 HEALTH_STATUS

Field	Definition	Format	Size
ID		serial	
DEPLOYMENT_STATUS_ID	Identifies the execution cycle for the deployment.	int	
RULE_ID	Policy Monitor rule ID.	smallint	
RULE_DESCRIPTION	Description of what the check is about.	varchar	255

TABLE 175 HEALTH_TARGET_STATUS

Field	Definition	Format	Size
ID		serial	
HEALTH_STATUS_ID	Identifies the execution cycle for the deployment.	int	
TARGET_ID	In case of fabric, this is fabric DB ID; for switch, this is switch DB ID; for host, this is host db ID.	int	
TARGET_TYPE		smallint	
STATUS	0 - Failed 1 - Successful	smallint	
MESSAGE	Check result message.	varchar	16384
MESSAGE_TYPE		text	
LEGACY_NAME	Target legacy name.	varchar	256

TABLE 176 HOST_DISCOVERY_OPTION

Field	Definition	Format	Size
ID	Auto generated primary key	int	
DISCOVER_JSON	Flag to indicate JSON agent based discovery. The default value is 1.	smallint	

TABLE 176 HOST_DISCOVERY_OPTION (Continued)

Field	Definition	Format	Size
JSON_USERNAME	Username for the JSON agent	varchar	128
JSON_PASSWD	Password for the JSON agent	varchar	512
DISCOVER_CIM	Flag to indicate CIM based discovery. on/off. The default value is 0.	smallint	
CIM_IMPL	CIM implemenation used. 1: SMI, 2: WMI. The default value is 0.	smallint	
CIM_USERNAME	Username for the CIM based agent	varchar	128
CIM_PASSWORD	Password for the CIM based agent'	varchar	512
CIM_NAMESPACE	CIM Namespace. The default value is 'root/brocade	varchar	128
CIM_PORT	Port number used for the CIM agent. The default value is 5988.	int	
DISCOVER_VM	Flag to indicate VM discovery for a host. On/Off'. The default value is 0.	smallint	
VM_USERNAME	Username to be used for VM discovery	varchar	128
VM_PASSWORD	Password to be used for VM discovery	varchar	512
JSON_PORT	Port Number used for the Json agent. The default value is 34568.	int	
VM_PORT	Port Number used for the VM agent. The default value is 443.	int	
*Application_Name*_USER_NAME	Management application User Name of the user who generated the last operation on the request	varchar	255
*Application_Name*_SERVER_ADDRESS	Management application Server address which generated the last operation on this request	varchar	50

TABLE 177 HOST_DISCOVERY_REQ_GROUP

Field	Definition	Format	Size
ID	Auto generated primary key	int	
NAME	Unique name for the host request. The default value is ‘ New Host Group'.	varchar(	256
DISCOVERY_OPTIONS_ID	Primary key from the host discovery options table. Points to the associated discovery options	int	
MANAGEMENT_STATE	Reflects the status of the request E.g. 0-> Completed, 1->Delete Pending. The default value is 0.	int	

TABLE 178 HOST_DISCOVERY_REQUEST

Field	Definition	Format	Size
ID	Autogenerated primary key	int	
HOST_NAME	Hostname: IP address or host name	varchar	256

TABLE 178 HOST_DISCOVERY_REQUEST (Continued)

Field	Definition	Format	Size
DEVICE_ENCLOSURE_ID		int	
REQUEST_GROUP_ID	Primary key from the request group table. Null allowed	int	
HOST_DISCOVERY_OPTION_ID	This id is a foreign key to the id in the host_discovery_option table. The default value is -1.	int	
VM_MANAGEMENT_STATE	The status of VM Discovery indicating success or failure. The default value is 0.	int	
JSON_MANAGEMENT_STATE	The status of HBA discovery using JSON agent, indicating success or failure. The default value is 0.	int	
CIM_MANAGEMENT_STATE	The status of HBA Discovery using CIM, indicating success or failure. The default value is 0.	int	
MANAGEMENT_STATE	Reflects the status of the request E.g. 0-> Completed, 1->Add Pending 2->Delete Pending 3->Edit Pending 4->Delete Failed. The default value is 1.	int	
MANAGEMENT_STATE_DETAILS	This field holds the detailed information on the management state if available. For example, in case of management state 3, this field will have details on all the manually created conflicting enclosures.	varchar	1024

TABLE 179 HYPER_V_VIRTUAL_MACHINE

Field	Definition	Format	Size
ID	Primary Key	int	
VM_NAME	Name of the Virtual Machine.	varchar	256
COMPUTER_NAME	Hyper V host name.	varchar	256
CONFIGURATION_LOCATION	Path where VM configuration data is located.	varchar	256
GUID	Globally Unique ID of the VM.	varchar	256
HARD_DRIVES_COUNT	Count of virtual hard drives in the VM.	int	
MEMORY_ASSIGNED	Amount of memory assigned to the VM.	varchar	256
PATH	Path to the primary disk of the Virtual Machine.	varchar	256
PROCESSOR_COUNT	Number of virtual CPUs of the VM.	int	
STATUS	Status of the VM.	varchar	64
STATE	Operational State of the VM.	varchar	64
NOTES	Notes describing the VM.	varchar	2048
UPTIME	The time since the VM was last powered up.	varchar	512

TABLE 180 HYPER_V_VM_HBA_PORT_MAP

Field	Definition	Format	Size
ID	Primary Key	int	
HYPER_V_VM_ID	ID of the HYPER_VIRTUAL_MACHINE instance.	int	
HBA_PORT_ID	ID of the HBA_PORT instance which is a Hyper V Virtual FC port.	int	

TABLE 181 IFL

Field	Definition	Format	Size
ID*	Primary key for this table. Serial number which is uniquely generated by DB.	int	
EDGE_FABRIC_ID	Edge fabric ID of this IFL link.	int	
EDGE_PORT_WWN	Edge switch port wwn of this IFL link.	varchar	128
BB_FABRIC_ID	Backbone fabric ID of this IFL link.	int	
BB_PORT_WWN	Backbone fabric switch port wwn of this IFL link.	varchar	128
BB_RA_TOV	Backbone fabric resource allocation time out value specified in milliseconds.	int	
BB_ED_TOV	Backbone fabric Error detect time out value specified in milliseconds.	int	
BB_PID_FORMAT	Backbone fabric port identifier format.	smallint	

TABLE 182 INTERFACE

Field	Definition	Format	Size
INTERFACE_ID		int	
SWITCH_SERVICE_ID		int	
DEVICE_ID		int	
NAME		varchar	255
IDENTIFIER		varchar	255
TABLE_SUBTYPE		varchar	255
TAG_MODE		smallint	
VLAN_TAG_TYPE		int	
UNTAGGED_VLAN_ID	The existing Data type short has been modified to integer. Hence it supports 16 bit additionally.	int	
IF_NAME		varchar	64
LLDP_PORT_ID_SUBTYPE		smallint	
LLDP_PORT_ID		bytea	
IS_FDP_ENABLED		num	(1,0)
IS_CDP_ENABLED		num	(1,0)
PORT_STATUS		smallint	
PORT_STATE		smallint	

TABLE 182 INTERFACE (Continued)

Field	Definition	Format	Size
IF_INDEX	This column is used to store the ifIndex of the interface. The value will be populated by the DCB collector during the discovery of the DCB switch. Since this value is not populated by IP discovery engine, making the field as nullable.	int	
AMPP_PROFILE_MODE	Specifies whether the interface is set to AMPP profile mode.	smallint	
DOT1D_PORT_NUM	To store dot1d port number in DB to reduce SNMP calls to switch from IfIndexUtility	int	
EDGE_TYPE	The type of the device that is connected to the edge switch port. -1 : NA, 0 : connected to device with unknown type, 1 : connected to managed Brocade branded AP, 2 : connected to standalone Brocade branded AP.	int	
USER_DEFINED_VALUE_1	User defined value used for IP Port.	varchar	256
USER_DEFINED_VALUE_2	User defined value used for IP Port.	varchar	256
USER_DEFINED_VALUE_3	User defined value used for IP Port.	varchar	256

TABLE 183 INTERFACE_DEPLOYMENT_CONFIG

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
DEPLOYMENT_ID	Deployment configuration ID. Foreign Key for DEPLOYMENT table.	int	
CLEAR_CONFIGURATION	1/0 corresponding to "Clear Assignment" / "Assign Configuration" for interface level configuration.	smallint	
WRITE_TO_DEVICE	1/0 corresponding to Write to device/not write to device for outbound traffic.	smallint	
BINDING_DIRECTION	Represents the binding direction. 0/1 corresponds to IN / OUT direction.	smallint	

TABLE 184 IP_DEVICE_LICENSE

Field	Definition	Format	Size
ID	Primary Key field for the DEVICE_LICENSE	int	
DEVICE_ID	This is the foreign key reference to the Device table	int	
HASH	A unique hash for identifying a license entry in the device. This helps to traverse through the entries with same package name and LID.	varchar	24
PACKAGE_NAME	Name of the license package. Package defines the features enabled by the license. Example:SW-NI-CES-2024-L3U	varchar	64
LICENSE_ID	License ID of the chassis or the line module for which, this entry displays license information.Example: fJucJFgFHG	varchar	24

TABLE 184 IP_DEVICE_LICENSE (Continued)

Field	Definition	Format	Size
LICENSE_TYPE	The type of the license, which can be either normal or trial. Values are: permanent(1), trial(2).The default value is 1.	smallint	
EXPIRY_DATE	Expiry Date of the trial license. For normal license, the value is 0.	varchar	19
PRECEDENCE	Defines the priority of a particular trial license among those having the same package and License ID. This is primarily used for determining which license to use, when there are many trial and normal licenses with same package name and LID. The value range is (0..65535)	int	
LICENSE_STATE	This indicates the state of the license. Possible values:invalid(1),unused(2),active(3),expired(4)	smallint	

TABLE 185 IP_INTERFACE

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
ETHERNET_PORT_ID	GigE Port ID.	int	
IP_ADDRESS	IP address on the Ip_interface.	varchar	64
NET_MASK	Subnet mask for the interface.	varchar	64
MTU_SIZE	MTU Size for that interface.	int	
CHECKSUM	Check Sum.	varchar	64
GIGE_PORT_TYPE	Whether the IP interface is created on a 10G cross port or not. Non-zero value denotes a cross port.	smallint	

TABLE 186 IP_PORT_GROUP

Field	Definition	Format	Size
PORT_GROUP_ID	Unique database generated identifier.	int	
NAME	Name for Port group.	varchar	64
USER_ID	Database ID of the USER_ instance refer a user who created the group.	int	
DESCRIPTION	Description for Port group.	varchar	255
IS_PUBLIC	Represents if the port group is public or not. private-0, public-1.	num	(1,0)
IS_AP_GROUP	Represents if the group created using AP port(s) or not. Non-AP Port group-0, AP Port group-1.	num	(1,0)

TABLE 187 IP_ROUTE

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
ETHERNET_PORT_ID	GigE Port ID.	int	
PORT_NUMBER	Port Number related to the GigE Port.	int	
SLOT_NUMBER	Slot Number related to the GigE Port.	int	
NET_MASK	Subnet Mask for the Route.	varchar	64
GATEWAY	Gateway for the Route.	varchar	64
IP_ADDRESS	IP Address created after "”&”" operation of gateway.	varchar	64
METRIC	Metric.	int	
FLAG	Flag.	int	
CHECKSUM	Check Sum.	varchar	64
GIGE_PORT_TYPE	Whether the IP interface is created on a 10G cross port or not. Non-zero value denotes a cross port.	GIGE_PORT_TYPE	

TABLE 188 IP_SUBNET_VLAN

Field	Definition	Format	Size
VLAN_DB_ID	Database ID of the VLAN instance which is associated with the IP subnet.	int	
IP_ADDRESS	IP address for subnet.	varchar	40
SUBNET_MASK	Subnet Mask of the IP subnet.	varchar	40

TABLE 189 IPX_NETWORK_VLAN

Field	Definition	Format	Size
VLAN_DB_ID	Database ID of the VLAN instance which is associated with the IPX network.	int	
NETWORK_NUMBER	Number for IPX network.	varchar	32
FRAME_TYPE	Frame type for IPX. Possible values are 0-Not Applicable, 1-802.2, 2-802.3, 3-Ethernet II and 4-SNAP.	num	(4,0)

TABLE 190 ISL

Field	Definition	Format	Size
ID*	Primary key for the table.	int	
FABRIC_ID	Fabric ID of the associated fabric for this ISL.	int	
SOURCE_DOMAIN_ID	Source domain ID of the ISL.	int	
SOURCE_PORT_NUMBER	Source port number of the ISL.	smallint	
DEST_DOMAIN_ID	Destination or remote domain ID of the ISL.	int	
DEST_PORT_NUMBER	Destination or remote port number of the ISL.	smallint	
COST	The cost of the ISI link.	int	

TABLE 190 ISL (Continued)

Field	Definition	Format	Size
TYPE	The type of link.	smallint	
TRUSTED	Denotes whether ISL link is trusted or not. • 0 denotes untrusted • 1 denotes trusted.	smallint	
CREATION_TIME	Creation time of the ISL record in the Management application database.	timestamp	
MISSING	Denotes whether ISL link is missing or not. • 0 denotes present • 1 states that ISL is missing	smallint	
MISSING_TIME	States the missing time of the this ISL.	timestamp	
missing_reason	The ISL disabled reason. For an ISL either one or both ends might have been disabled. This field will capture the port disable message from both side of ISL. The data is formatted as follows: "<port_wwn>: <disabled_reason> ; <port_wwn>: <disabled_reason>".	varchar	1024
TRUNKED	Determines whether the isl is part of a trunk or not. The value of 0 means not trunked, 1 means this isl is part of a trunk and -1 means not applicable status. Default value is -1.	smallint	

TABLE 191 ISL_CONNECTION

Field	Definition	Format	Size
ID	The primary key of the table.	int	
FABRIC_ID	This is the fabric ID	int	
SOURCE_SWITCH_PORT_ID	The Switch port ID of the Source Switch (local end of the ISL). Maintained as a nullable foreign key to account for ports being moved from one VF to other.	int	
TARGET_SWITCH_PORT_ID	The Switch port ID of the Target Switch (remote end of the ISL). Maintained as a nullable foreign key to account for ports being moved from one VF to other.	int	
COST	Cost of the ISL link.	int	
TYPE	Type of the IS.	int	
TRUSTED	Denotes whether ISL link is trusted or not. 0 denotes untrusted and 1 is for trusted.	int	
MISSING	Denotes whether ISL link is missing or not. 0 denotes present and 1 states that ISL is missing.	int	
MISSING_TIME	Missing timestamp.	timestamp	
CREATION_TIME	Creation timestamp.	timestamp	
TRUNKED	This column is used to determine whether the isl is part of a trunk or not. The value of 0 means not trunked, 1 means this isl is part of a trunk and -1 means not applicable status. Default value is -1.	int	

TABLE 191 ISL_CONNECTION

Field	Definition	Format	Size
MASTER_CONNECTION_ID	This will hold the id of the master ISL connection for a ISL between trunk members. The ISL Connection between masters will have its own ID in this column. Non trunk ISLs will have the default value of -1.	int	
SOURCE_MASTER_PORT	This column will hold the trunk master port for the source port, if the connection is trunked. For the master connection it will have its source por"s port number. For non-trunk connections it will have the default value -1.	int	
TARGET_MASTER_PORT	This column will hold the trunk master port for the target port, if the connection is trunked. For the master connection it will have its target port"s port number. For non-trunk connections it will have the default value -1.	int	

TABLE 192 ISL_TRUNK_GROUP

Field	Definition	Format	Size
ID*	Primary key for the table.	int	
VIRTUAL_SWITCH_ID	Foreign key reference to Virtual Switch record associated with the trunk group.	int	
MASTER_USER_PORT	Stores the master user port for the ISL trunk..	smallint	
TRUSTED	Denotes whether ISL trunk group is trusted or not. 0 denotes untrusted and 1 is for trusted.	smallint	
MISSING	Denotes whether ISL trunk group is missing or not. 0 denotes present and 1 states that ISL trunk is missing	smallint	
MISSING_TIME	States the missing time of the this ISL trunk group. If the trunk is not missing then it will be null	timestamp	
MEMBER_TRACKING_STATUS	Member added/removed status of this trunk. This is represented as bitmap value. Each bit is set based on membership state change. Currently only 2 bits from LSB are used. Bit 1 - Member added Bit 2 - Member removed For example if the trunk group has membership change (some members are added and some existing members are removed) then the value would be 3.	int	

TABLE 193 ISL_TRUNK_MEMBER

Field	Definition	Format	Size
GROUP_ID*	Foreign key reference to the trunk group table for this member.	int	
PORT_NUMBER*	Member port number for this trunk..	smallint	
TRUSTED	Denotes whether ISL trunk member is trusted or not. 0 denotes untrusted and 1 is for trusted.	smallint	
MISSING	Denotes whether ISL trunk member is missing or not. 0 denotes present and 1 states that ISL trunk member is missing.	smallint	
MISSING_TIME	We could change this as "States the missing time of the this ISL trunk member. If the member is not missing then it will be null.	timestamp	

TABLE 194 KEY_VAULT

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
IP_ADDRESS	The IP Address (IPv4, IPv6, or hostname) of the key vault	varchar(	512
PORT_NUMBER	The TCP port number for the key vault	int	
PUBLIC_CERTIFICATE	The key vault''s public key certificate. Switches use this to establish a secure connection to the key vault	varchar(	4096
CERTIFICATE_LABEL	A text name to identify the certificate	varchar(	256
POSITION_	Specifies whether this key vault is the primary key vault or the backup key vault. 0 = primary, 1 = backup.	smallint	
VENDOR_NAME	Indicates the name of the key vault vendor. For non KMIP key vaults, this column will contain value as Not Applicable.	varchar	256

TABLE 195 L2_ACCESS_CONTROL_ENTRY

Field	Definition	Format	Size
ID		serial	
ACCESS_CONTROL_LIST_ID	L2 access control list ID, to which the ACL entry is associated.	int	
SEQUENCE_NUMBER		int	
ACTION	Specifies the action: 0 = Permit 1 = Deny	smallint	
SOURCE_MAC	Source MAC address.	varchar	24
SOURCE__MASK	Source MAC address mask.	varchar	24
DEST_MAC	Destination MAC address.	varchar	24
DEST_MASK	Destination MAC address mask.	varchar	24
VLAN_ID	Specifies the VLAN ID for the L2 ACL entry.	int	

TABLE 195 L2_ACCESS_CONTROL_ENTRY (Continued)

Field	Definition	Format	Size
ETHERNET_TYPE		varchar	24
LOG_ENABLE	Specifies whether logging is enabled or not: 1 = Enabled 0 = Not Enabled	smallint	
SOURCE_TYPE	Indicates the source MAC type (any, host or mac) for DCB Switch L2 ACL entry.	varchar	24
DEST_TYPE	Indicates the destination MAC type (any, host or mac) for DCB Switch L2 ACL entry.	varchar	24

TABLE 196 L2_ACCESS_CONTROL_LIST

Field	Definition	Format	Size
ID		serial	
ACCESS_CONTROL_LIST_TYPE	Specifies the ACL Type: • 0 = Standard • 1= Extended	smallint	
ACCESS_CONTROL_LIST_NUM	L2 ACL number.	int	
ACCESS_CONTROL_LIST_NAME	L2 ACL name.	varchar	255
STARTING_SEQUENCE_NUMBER		int	
INCREMENTAL_VALUE		int	
CLEAR_STATS	• 1 = Clear stats is enabled. • 0 = Clear stats is disabled.	smallint	
OPERATION_TYPE		varchar	10
DEPLOYMENT_ID	Deployment configuration ID. Foreign Key for DEPLOYMENT table.	int	
INT_BINDING_DIRECTION	Represents the interface binding direction. 0/1/2 corresponds to IN /OUT/BOTH direction.	smallint	

TABLE 197 L2_ACL_DEVICE_DEPLOY_MAP

Field	Definition	Format	Size
DEPLOYMENT_ID	Deployment configuration ID. Foreign Key for DEPLOYMENT table.	int	
L2_ACCESS_CONTROL_LIST_ID	L2 Access control List ID for reference to the L2_ACCESS_CONTROL_LIST. Foreign Key for L2_ACCESS_CONTROL_LIST table.	int	

TABLE 198 L2_ACL_INTERFACE_DEPLOY_MAP

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
DEPLOYMENT_ID	Deployment configuration ID. Foreign Key for DEPLOYMENT table.	int	

TABLE 198 L2_ACL_INTERFACE_DEPLOY_MAP (Continued)

Field	Definition	Format	Size
INBOUND_L2_ACL_ID	L2 Access control List ID of the L2 ACL selected for inbound. Foreign Key for L2_ACCESS_CONTROL_LIST table.	int	
INBOUND_WRITE_TO_DEVICE	1/0 corresponding to Write to device/not write to device for inbound traffic.	smallint	
OUTBOUND_L2_ACL_ID	L2 Access control List ID of the L2 ACL selected for outbound. Foreign Key for L2_ACCESS_CONTROL_LIST table.	int	
OUTBOUND_WRITE_TO_DEVICE	1/0 corresponding to Write to device/not write to device for outbound traffic.	smallint	

TABLE 199 L2_NEIGHBOR

Field	Definition	Format	Size
L2_NEIGHBOR_ID		int	
INTERFACE_ID		int	
RMT_IP_ADDRESS		varchar	40
RMT_IF_NAME		varchar	256
LAST_SEEN_TIME		int	
LLDP_REM_CHASSIS_ID_SUBTYPE		smallint	
LLDP_REM_CHASSIS_ID		bytea	
LLDP_REM_PORT_ID_SUBTYPE		smallint	
LLDP_REM_PORT_ID		bytea	
LLDP_REM_CHASSIS_ID_VALUE	To store the MAC or Network address value in ascii format	varchar	40
LLDP_REM_PORT_ID_VALUE	To store the MAC or Network address value in ascii format	varchar	40

TABLE 200 L3_ACL_DEVICE_DEPLOYMENT_MAP

Field	Definition	Format	Size
DEPLOYMENT_ID	Deployment configuration ID.	int	
L3_ACCESS_CONTROL_LIST_ID		int	

TABLE 201 L3_ACL_INT_DEPLOYMENT_MAP

Field	Definition	Format	Size
ID		serial	
DEPLOYMENT_ID	Deployment configuration ID.	int	
INBOUND_L3_ACL_ID	L3 Access control List ID of the L3 ACL selected for inbound.	int	
INBOUND_WRITE_TO_DEVICE	1/0 corresponding to Write to device/not write to device for inbound traffic.	smallint	

TABLE 201 L3_ACL_INT_DEPLOYMENT_MAP (Continued)

Field	Definition	Format	Size
OUTBOUND_L3_ACL_ID	L3 Access control List Id of the L3 ACL selected for outbound. Foreign Key for ACCESS_CONTROL_LIST table.	int	
OUTBOUND_WRITE_TO_DEVICE	1/0 corresponding to Write to device/not write to device for outbound traffic.	smallint	

TABLE 202 LAG

Field	Definition	Format	Size
ID	DB ID of LAG(Port-Channel).	int	
VIRTUAL_SWITCH_ID	FK to owning VIRTUAL_SWITCH	int	
LAG_ID	LAG ID	int	
IF_INDEX	Interface index	int	
IF_NAME	Interface name	varchar	256
ENABLED	LAG is enabled=1, disabled=0	smallint	
LAG_MODE	Static or dynamic (1=dynamic, 2=static)	smallint	
ACTIVE	LACP active or passive (1=active, 2=passive) valid if mode=dynamic	smallint	
TYPE	Trunking type (1=standard, 2=brocade, 3=hybrid)	smallint	
IF_MODE	L2 or L3 mode	varchar	8
L2_MODE	Type of L2 mode (default=access	varchar	32
MAC_ACL_POLICY	stores the MAC ACL policy information of the LAG	varchar	64
VLAN_LIST	Comma separated vlan ID list.	text	
MAC_ADDRESS	MAC address of LAG(Port-Channel).	varchar	64
IP_ADDRESS	Primary IPAddress of the LAG	varchar	128
NET_MASK	Netmask of the Primary IPAddress of the LAG	varchar	128
MINIMUM_LINKS	Least number of operationally UP links to declare the port-channel UP. range 1..16.	int	
MTU	Maximum transmission unit in bytes. range 1522..9208.	int	
LOAD_BALANCE	Load balancing details.	varchar	64
VLAG	Specifies whether the lag is a vlag or not.	smallint	

TABLE 203 LAG_MEMBER

Field	Definition	Format	Size
ID	DB ID of LAG member(port).	int	
LAG_ID	FK to owning LAG	int	
NAME	Member name	varcha	64

TABLE 203 LAG_MEMBER (Continued) (Continued)

Field	Definition	Format	Size
TYPE	currently not used. The default value is 0.	smallint	
MEMBER_MODE	Dynamic Mode Active/passive. The default value is 0.	smallint	

TABLE 204 LAST_CONFIG_UPDATE_TIME

Field	Definition	Format	Size
ID	Primary key.		
MANAGED_ELEMENT_ID	The managed element id of the device. This is the foreign key to MANAGED_ELEMENT table.	int	
CONFIG_XPATH	The xpath string.	varchar	1024
LAST_UPDATE_TIME	Timestamp returned by the device for this particular xpath.	bigint	

TABLE 205 LAUNCH_IN_CONTEXT_MODULE

Field	Definition	Format	Size
NAME	Unique dialog name used as a module name when launching in context.	varchar	64
DESCRIPTION	Description about the dialog features.	varchar	256
XML_FILE_NAME	The dialog XML XUL file name used to launch the dialog.	varchar	64
PRIVILEGE_ID	This is the comma separated list of privilege IDs required to launch this dialog. This is either the list of values from PRIVILEGE.ID column or -1 if no privilege is required to launch this dialog.	varchar	64
READ_WRITE_ACCESS	Specifies the read or write access privilege required to launch this dialog. 0 = no access is required to launch this dialog. 1 = At least the read-only access is required for the above privilege to launch this dialog. 2 = The read-write access is required for the above privilege to launch the dialog.	int	
EMPTY_DIALOG_ALLOWED	This field indicates whether the dialog can be launched even when there are no fabrics discovered. • 0 = Yes • 1= No	int	
INTERNAL_MODE_DIALOG	The DCFM main client is not visible when the dialog is launched in internal mode. This mode is used when launching from SMIA config tool. • 0- No • 1- Only internal mode • 2- Internal and external	int	

TABLE 205 LAUNCH_IN_CONTEXT_MODULE (Continued)

Field	Definition	Format	Size
LICENCE_PACKAGE_TYPE	Column to indicate whether the dialog is related to SAN or IP license package type. • 0 = SAN package • 1 = IP Package	int	
OPTIONAL_PARAMS	Comma separated names of all the optional parameters such as WWN.	varchar	256
OPTIONAL_PARAMS_DESC	Comma separated descriptions for the above optional parameters.	varchar	1024

TABLE 206 LICENSE

Field	Definition	Format	Size
ID	Unique Number assigned for the license information.	int	
LICENSE_KEY	License key string which has encoded value of number of products, ports licensed and package which this license isapplicable, etc.	varchar	1024
SERIAL_NO	Unique serial number string that helps to identify the customer or organization which this license is issued for.	varchar	255
CREATION_TIME	Time at which this license key is added	timestamp	
TYPE	Type of license: • 0 - Trial, • 1 - Permanent. The default value is 0.	smallint	
SUB_TYPE	Sub Type of license: • 0 - Base, • 1 - Addon. The default value is 0.	smallint	
VALID	Is this license still considered: • 0 - No, • 1 - Yes. The default value is 1.	smallint	

TABLE 207 LICENSE_DOWNGRADE_DETAILS

Field	Definition	Format	Size
ID	Primary key ID.		
PREVIOUS_LICENSE_INFO	Previous License information during downgrade. The details will have license type, license count like fabric, device, port etc.	varchar	512
NEW_LICENSE_INFO	New License information during downgrade. The details will have license type, license count like fabric, device, port etc.	varchar	512
DOWNGRADE_TIME	Time when License is downgraded.	timestamp	

TABLE 207 LICENSE_DOWNGRADE_DETAILS (Continued)

Field	Definition	Format	Size
DOWNGRADED_BY	User who performed license downgrade.	int	
IS_ACTIVE	Takes the value 0 or 1. • 1 - currently active downgrade • 0 - inactive or older downgrade.	smallint	

TABLE 208 LICENSE_FEATURE_MAP

Field	Definition	Format	Size
LICENSE_ID*	Foreign Key (SWITCH_LICENSE.ID) and is part of the primary key.	int	
FEATURE_ID*	Foreign Key (LICENSED_FEATURE.ID) and is part of the primary.	int	

TABLE 209 LICENSE_RULE

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
NAME	Name of the license rule	varchar	
DESCRIPTION	Description of the rule	varchar	
SCOPE	Scope of the rule - is it applicable to Fabric, switch or ports	varchar	
CATEGORY	Category of the rule - is it used by unknown - 0, asset collection - 1, or 2 - the license manager service	smallint	
ENABLE	Whether the rule needs to be considered or not. 1 - consider, 0 - do not consider for calculation. The default value is 1.	smallint	

TABLE 210 LICENSED_FEATURE

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
NAME	License feature name, a short text description.	varchar	64
DESCRIPTION	Optional detailed description about the license feature.	varchar	256

TABLE 211 LINK

Field	Definition	Format	Size
LINK_ID	Unique database generated identifier.	int	
TYPE	Type of the link. Currently it is always U.	varchar	1
NAME	Name of the link which is combination of device display name and ifName of the interface which this link associated.	varchar	255

TABLE 212 LOCK

Field	Definition	Format	Size
NAME	The name of this transaction synchronization lock. The name should be upper case and should describe the activity being synchronized, such as MANAGED_ELEMENT_CREATION.	varchar	40
LAST_USED_BY	Identifies the transaction that last updated this lock record, such as IP_DISCOVERY. This field is primarily here just to have something to modify. The new value does not need to be different than the previous value.	varchar	40
LAST_USED_TIME	Optional time when the lock was last modified. Might be useful for debugging someday.	timestamp	

TABLE 213 LSAN_DEVICE

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
BB_FABRIC_ID	Backbone fabric DB ID.	int	
FCR_FABRIC_ID	FID assigned to edge fabric.	int	
DEVICE_PORT_WWN	Device port WWN of physical device.	char	23
PHYSICAL_PID	PID of physical device.	char	6

TABLE 214 LSAN_TAG_CONFIG

Field	Definition	Format	Size
ID*	Unique id for FCR LSAN Tags configuration	int	
VIRTUAL_SWITCH_ID	Database identifier of virtual switch which represent FC Router.	int	
TAG_ENABLED	Indicates whether the LSAN tag is enabled or not. Possible values are 0 -false, 1 - true.	smallint	
ENFORCE_TAGS	List of enforcement tags configured in FC router. Enforce tag reduces the resources used in an FC router by limiting the number of LSAN zones that will be enforced in that FC router. There can be maximum of 8 enforce tags per FC router.	varchar	128
SPEED_TAGS	Speed tag configured in FC router. Speed tag allows you to speed up the discovery process by importing the devices into the remote edge fabrics when the devices come online.	varchar	16

TABLE 215 LSAN_PROXY_DEVICE

Field	Definition	Format	Size
FCR_FABRIC_ID*	FID assigned to edge fabric	int	
PROXY_PID*	Proxy device PID	char	6
STATE	State of the device	varchar	128
LSAN_DEVICE_ID*	LSAN_DEVICE record reference	int	

TABLE 216 LSAN_ZONE

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
BB_FABRIC_ID	Backbone fabric DB ID.	int	
EDGE_FABRIC_ID	FID assigned to edge fabric.	int	
NAME	LSAN zone name.	varchar	128
BACKBONE	0= is not a backbone lsan zone, 1= is a backbone lsan zone. Default value is 0.	smallint	

TABLE 217 LSAN_ZONE_DB_CONFIG

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
BB_FABRIC_ID	Backbone fabric db ID.	int	
EDGE_FABRIC_ID	FID assigned to edge fabric.	int	
ZONE_CONTENT	LSAN zone string.	text	
BACKBONE	0= is not a backbone lsan zone configuration. 1= is a backbone lsan zone configuration.	smallint	

TABLE 218 LSAN_ZONE_MEMBER

Field	Definition	Format	Size
LSAN_ZONE_ID*	LSAN_ZONE record reference.	int	
MEMBER_PORT_WWN*	Zone member WWN.	char	23

TABLE 219 MCT_CLIENT

Field	Definition	Format	Size
MCT_CLIENT_ID	MCT Client db ID.	int	
RBRIDGE_ID	MCT Client rbridge ID.	int	
CLIENT_NAME	MCT Client name.	varchar	(100)
PORT_ID	MCT Client port foreign key.	int	
OPER_STATE	MCT Client operational state.	smallint	
DEPLOY_STATE	MCT Client deployment state: • Deployed(0) • Undeployed(1)	smallint	
VCN_MEMBER_ID	Virtual Cluster Node member Cluster id foreign key.	int	

TABLE 220 MAC_FILTER

Field	Definition	Format	Size
ID		serial	
MAC_FILTER_NUMBER	MAC Filter number.	int	
FILTER_ACTION	Defined Permit - 0 or Deny -1	smallint	

TABLE 220 MAC_FILTER (Continued)

Field	Definition	Format	Size
DESCRIPTION	Description associated with each MAC Filter entry.	varchar	256
SOURCE_MAC_ADDRESS	Source MAC Address.	varchar	24
SOURCE_ADDRESS_MASK	Source MAC address mask.	varchar	24
DEST_MAC_ADDRESS	Destination MAC Address.	varchar	24
DEST_ADDRESS_MASK	Destination MAC address mask.	varchar	24
ETHERNET_TYPE	This column specifies the Ethernet Type. This field can take 0(not used), 1(etype), 2(llc), 3(snap).	smallint	
OPERARTOR	This column specifies the operator. This field can take 0(=), 1(!=), 2(<), 3(>).	smallint	
FRAME_NUMBER	This column specifies the Frame Number. Range is from 0600-FFFF in hex presentation.	int	
OPERATION_TYPE		varchar	10
DEPLOYMENT_ID	Deployment configuration ID. Foreign Key for DEPLOYMENT table.	int	
INT_BINDING_DIRECTION	Represents the interface binding direction. 0/1/2 corresponds to IN / OUT/BOTH direction.	smallint	

TABLE 221 MAC_FILTER_DEV_DEPLOYMENT_MAP

Field	Definition	Format	Size
DEPLOYMENT_ID	Deployment configuration ID.	int	
MAC_FILTER_ID	MAC FILTER Id for reference to the MAC_FILTER.	int	

TABLE 222 MAC_FILTER_INT_DEPLOYMENT_MAP

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
DEPLOYMENT_ID	Deployment configuration ID. Foreign Key for DEPLOYMENT table.	int	
INBOUND_MAC_FILTER_ID	MAC FILTER Id of the MAC Filter selected for inbound. Foreign Key for MAC_FILTER table.	int	
INBOUND_WRITE_TO_DEVICE	1/0 corresponding to Write to device/not write to device for inbound traffic.	smallint	

TABLE 223 MAC_GROUP

Field	Definition	Format	Size
ID	Sequence number of the records	int	
NAME	Name of the mac group, for internal representation of the group.	varchar	128

TABLE 223 MAC_GROUP

Field	Definition	Format	Size
MAC_GROUP_ID	The ID will represent any one of the following. 1 A cluster wide unique identifier defined in Network OS switch to be used in mac-based GVLAN classification at access port. Allowed range is 0 through 500 both inclusive. 2 INTERNAL GROUP ID - A dummy group ID (-1), used to represent one or more mac addresses that can be associated with a GVLAN. 3 CUSTOM MAC GROUP ID: Reserved for future usage if Network Advisor provides an option through UI to create MAC GROUPs.	Int	
TYPE	This indicates if the mac group is internal to BNA or mapped to device. 0- internal mac group, 1- external mac group defined in network OS switch, 2- User defined mac groups.	int	

TABLE 224 MAC_GROUP_MEMBER

Field	Definition	Format	Size
ID	Primary Key. Sequence number of the records.	int	
MAC_GROUP_DB_ID	Foreign Key Reference to the MAC_GROUP table.	int	
MAC_ADDRESS	Mac Address that belongs to the Mac group.	varchar	64
MASK	Mask applied on the mac address.	varchar	64

TABLE 225 MANAGED_ELEMENT

Field	Definition	Format	Size
ID	An ID that is unique across managed elements of all types: SAN physical switches, SAN logical switches, IP switches, and hosts. Also the primary key for the MANAGED_ELEMENT table.	int	
PLACEHOLDER	Not used. iBatis/Abator requires at least one non-serial column to generate correct objects. The default value is 0.	int	

TABLE 226 MAPS_EVENT

Field	Definition	Format	Size
ID	The primary key of the table.	int	
HOST_TIME	The time at which the server processed the event.	timestamp	
CATEGORY	The violations category. i.e. Port Health, Fabric Health, etc.	int	
VIOLATION_TYPE	The type of the violation. i.e. CRC, ITW.	int	
MANAGED_ELEMENT_ID	The managed element corresponding to this event.	int	
ORIGIN_FABRIC_ID	The fabric from which the event originated. Retaining this id as historical data.	int	

TABLE 226 MAPS_EVENT (Continued)

Field	Definition	Format	Size
SWITCH_PORT_ID	Nullable foreign key. The FC port for which the event occurred. This will only be populated for port events.	int	
FCIP_CIRCUIT_ID	Nullable foreign key. The FCIP tunnel circuit for which the event occurred. This will only be populated for FCIP tunnel events.	int	
FRU_NAME	For switch policy status events, the object name is provided in the event and indicates the name of the FRU affected. i.e. PS 1, Fan 2. As this FRU object name is only provided for one category of events, making the column nullable.	varchar	32
VM_ID	Nullable foreign key. The VM for which the event occurred. This will only be populated for vCenter events.	int	
FLOW_DEFINITION_ID	Nullable foreign key. The NP flow definition for which the event occurred. This will only be populated for flow events	int	
INTERFACE_ID	Denotes interface_id for NOS interface related interface violations. This will only be populated for NOS Ethernet related port Events, for other FC ports of NOS switch_port_id will be populated.	int	

TABLE 227 MAPS_EVENT_DETAILS

Field	Definition	Format	Size
ID	The primary key of the table.	int	
MAPS_EVENT_ID	The corresponding maps_event.	int	
SWITCH_TIME	The switch timestamp from the event.	timestamp	
RULE_NAME	The name of the threshold rule.	varchar	32
RULE_CONDITION	The threshold condition in string format. i.e. CRC > 30	varchar	128
TIME_BASE	The time base for the threshold. 0 - None, 1 - Minute, 2 - Hour, 3 - Day	int	
ACTIONS	A bit map for the actions configured for the rule. 0 - None, 1 - RASLOG, 2 - SNMP, 4 - Email, 8 - Fence Port, 16 - SW_ST_DOWN, 32 - SW_ST_MARGINAL.	int	
CURRENT_VALUE	The current value of the measure that triggered the violation.	varchar	32
SWITCH_ENABLED_ACTIONS	MAPS actions enabled on the switch at the time the violation occurred.	int	

TABLE 228 MAPS_EVENT_CAUSE_ACTION

Field	Definition	Format	Size
VIOLATION_TYPE	The type of the violation. i.e. CRC, ITW, as defined in MapsConstants.	int	
ACTION	Description of the recommended action for the MAPS violation.	varchar	4096

TABLE 229 MAPS_POLICY

Field	Definition	Format	Size
ID	The primary key of the table.	int	
VIRTUAL_SWITCH_ID	The id of the virtual switch.	int	
NAME	The name of the MAPS policy.	varchar	32
IS_ACTIVE	Indicates if the policy is the active policy on the switch. 0 - No, 1 - Yes.	int	
IS_DEFAULT	Indicates if the policy is a default policy on the switch. 0 - No, 1 - Yes.	int	

TABLE 230 MARCHING_ANTS

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
THRESHOLD1_VALUE	The marching ants low boundary threshold value (T1).	int	
THRESHOLD2_VALUE	The marching ants high boundary threshold value (T2).	int	

TABLE 231 MEASURE

Field	Definition	Format	Size
ID	Primary key column.	int	
MEASURE_TYPE	Measure type 0 - SNMP MIB, 1-- Expression 2-- EE Monitor counter 3-- HBA counter,4 - Custom, 5 - NetworkPatroller, 6 - NOS Ethernet Port optics etc.	smallint	
INDEX_TYPE	Identifies the index type for a given SNMP MIB or Expression measure. Various index type supported are 0 - UNKNOWN, 1 - SCALAR, 2 - IF_INDEX, 3 - ETHER_STATS_INDEX, 4 - CONN_UNIT_INDEX, 5 - FCIP_LINK_TABLE_INDEX, 6 - CUSTOM, 7 - SW_TEMP_SENSOR_INDEX, 8 - SW_FAN_SENSOR_INDEX, 9 - SW_POWER_SENSOR_INDEX. For non-SNMP measures like EE Monitors, Ping statistics etc. index type is not applicable. In that case index type would be updated as 0 - Unknown.	smallint	
NAME	Name of the measure.	varchar	64
DETAIL	For SNMP MIB, stores the OID, for expression, stores the expression formula.	varchar	1024
UNIT	Unit string thats used for displaying the chart.	varchar	64
DESCRIPTION	Description for the measure. Default: 1	varchar	512
IS_SYSTEM	Indicates whether this is a system built in measure, for system expressions , user cannot delete it.	smallint	

TABLE 232 MESSAGE_RECIPIENT

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
DESCRIPTION	Description about recipient.	varchar	256
IP_ADDRESS	IP Address of the recipient.	varchar	128
PORT	Port number of the recipient.	int	
RECIPIENT_TYPE_ID	Recipient Type (Syslog or SNMP).	int	
ENABLED	If forwarding to destination is enabled.	smallint	
SOURCE_ADDRESS_ADDED	If source address is added as another varbind in trap. -1 for Syslog i.e RECIPIENT_TYPE_ID: 2. Default value is -1.	smallint	
REPEATER_ENABLED	If filtering is disabled. -1 for Syslog i.e RECIPIENT_TYPE_ID: 2. Default value is -1.	smallint	
VERSION	Snmp version(v1/v2/v3)	varchar	8

TABLE 233 MIGRATION_HISTORY

Field	Definition	Format	Size
ID	The primary key of the table.	int	
SOURCE_RELEASE	Source release name, version number and patch number. Example Network Advisor 11.3.0a.	varchar	128
SOURCE_RELEASE_BUILD_NUMBER	Source release build number.	int	
TARGET_RELEASE	Target release name and version. Example Network Advisor 12.1.0.	varchar	128
TARGET_RELEASE_BUILD_NUMBER	Target release build number.	int	
MIGRATION_TIME	Date and Time at which this migration completed.	timestamp	

TABLE 234 MODULE

Field	Definition	Format	Size
MODULE_TYPE_ID	Primary key for this table.	int	
MODULE_TYPE	Type of the module.		
NAME	Name of the module configured in this device.		
DESCRIPTION	Description of the module.	varchar	128
NUM_PORTS	Number of ports present in this module.	num	(4,0)
TABLE_SUBTYPE	Identifies the table name which more properties/attributes about this module stored. Possible value is FOUNDRY_MODULE.	varchar	32
IS_PRESENT	Identifies the module is present or not. Not Present-0, Present-1.	num	(1,0)
IS_MANAGEMENT_MODULE	Identifies the module is management module or not. Other module-0, Management module-1.	num	(1,0)

TABLE 234 MODULE (Continued)

Field	Definition	Format	Size
NUM_CPUS	The number of CPUs present in the module.	smallint	
HW_REVISION	The vendor-specific hardware revision string. Refer entPhysicalHardwareRev of RFC4133-ENTITY-MIB.mib for more details.	varchar	64
FW_REVISION	The vendor-specific firmware revision string. Refer entPhysicalFirmwareRev of RFC4133-ENTITY-MIB.mib for more details.	varchar	64
SW_REVISION	The vendor-specific software revision string. Refer entPhysicalSoftwareRev of RFC4133-ENTITY-MIB.mib for more details.	varchar	64
MODULE_STATUS	Specifies the status of the module. Possible values are 0, 2, 3, 4, 8, 9, 10, 11. 0 - moduleEmpty, 2 - moduleGoingDown, 3 - moduleRejected, 4 - moduleBad, 8 - moduleConfigured, 9 - moduleComingUp, 10 - moduleRunning, 11 - moduleBlocked.	int	
REDUNDANT_STATUS	Specifies the redundant status of the module. Possible values are 1, 2, 3, 4, 5. 1 - other, 2 - active, 3 - standby, 4 - crashed, 5 - comingUp. Non management modules always return value as other. Management module returns the rest of the states.	int	
OPERATIONAL_STATUS	Specifies the operational status of the module. Possible values for NI series products are as below: • CARD_STATE_NOT_PRESENT, • CARD_STATE_INIT, • CARD_STATE_BOOT, • CARD_STATE_LP_SYNC, • CARD_STATE_INTERACTIVE, • CARD_STATE_SW_LOADED, • CARD_STATE_STRIPE_SYNC, • CARD_STATE_UP, • CARD_STATE_DOWN, • CARD_STATE_POWERED_OFF, • CARD_STATE_RECOVERY, • CARD_STATE_REBOOT, • CARD_STATE_SYNC_FID. Empty string indicates, module has not been inserted to the chassis or not applicable for this product.	varchar	64

TABLE 235 MODULE_SLOT_PRESENT

Field	Definition	Format	Size
MODULE_SLOT_PRESENT_ID	Unique database generated identifier.	int	
MODULE_ID	Database ID of the MODULE instance.	int	
SLOT_ID	Database ID of the SLOT instance.	int	

TABLE 236 MPLS_ADMIN_GROUP

Field	Definition	Format	Size
MPLS_ADMIN_GROUP_DB_ID	Unique database generated identifier.	int	
NAME	The group name that this administrative group is associated with.	varchar	255
ID	Identifies the administrative group.	int	
DEVICE_ID	Database ID of the DEVICE instance from which this admin group is retrieved.	int	

TABLE 237 MPLS_ADMIN_GROUP_INTERFACE_RELATION

Field	Definition	Format	Size
MPLS_ADMIN_GROUP_INTERFACE_RELATION_DB_ID	Unique database generated identifier.	int	
MPLS_ADMIN_GROUP_DB_ID	Database ID of the MPLS_ADMIN_GROUP instance.	int	
INTERFACE_ID	Database ID of the INTERFACE instance.	int	

TABLE 238 MPLS_LSP

Field	Definition	Format	Size
MPLS_LSP_DB_ID	Unique database generated identifier.	int	
TABLE_SUBTYPE	Refers to the subtype of the LSP where additional attributes/properties of different type of LSP stored. The possible values are MPLS_RSVP_LSP, MPLS_LSP.	varchar	32
NAME	Name of the Label Switched Path.	varchar	255
DESTINATION_IP_ADDRESS	Destination IP Address of the egress LSR associated with this tunnel instance.	varchar	255
OPER_STATUS	Actual operational status of this tunnel, which is typically but not limited to, a function of the state of individual segments of this tunnel. Up-1, Down-2, Testing-3, Unknown-4, Dormant-5, Not present-6, Lower Layer Down-7.	smallint	
DEVICE_ID	Database ID of the DEVICE Instance from which this LSP retrieved.	int	

TABLE 239 MPLS_PATH

Field	Definition	Format	Size
MPLS_PATH_DB_ID	Unique database generated identifier.	int	
NAME	Name of the MPLS Path as configured in the device. Refer mplsTunnelHopPathOptionName of RFC3812 for more details.	varchar	255
DEVICE_ID	Database ID of the DEVICE Instance from which this path information retrieved.	int	

TABLE 240 MPLS_PATH_HOP

Field	Definition	Format	Size
MPLS_PATH_HOP_DB_ID	Unique database generated identifier.	int	
HOP_INDEX	Index of the MPLS hop.	int	
HOP_IP_ADDRESS	The Tunnel Hop Address for this tunnel hop.	varchar	255
HOP_TYPE	Denotes whether this tunnel hop is routed in a strict or loose fashion. Possible Values are Strict-1 and Loose-2.	smallint	
MPLS_PATH_DB_ID	Database ID of the MPLS_PATH Instance which this hop is part of.	int	

TABLE 241 MPLS_RSVP_LSP

Field	Definition	Format	Size
MPLS_LSP_DB_ID	Unique database generated identifier.	int	
IS_ENABLED	Represents whether the LSP is enabled. Enabled-1, Disabled-0.	num	(1,0)
IS_BYPASS	Represents if the LSP is a Bypass LSP or not. Not a Bypass-0, Bypass LSP-1. Currently ByPass LSPs are not supported. So the value will be always 0.	num	(1,0)
FROM_IP_ADDRESS	Represents the Source IP Address of the LSP.	varchar	255
METRIC	Represents the metric of the LSP used by the routing protocols to determine the relative preference among several LSPs towards a given destination. Accepts a range of 1 - 65535.	int	
PATH_SELECT_MODE	Specifies the path selection mode to use. Refer mplsLspPathSelectMode MIB of foundry.mib for more details and possible values.	smallint	
PATH_SELECT_PATH	The user-selected pathname when the Path Selection mode is either Manual or Unconditional. If the device returns null or empty string, this value would be primary.	varchar	255
REVERT_TIMER	The number of seconds to wait after the primary or selected path comes up before traffic reverts to that path. A value of 0 indicates that it will switch immediately after the current working path goes down. The range of values supported are 0-65535.	int	
TIE_BREAKING_MODE	Specifies the tie breaking mode for selecting the Constrained Shortest Path First(CSPF) equal-cost paths. Possible values are Random-1, LeastFill-2 and MostFill-3.	smallint	

TABLE 241 MPLS_RSVP_LSP (Continued)

Field	Definition	Format	Size
IS_USE_LSP_FOR_OSPF_SHORTCUTS	Indicates that this LSP allows shortcut between nodes in an AS. OSPF includes the LSP in its SPF calculation. Possible values are Not Allowed-0 and Allowed-1.	num	(1,0)
IS_USE_LSP_FOR_ISIS_SHORTCUTS	Flag to indicate if the LSP is to be used by ISIS destinations.	num	(1,0)
LSP_FOR_ISIS_SHORTCUTS_LEVEL	ISIS level to which the LSP is advertised into	int	
LSP_FOR_ISIS_SHORTCUTS_RELATIVE_METRIC	Add or subtract relative metric.	int	
IS_LSP_FOR_ISIS_SHORTCUTS_ANNOUNCE	Flag that indicates if the LSP is to be announced into ISIS domain.	num	(1,0)
LSP_FOR_ISIS_SHORTCUTS_ANNOUNCE_METRIC	If announced into ISIS domain metric used by the LSP.	int	

TABLE 242 MPLS_RSVP_LSP_ACTUALLY_ROUTED_HOP

Field	Definition	Format	Size
MPLS_RSVP_LSP_ACTUALLY_ROUTED_HOP_DB_ID	Unique database generated identifier.	int	
HOP_INDEX	Index of actually routed hop.	varchar	255
HOP_IP_ADDRESS	The Tunnel Hop Address for this tunnel hop.	int	
MPLS_LSP_DB_ID	Database ID of the MPLS_RSVP_LSP instance which this hop is part of.	int	

TABLE 243 MPLS_RSVP_LSP_ADMIN_GROUP

Field	Definition	Format	Size
MPLS_RSVP_LSP_ADMIN_GROUP_DB_ID	Unique database generated identifier.	int	
AFFINITY_TYPE	Represents the affinity type of the MPLS Admin Group. Possible values are Unknown-0, Include Any-1, Include All-2 and Exclude Any-3.	smallint	
MPLS_ADMIN_GROUP_DB_ID	Database ID of the MPLS_ADMIN_GROUP Instance.	int	
MPLS_RSVP_LSP_ADMIN_GROUP_CONTAINER_DB_ID	Database ID of the MPLS_RSVP_LSP_ADMIN_GROUP_CONTAINER instance.	int	

TABLE 244 MPLS_RSVP_LSP_ADMIN_GROUP_CONTAINER

Field	Definition	Format	Size
MPLS_RSVP_LSP_ADMIN_GROUP_CONTAINER_DB_ID	Unique database generated identifier.	int	
MPLS_RSVP_LSP_PARAMETERS_DB_ID	Database ID of the MPLS_RSVP_LSP_PARAMETERS instance.	int	
MPLS_RSVP_LSP_FRR_PARAMETERS_DB_ID	Database ID of the MPLS_RSVP_LSP_FRR_PARAMETERS instance.	int	

TABLE 245 MPLS_RSVP_LSP_FRR_PARAMETERS

Field	Definition	Format	Size
MPLS_RSVP_LSP_FRR_PARAMETERS_DB_ID	Unique database generated identifier.	int	
BANDWIDTH	Specifies the bandwidth constraint for the MPLS Fast Reroute Path. The value 0 means that the detour route uses a best-effort value for bandwidth.	int	
HOP_LIMIT	Represents the limit for the number of hops the LSP can traverse. Accepted range is 0 - 255.	num	(3,0)
IS_FACILITY_BACKUP	Specifies whether the request for Facility backup is enabled or not. If the FRR mode is facility then this value will be 1. 0 otherwise.	num	(1,0)
SETUP_PRIORITY	The setup priority for MPLS Fast Reroute.Allowed range between 0-7.	num	(1,0)
HOLD_PRIORITY	'The hold priority for MPLS Fast Reroute. Allowed range between 0-7.	num	(1,0)
MPLS_LSP_DB_ID	Database ID of the MPLS_RSVP_LSP instance which these reroute parameters associated with.	int	

TABLE 246 MPLS_RSVP_LSP_PARAMETERS

Field	Definition	Format	Size
MPLS_RSVP_LSP_PARAMETERS_DB_ID	Unique database generated identifier.	int	
IS_ADAPTIVE	Indicates if the LSP supports adaptive mechanism or not. Non Adaptive-0, Adaptive-1.	num	(1,0)
BFD_TRANSMIT	This object specifies the minimum interval, in milliseconds, that the local system would like to use when transmitting The Bidirectional Forwarding Detection(BFD) Control packets. Accepts a range of 50-30000.	int	
BFD_RECEIVE	This object specifies the minimum interval, in milliseconds, between received Bidirectional Forwarding Detection (BFD) Control packets the local system is capable of supporting. Accepts a range of 50-30000.	int	
BFD_MULTIPLIER	The Bidirectional Forwarding Detect time multiplier. Accepts a range of 3-50.	int	
COS	The Class of Service for this LSP. Allowed range is 0-7 and 255. 255 means COS is not explicitly configured.	smallint	
HOP_LIMIT	Represents the limit for the number of hops the LSP can traverse. Accepted range is 0-255.	num	(3,0)
IS_CSPF	Specifies whether the Constrained Shortest Path First (CSPF) calculation is enabled. Possible values are Disabled-0, Enabled-1.	num	(1,0)
MTU	Specifies the Maximum IP Packet Size of the packets without being fragmented. Valid range is 0-65535.	num	(4,0)
SETUP_PRIORITY	The setup priority of the tunnel. Valid range is 0-7.	num	(1,0)

TABLE 246 MPLS_RSVP_LSP_PARAMETERS (Continued)

Field	Definition	Format	Size
HOLD_PRIORITY	The holding priority of the tunnel. Valid range between 0-7.	num	(1,0)
IS_RECORD_ROUTES	Specifies whether the route is actually recorded route or not. Not Recorded-0 and Recorded-1.	num	(1,0)
REOPTIMIZE_TIMER	The number of seconds from the beginning of one reoptimization attempt to the beginning of the next attempt. Valid range is 300-65535 seconds. 0 is also accepted.	int	
MPLS_LSP_DB_ID	Database ID of the MPLS_RSVP_LSP instance which these parameters are associated with.	int	
MPLS_RSVP_LSP_PATH_DB_ID	Database ID of the MPLS_RSVP_LSP_PATH instance which these parameters are associated with.	int	

TABLE 247 MPLS_RSVP_LSP_PATH

Field	Definition	Format	Size
MPLS_RSVP_LSP_PATH_DB_ID	Unique database generated identifier.	int	
PATH_TYPE	The type of path that is active, i.e., a primary path, a standby path, or a generic secondary path. Possible values are Other-1, Primary-2, Standby-3 and Secondary-4.	smallint	
IS_STANDBY	Specifies whether the path is standby or not. Currently it is unused and value is always 0 (Not standby)	num	(1,0)
MPLS_LSP_DB_ID	Database ID of the MPLS_RSVP_LSP instance.	int	
MPLS_PATH_DB_ID	Database ID of the MPLS_PATH instance.	int	

TABLE 248 MPLS_RSVP_LSP_TUNNEL_RESOURCE

Field	Definition	Format	Size
MPLS_RSVP_LSP_TUNNEL_RESOURCE_DB_ID	Unique database generated identifier.	int	
MAX_RATE	Specifies the maximum data rate (kilo bits/secs) of the packet travelling over the LSP.	int	
MEAN_RATE	Specifies the mean data rate (kilo bits/secs) of the packet travelling over the LSP.	int	
MAX_BURST	The maximum burst size in bytes that the LSP can send at the maximum rate.	int	
MPLS_RSVP_LSP_PARAMETERS_DB_ID	Database ID of the MPLS_RSVP_LSP_PARAMETERS instance.	int	

TABLE 249 MPLS_SERVICE

Field	Definition	Format	Size
MPLS_SERVICE_DB_ID	Unique database generated identifier.	int	
NAME	Specifies the name of the MPLS Service.	varchar	255
VCID	Virtual Circuit Identifier of the MPLS Service.	bigint	

TABLE 249 MPLS_SERVICE (Continued)

Field	Definition	Format	Size
MPLS_SERVICE_TYPE	The type of the MPLS Service. Local VLL-1, Remote VLL-2, VLL-3, VPLS-4, Admin Group-8, Path-9, RSVP LSP-10.	smallint	
VLL_MODE	Specifies the Virtual Local Loop (VLL) Mode. Possible values are Unknown-0, Raw-1 and Taggged-2.	smallint	
STATUS	Status of the MPLS Service. All Peers Up-1, All Peers Down-2, Some Peers Down-3, Undefined-0.	smallint	
CONFLICTS	The type of Conflict. Possible values are None-0, Name Mismatch-1, VLL Mode Mismatch-2, Peer Incomplete-4, No Endpoints-8, Peer Missing-16, Duplicate VCID-32, Unknown-65535.	int	
LAST_UPDATED_TIME	Time when this service record last updated in the database.	num	(20,0)

TABLE 250 MPLS_SERVICE_DEVICE_RELATION

Field	Definition	Format	Size
MPLS_SERVICE_DEVICE_RELATION_DB_ID	Unique database generated identifier.	int	
MPLS_SERVICE_DB_ID	Database ID of the MPLS_SERVICE instance.	int	
DEVICE_ID	Database ID of the DEVICE instance.	int	
TABLE_SUBTYPE	Specifies the type of MPLS Service Relation with Device. Possible values are VLL_DEVICE_RELATION and VPLS_DEVICE_RELATION.	varchar	32
NAME	Name of the MPLS Service.	varchar	255
COS	This value indicates the Class Of Service for this endpoint (VLL/VPLS). Allowed range is 0-7 and 255. 255 means COS is not explicitly configured.	smallint	
MTU	Represents the maximum packet size configured on the VLL/VPLS instance.	int	

TABLE 251 MPLS_SERVICE_ENDPOINT_RELATION

Field	Definition	Format	Size
MPLS_SERVICE_ENDPOINT_RELATION_DB_ID	Unique database generated identifier.	int	
MPLS_SERVICE_DEVICE_RELATION_DB_ID	Database ID of the MPLS_SERVICE_DEVICE_RELATION instance.	int	255
INTERFACE_ID	Database ID of the INTERFACE instance associated with this end point (VLL/VPLS).	int	
TABLE_SUBTYPE	The Type of the MPLS Service endpoint relation. Possible values are VLL_ENDPOINT_RELATION and VPLS_ENDPOINT_RELATION.	varchar	32
TAG_MODE	This value indicates the vlan mode for this endpoint. Possible values are Tagged-1, Untagged-2.	smallint	

TABLE 251 MPLS_SERVICE_ENDPOINT_RELATION (Continued)

Field	Definition	Format	Size
VLAN_ID	Specifies the Outer VLAN ID value of this endpoint (VLL/VPLS).	smallint	
OPER_STATUS	Operational status of the endpoint. Possible values are Up-1, Down-2.	num	(2,0)
TAG_TYPE	The type of tagging supported. Possible values are Untagged-1, Dual-2 and Inner VLAN/ISID-3. ISID applicable only when dual tagging enabled for VPLS.	smallint	
INNER_VLAN_ID	This value indicates the inner tag for this endpoint. If tagging type is dual, then it returns the inner vlan id of the end point (VLL/VPLS). If tagging type is ISID and Untagged this value will be 0.	smallint	

TABLE 252 MPLS_SERVICE_PEER_RELATION

Field	Definition	Format	Size
MPLS_SERVICE_PEER_RELATION_DB_ID	Unique database generated identifier.	int	
MPLS_SERVICE_DEVICE_RELATION_DB_ID	Database ID of the MPLS_SERVICE_DEVICE_RELATION instance.	int	
PEER_DEVICE_ID	Database ID of the peer device.	int	
PW_INDEX	The pseudo-wire service index Mask.	int	
PEER_IP	The IP of the Peer Device of the PW/PE maintenance protocol entity.	varchar	255
OPER_STATUS	Operational Status of the peer with the MPLS Service. Refer PwOperStatus MIB of foundry.mib for more details and possible values.	smallint	

TABLE 253 MRP_RING

Field	Definition	Format	Size
MRP_RING_ID	Auto generated database ID for MRP ring.	int	
RING_ID	User configured unique ring number for MRP ring, Valid values are 1 – 255.	num	(8,0)
RING_NAME	Represents name of MRP ring.	varchar	255
STATUS	Computed Status of MRP ring. Status is computed based on MRP_RING devices. Possible status values are Normal-1, Warning-2 and Critical-3	smallint	
LAST_UPDATED	Time when this ring record was last updated in the database.	bigint	

TABLE 254 MRP_RING_DEVICE

Field	Definition	Format	Size
MRP_RING_DEVICE_DB_ID	Auto generated database ID for device in MRP Ring.	int	
MRP_RING_ID	Database ID of MRP ring.	int	
DEVICE_ID	Database ID of member device.	int	

TABLE 254 MRP_RING_DEVICE (Continued)

Field	Definition	Format	Size
PORT_VLAN_DB_ID	The database ID of the port VLAN. The master VLAN in the topology group used by this ring. If a topology group is used by MRP, the master VLAN controls the MRP settings for all VLANs in the topology group.	int	
MRP_RING_NAME	User configured name for the ring.	varchar	255
TOPO_GRP_ID	Topology group ID.	int	
STATE	Whether MRP is enabled or disabled on the device. Disabled-1, Enabled -2.	smallint	
ROLE	Represents role of device in MRP topology. Master-2, Member-3.	smallint	
HELLO_TIME	The interval, in milliseconds, at which the Forwarding port on the ring's master node sends Ring Health Packets (RHPs).	int	
PRE_FWD_TIME	The number of milliseconds a MRP interface that has entered the Pre forwarding state will wait before changing to the Forwarding state.	int	
PRI_PORT_INTERFACE_ID	Interface database ID for the Primary port of the device.	int	
PRI_PORT_STATE	State of device's primary port. Other-1, Pre-Forwarding- 2, Forwarding-3, Blocking-4, Disabled-5.	smallint	
PRI_PORT_TYPE	Type of device's primary port. Other-1, Regular port-2, Tunnel port-3.	smallint	
PRI_PORT_ACTIVE_INTERFACE_ID	Interface database ID of an primary active port, which is sending RHPs.	int	
SEC_PORT_INTERFACE_ID	Interface database ID for the Secondary port of the device.	int	
SEC_PORT_STATE	State of device's secondary port. Other-1, Pre-Forwarding- 2, Forwarding-3, Blocking-4, Disabled-5.	smallint	
SEC_PORT_TYPE	Type of device's secondary port. Other-1, Regular port-2, Tunnel port-3.	smallint	
SEC_PORT_ACTIVE_INTERFACE_ID	Interface database ID of an secondary active port, which is receiving RHPs.	int	
RHP_TX	The number of RHPs sent on the active interface.	bigint	
RHP_RC	The number of RHP packets received on the interface.	bigint	
STATE_CHANGED	The number of MRP interface state changes that have occurred.	int	
TC_BPDU_RC	The number of Topology Change RHPs received on the interface. A Topology Change RHP indicates that the ring topology has changed.	int	

TABLE 254 MRP_RING_DEVICE (Continued)

Field	Definition	Format	Size
STATUS	Computed status of device in MRP Ring. Possible status values are Normal-1, Warning-2 and Critical-3.	smallint	
LAST_UPDATED	Time when this record was last updated in the database.	bigint	

TABLE 255 N2F_PORT_MAP

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
VIRTUAL_SWITCH_ID	Virtual switch ID of AG for N to F_port mapping, foreign key to VIRTUAL_SWITCH table.	int	
N_PORT	Port number of port type N_Port which is being mapped, One N_Port can be mapped to multiple F_ports.	smallint	
F_PORT	Port number of port type F_Port which is being mapped.	smallint	

TABLE 256 NETWORK_VLAN

Field	Definition	Format	Size
VLAN_DB_ID	Database ID of the VLAN instance which is associated with the Network.	int	

TABLE 257 NETWORK_SCOPE_TYPE

Field	Definition	Format	Size
ID	The primary key of the table.	int	
NAME	Name of the Scope.	varchar	128
DESCRIPTION	Description of the Scope.	varchar	512
HANDLER_CLASS_NAME	Fully defined Handler Class for the predefined SCOPE.	varchar	128

TABLE 258 NIC_PROFILE

Field	Definition	Format	Size
ID*		int	
NAME	The name of the network interface in the format network interface name / host address.	varchar	255
IP_ADDRESS	The host address of the interface.	varchar	128

TABLE 259 NPORT_WWN_MAP

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
VIRTUAL_SWITCH_ID	AG switch reference on which the Nport wwn mapping resides.	int	

TABLE 259 NPORT_WWN_MAP (Continued)

Field	Definition	Format	Size
N_PORT	N Port through which AG is connected to the edge switch	smallint	
DEVICE_PORT_WWN	Device Port which is mapped to the N port. This device could be offline device as well.	char	23

TABLE 260 NP_FLOW_DEFINITION

Field	Definition	Format	Size
ID	The primary key of the table.	int	
NAME	The name of the table.	varchar	20
VIRTUAL_SWITCH_ID	The id for the virtual switch.	int	
SRCDEV	Comma separated list of source device ports.	varchar	1024
DSTDEV	Comma separated list of destination device ports.	varchar	1024
SRCPORT	Comma separated list of source switch ports.	varchar	1024
DSTPORT	Comma separated list of destination switch ports.	varchar	1024
BIDIR	This specifies if traffic in both direction has to be monitored, where, 0 - false, 1 - true.	smallint	
SFID	Source fabric ID.	int	
DFID	Destination fabric ID	int	
SRCDOMAIN	Source domain ID	int	
DSTDOMAIN	Destination domain ID	int	
LUNID	Comma separate list of LUN IDs	varchar	1024
OXID	FC Originator Exchange ID for the frame.	varchar	1024
QOS	Quality of Service, can be comma separated values of: 1 - low, 2 - medium, 3 - high.	varchar	1024
“OPTION”	A bitmask for options with following bit mapping: Noactive (0th bit) = 2^0 = 1 Noconfig (1st bit) = 2^1 = 2 NoZoneCheck (2nd bit) = 2^2 = 4	int	
SCSICMD	SCSI command frame types.	varchar	32
TYPE	Frame type value	varchar	32
RCTL	Routing control byte.	varchar	32
PROTOCOL_TYPE	Protocol types.	varchar	32
FRAME_OFFSET	Generic frame offset in format of byte offset, mask, value.	varchar	1024
“SIZE”	Size of the frame payload. Range: 64 bytes to max 2112 bytes, 0 for random size.	int	
PATTERN	String to specify the pattern of the payload.	varchar	32
LAST_UPDATED_TIME	Last updated time	timestamp	
MONITOR_FEATURE	Flow Monitor feature state. 0 - not selected, 1 - deactivated, 2 - selected and activated.	int	

TABLE 260 NP_FLOW_DEFINITION (Continued)

Field	Definition	Format	Size
GENERATOR_FEATURE	Flow generator feature state. 0 - not selected, 1 - deactivated, 2 - selected and activated.	int	
MIRROR_FEATURE	Flow mirror feature state. 0 - not selected, 1 - deactivated, 2 - selected and activated.	int	
IS_PREDEFINED	Flag which identifies if the flow definition is one of the pre-defined flow definitions on the switch.	smallint	

TABLE 261 NP_SUB_FLOW

Field	Definition	Format	Size
ID	The primary key of the table.	int	
FLOW_DEFINITION_ID	The id of the flow definition	int	
FEATURE	Feature this sub flow is associated with. Feature can be one of the following: Monitor - 0, Generator - 1, Mirror - 2	int	
SRCDEV	Source device port.	varchar	32
DSTDEV	Destination device port.	varchar	32
SRCPORT	Switch Source port.	varchar	32
DSTPORT	Switch Destination port.	smallint	
BIDIR	This specifies if traffic in both direction has to be monitored, where, 0 - false, 1 - true		
SFID	Source fabric ID	int	
DFID	Destination fabric ID	int	
SRCDOMAIN	Source domain ID	int	
DSTDOMAIN	Destination domain ID	int	
LUNID	LUN ID.	varchar	32
LAST_UPDATED_TIME	Last updated time	timestamp	
IS_MISSING	Is the sub flow no more available on the switch? 0 - false, 1 - true.	smallint	
OXID	FC Originator Exchange ID for the frame..	int	
RXID	FC Responder Exchange ID for the frame.	int	
CS_CTL	Frame header CS_CTL..	int	
"SIZE"	Size of the frame payload. Range: 64 bytes to max 2112 bytes, 0 for random size.	int	
PATTERN	String to specify the pattern of the payload.	varchar	32

TABLE 262 OUI_GUESSED_DEVICE_MAP

Field	Definition	Format	Size
OUI*	Vendor OUI.	char	6
TYPE	Guessed device type for this vendor.	varchar	32

TABLE 263 OUI_VENDOR

Field	Definition	Format	Size
OUI*	Vendor OUI, 6-digit hexadecimal number which can have leading digits as zero.	char	6
VENDOR	Vendor name.	varchar	64
VENDOR_CATEGORY	Default is ‘none’.	varchar	32

TABLE 264 PASSWORD_HISTORY

Field	Definition	Format	Size
USER_NAME		varchar	128
PASSWORD_UPDATED_DATETIME	The date and time the user updated password recently.	timestamp	
PREVIOUS_PASSWORD	User"s Previous password	varchar	512

TABLE 265 PBR_INTERFACE_CONFIG

Field	Definition	Format	Size
ID	Primary key.	int	
POLICY_ID	PBR policy ID.	int	
INTERFACE_NAME	Name of the ingress interface.	varchar	32
IP_TYPE	Defines the ip type, v4 or v6, of the pbr policy the interface is bound to. Value 1 indicates IPv4 policy. Value 2 indicates IPv6 policy.	int	
ALLOW_VLAN	Indicates if the packets arriving at the ingress ports allow all VLANs or not.	smallint	

TABLE 266 PERF_COLLECTOR

Field	Definition	Format	Size
COLLECTOR_ID	Primary key autogenerated ID.	int	
NAME		varchar	128
STATUS	Status of the collector. if the value is set to "E" means the collector is enabled state and "D" means disabled.	char	1
TYPE	Target type of the SNMP collector data. The target type for, • device level collector is 0 • port level collector is 1.	num	(2,0)
POLLING_INTERVAL	Time interval in seconds; indicates the frequency with which the collector will poll the device to get the data.	int	
CREATED_TIME_SECONDS	Collector created time.	int	
PROPS_STR	Serialized string for the threshold or rearm property.	varchar	256

TABLE 267 PBR_NEXT_HOP

Field	Definition	Format	Size
ID	Primary key.	int	
RULE_ID	PBR rule id.	int	
NEXT_HOP_SEQUENCE	The sequence of the next hop entry that corresponds to a rule within a route map. The sequence of 1 indicates it is the first next hop to be tried for that rule. This is a running integer.	int	
HOP_TYPE	The Next hop type. 1 indicates INTERFACE, 2 indicates IP_ADDRESS, 3 indicates FLOOD VLAN.	smallint	
HOP_VALUE	Depending on the hop type the value can be an IP Address, Vlan id or Interface name.	varchar	64
PRESERVE_VLAN	0 indicates do not preserve vlan, 1 indicates preserve vlan.	smallint	

TABLE 268 PBR_POLICY

Field	Definition	Format	Size
ID	Primary key.	int	
POLICY_NAME	The name of the pbr policy.	varchar	81
IP_POLICY_TYPE	Defines the ip type of the policy, v4, v6 or both v4 and v6. Type v4 will have a value 1, type v6 will have a value 2, both will have a value 3.	smallint	
OPERATION_TYPE	Indicates the action to take on the policy. 1 means ADD, 2 means EDIT, 3 means DELETE.	smallint	
DEPLOYMENT_ID	ID of the deployment_configuration table entry.	int	

TABLE 269 PBR_RULE

Field	Definition	Format	Size
ID	Primary key.	int	
POLICY_ID	PBR policy ID.	int	
RULE_NAME	Name of the pbr rule.	varchar	127
ROUTE_MAP_SEQUENCE	The sequence of the route-map entry that corresponds to a rule within a route-map. The sequence of 1 indicates it is the first rule within the route map. This number will be incremented for every rule entry within a route-map.	int	
OPERATION_TYPE	Indicates the action to take on the rule. 1 is ADD, 2 is EDIT, 3 is DELETE.	smallint	

TABLE 270 PBR_RULE_ACL_LIST

Field	Definition	Format	Size
ID	The primary key of the table.	int	
RULE_ID	PBR_RULE id. This is a foreign key.	int	

TABLE 270 PBR_RULE_ACL_LIST (Continued)

Field	Definition	Format	Size
ACL_MATCH_SEQUENCE	The sequence of the matching acl entry that corresponds to a rule within a route map. The sequence of 1 indicates it is the first matching acl for that rule. This is a running integer.	int	
ACL_NAME	Name of the ACL for the rule.	varchar	81
ACL_TYPE	Indicates the ACL type. Value of 4 denotes IPV4, Value of 6 denotes IPV6.	smallint	

TABLE 271 PHANTOM_PORT

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
WWN	The Wwn of the phantom port.	char	23
VIRTUAL_SWITCH_ID	The id of the phantom switch.	int	
PORT_NUMBER	The port number of the phantom port. The default value is -1.	smallint	
PORT_ID	The portId of the phantom port. The default value is 000000.	varchar	8
SPEED	The speed of the phantom port. The default value is 0.	int	
MAX_SPEED	The max speed of the phantom port. The default value is 0.	int	
TYPE	The portType of the phantom port.The default value is 'Unknown'.	varchar	16
REMOTE_NODE_WWN	The remote node wwn(for E-ports only). Attached port device info must be retrieved from DevicePort table.	char	23
REMOTE_PORT_WWN	The remote port wwn(for E-ports only). Attached port device info must be retrieved from DevicePort table.	char	23
PHANTOM_TYPE	The phantom type of the port, either front or xlate	int	
BB_FABRIC_ID	Denotes the Backbone Fabric ID.	int	

TABLE 272 PHYSICAL_DEVICE

Field	Definition	Format	Size
PHYSICAL_DEVICE_ID	Unique generated database identifier.	int	
DEVICE_ID	Database identifier of the DEVICE instance.	int	
DESCRIPTION	System description of the device.	varchar	255
NUM_SLOTS	Number of slots present in the device.	num	(4,0)
TABLE_SUBTYPE	Table name where additional properties/attributes about this physical device stored. Possible value is FOUNDRY_PHYSICAL_DEVICE.	varchar	32
UNIT_NUMBER	Unit number in the stack if it is stackable device . For non-stacking device it will be always 0.	num	(2,0)

TABLE 272 PHYSICAL_DEVICE (Continued)

Field	Definition	Format	Size
UNIT_NEIGHBOR1	Stacking neighbor's unit(left) number for the stackable devices. If there is no neighbor unit/non stackable devices, then set to 0.	num	(2,0)
UNIT_NEIGHBOR2	Stacking neighbor's unit(left) number for the stackable devices . If there is no neighbor unit/non stackable devices, then set to 0.	num	(2,0)
UNIT_PRESENT	Used to identify the stack unit is present in the chassis or not. Present-1 and Not Present-2.	num	(1,0)

TABLE 273 PHYSICAL_INTERFACE

Field	Definition	Format	Size
INTERFACE_ID	Primary key for this table.	int	
PHYSICAL_PORT_ID	Foreign key which refers PHYSICAL_PORT table.	int	
SPEED_IN_MB	Interface speed in Mega Bytes.	int	
PHYSICAL_ADDRESS	MAC address of this interface.	varchar	64
LINK_ID	Foreign key which refers LINK table.	int	
DUPLEX_MODE	Interface duplex mode. Full/Half/Auto.	smallint	
IS_STACKING_INTERFACE	This flag is to indicate whether the interface is stacking interface or peri port. 0 indicates non-stacking, 1-indicates stacking interface, 2-indicates peri port.	num	(1,0)
IS_PORT_PRESENT	This flag is to indicate whether the port is presented in the device. 0 = Unknown 1 = Present 2 = Not present	int	
PHYSICAL_DEVICE_ID	For DCB switch, this is the core switch id. For IP products, this is the physical_device_id in physical_device table.	int	
UNIT_NUMBER	This is the unit number of which the interface is located for IP stacking products. If it is not applicable, the value is -1.	int	
SLOT_NUMBER	This is the slot number of which the interface is located for the devices and switches. If it is not applicable, the value is -1.	int	
PORT_NUMBER	This is the port number of the interface.	int	
PORT_TYPE	This column is used to store the port type of the interface. The value will be populated by the NosSwitchAssetCollector during the discovery of the VCS switch.The value of 0 means its edge port, and 1 means its trill port. Default value is 0.	smallint	
UNIT_TYPE	Indicates unit type in the stack. This column stores the model type of a stackable unit such as "ICX6610-48P". For non-stacking device it will be empty	varchar	64

TABLE 273 PHYSICAL_INTERFACE (Continued)

Field	Definition	Format	Size
IMAGE_VERSION	Image version of the unit in the stack. For non-stacking device it will be always empty.	varchar	
UNIT_ROLE	Indicates unit role in the stack. Possible values: 1 - other, 2 - active, 3 - standby, 4 - member, 5 - standalone. For non-stacking device it will be always -1'	int	
UNIT_PRIORITY	Indicates unit priority. Possible values 0 to 255. For non-stacking device it will be always -1	int	
UNIT_STATE	Used to identify unit state in the stack. Possible values: 1 - local, 2 - remote, 3 - reserved, 4 - empty. For non-stacking device it will be always -1	int	

TABLE 274 PHYSICAL_PORT

Field	Definition	Format	Size
PHYSICAL_PORT_ID	Database unique generated identifier.	int	
PORT_NUM	Port number from interface identifier.	smallint	
MODULE_ID	Database ID of the module which this port is present.	int	
IS_PORT_PRESENT	This flag is to indicate whether the port is presented in the device. Unknown-0, Present-1 and Not present -2.	smallint	
TABLE_SUBTYPE	PHYSICAL_PORT table sub type.	varchar	32

TABLE 275 PM_COLLECTOR_MEASURE_SETTING

Field	Definition	Format	Size
COLLECTOR_ID	ID of the data_collector.	int	
MEASURE_ID	ID of the measure.	int	

TABLE 276 PM_COLLECTOR_TARGET_SETTING

Field	Definition	Format	Size
COLLECTOR_ID	ID of the data_collector.	int	
TARGET_TYPE	Target type associated to the collector. Possible values are 12 - IP_DEVICE_GROUP and 14 - VIRTUAL_GROUP. To identify the exact target type, combination of TARGET_TYPE and TARGET_ID values are used.	smallint	
TARGET_ID	Target Id associated to the collector. Possible values are 1 - ALL_IOS_PRODUCTS, 2 - ALL_NOS_PRODUCTS, 3 - ALL_IP_TRUNK, 4 - ALL_TRILL_TRUNK, 5 - ALL_PHYSICAL_PORT, 6 - ALL_SAN_FC_PORT, 7 - ALL_SAN_TE_PORT, 8 - ALL_SAN_FCIP_TUNNEL, 9 - ALL_SAN_PRODUCT, 10 - ALL_SAN_EE_MONITOR.	int	

TABLE 276 PM_COLLECTOR_TARGET_SETTING (Continued)

Field	Definition	Format	Size
ME_ID	ME_ID of the target.	int	
INDEX_MAP	Stores the index_map value in case of an expression.	varchar	8192

TABLE 277 PM_COLLECTOR_TIME_SERIES_MAPPING

Field	Definition	Format	Size
COLLECTOR_ID	DB ID of the pm_data_collector.	int	
TARGET_NAME	Time series data master table name. It could be either TIME_SERIES_DATA_1 or TIME_SERIES_DATA_2.	varchar	63

TABLE 278 PM_DASHBOARD_WIDGET

Field	Definition	Format	Size
DASHBOARD_WIDGET_ID	Primary key column.	int	
TIME_SCOPE	Time in unit of seconds, for which the data has to be fetched from DB going back from now applicable for top N, distribution, and top Flow, time series.	int	
REFRESHING_INTERVAL	The widget refreshing interval in seconds, in 11.3 we will fix it at 600 (10 mins) and not expose it to user.	int	
MONITOR_TYPE	The widget refreshing interval in seconds, in 11.3 we will fix it at 600 (10 mins) and not expose it to user.	int	
MEASURE_TYPE	TYPE of the user selection measure.	int	
CREATE_USER_ID	ID of the user who created the widget definition.	int	
CREATE_TIME	Widget definition created server time.	timestamp	
MODIFY_USER_ID	ID of the user who last modifed the widget definition.	int	
MODIFY_TIME	Widget definition last modified server time.	timestamp	
TOP_OR_BOTTOM_N	The Top N setting for the Top N, Bottom N and Top XXX monitor TYPE, for other monitor TYPE, this field set to default value. Default is 0.	int	
LEVEL1_ENABLED	Enable / disable the threshold check for first percentage band. This value is applicable only for Top N, Top Flow widgets. Default is 0.	smallint	
LEVEL1_VALUE	Limit value for the first percentage band. Default is 0.	double precision	
LEVEL1_COLOR	RGB color for the first percentage band.	int	
LEVEL2_ENABLED	Enable / disable the second threshold check. This value is applicable only for Top N, Top Flow widgets. Default is 0.	smallint	
LEVEL2_VALUE	Limit value for the second percentage band. Default is 0.	double precision	
LEVEL2_COLOR	RGB color for the second percentage band.	int	

TABLE 278 PM_DASHBOARD_WIDGET (Continued)

Field	Definition	Format	Size
LEVEL3_ENABLED	Enable / disable the third threshold check. This value is applicable only for Top N, Top Flow widgets. Default is 0.	smallint	
LEVEL3_VALUE	Limit value for the third percentage band. Default is 0.	double precision	
LEVEL3_COLOR	Limit value for the third percentage band.	int	
LEVEL4_ENABLED	Enable / disable the fourth threshold check. This value is applicable only for Top N, Top Flow widgets. Default is 0.	smallint	
LEVEL4_VALUE	Limit value for the fourth percentage band. In case of Top N, Top Flow widgets only three percentage bands are available. This value is not applicable. Default is 0.	double precision	
LEVEL4_COLOR	RGB color for the fourth percentage band.In case of Top N, Top Flow widgets we will use this column to store the color value for other percentage band.	int	
LEVEL5_ENABLED	Enable / disable the fifth threshold check. This value is applicable only for Top N, Top Flow widgets. Default is 0.	smallint	
LEVEL5_VALUE	Limit value for the fifth percentage band. In case of Top N, Top Flow widgets only three percentage band s are available. This value is not applicable. Default is 0.	double precision	
LEVEL5_COLOR	RGB color for the fifth percentage band. In case of Top N, Top Flow widgets only three percentage bands are available. This value is not applicable.	int	
CATEGORY	Category of the dashboard monitor. 0 - System defined, 1 - User defined, 2 - Promoted from Historical Graph, 3 - Promoted from Real time Graph. Default is 0..	smallint	
GRAPH_ENABLED	Enable or disable the time series graph for Top n or Bottom n widgets. 0 = disabled, 1 = enabled.	smallint	
FILTER_CRITERIA	Stores the filter criteria to be applied on the selected measure for products or ports.	varchar	256
FILTER_VALUE	Stores the measure value to be used in the filter criteria.	double precision	
USE_DASHBOARD_SCOPE	Use Dashboard scope or widget scope. 0 - Widget scope, 1 - Dashboard scope.	smallint	
PORT_TYPE	Types of ports to use for port measure widgets: 0 - All Ports, 1 - ISL Ports, 2 - Host Ports, 3 - Storage Ports.	smallint	

TABLE 279 PM_DATA_COLLECTOR

Field	Definition	Format	Size
ID	Primary key column.	int	
NAME	The name of the collector definition.	varchar	128

TABLE 279 PM_DATA_COLLECTOR (Continued)

Field	Definition	Format	Size
STATUS	Status of the collector. 0 - disabled and 1 - enabled. Default - 0.	smallint	
TYPE	Target type of the snmp collector data. for device level collector the target type is 0, for port level it is 1.	smallint	
POLLING_INTERVAL	Time interval in seconds; indicates the frequency with which the collector will poll the device to get the data.	int	
CREATED_TIME	Collector created time.	timestamp	
CREATE_USER_ID	The user id who has created this collector.	int	
ENABLE_THRESHOLD	Widget definition created server time.	smallint	
THRESHOLD	Stores the threshold value.	double precision	
REARM	Stores the rearm value.	double precision	
THRESHOLD_OP	Stores the threshold operator value.	varchar	10
REARM_OP	Stores the rearm operator value.	varchar	10
IS_REARM_ABS	Whether or not the rearm. Default - 0.	smallint	
THRESHOLD_SEVERITY	The severity for the threshold event.	smallint	
REARM_SEVERITY	The severity for the rearm event.	smallint	
IS_SYSTEM	Indicates whether this is a system built in collector, user cannot delete it. Default - 1.	smallint	

TABLE 280 PM_MEASURE

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
DESCRIPTION	The description of the .	varchar	64
NAME	Name of the measure.	varchar	32

TABLE 281 PM_STATS_AGING_POLICY

Field	Definition	Format	Size
ID	Auto generated unique Identifier. Primary key for the table.	int	
RAW_SAMPLE_AGE	The maximum time in seconds for retaining records in the PM stats raw sample tables (TIME_SERIES_DATA_1 or TIME_SERIES_DATA_2) in database.	int	64
THIRTY_MIN_SAMPLE_AGE	The maximum time in seconds for retaining records in the PM stats 30min sample tables (TIME_SERIES_DATA_1_30MIN and TIME_SERIES_DATA_2_30MIN) in database.	int	

TABLE 281 PM_STATS_AGING_POLICY (Continued)

Field	Definition	Format	Size
TWO_HOUR_SAMPLE_AGE	The maximum time in seconds for retaining records in the PM stats 2hour sample tables (TIME_SERIES_DATA_1_2HOUR and TIME_SERIES_DATA_2_2HOUR) in database.	int	
ONE_DAY_SAMPLE_AGE	The maximum time in seconds for retaining records in the PM stats 1day sample tables (TIME_SERIES_DATA_1_1DAY, TIME_SERIES_DATA_2_1DAY) in database.	int	
POLICY_TYPE	Type of the aging policy. 100 is Default aging; 101 is Raw samples to 1 day.	int	
ACTIVE	State of the aging policy. 1 is Active, 0 is Inactive.	int	32

TABLE 282 PM_WIDGET_MEASURE_TYPE

Field	Definition	Format	Size
Type	Primary key column.	int	
NAME	Storing the NAME of the measure.	varchar	64

TABLE 283 PM_WIDGET_MEASURE_TYPE_ENTRY

Field	Definition	Format	Size
WIDGET_ID	The id of the widget definition.	int	
MEASURE_TYPE	stores measure type id of the widget, a widget could map to multiple measure types.	int	

TABLE 284 PM_WIDGET_MONITOR_TYPE

Field	Definition	Format	Size
Type	Primary key column.	int	
NAME	Storing the NAME of the monitor type.	varchar	64

TABLE 285 PM_WIDGET_TARGET_ENTRY

Field	Definition	Format	Size
WIDGET_ID	The ID of the widget definition.	int	
TARGET_TYPE	0 - Device 1 - Port	smallint	
TARGET_ID	Stores device ID if taret_TYPE is Device, or interface DB ID if target TYPE is port.	int	

TABLE 286 PM_WIDGET_TIME_SERIES_ENTRY

Field	Definition	Format	Size
WIDGET_ID	The ID of the widget definition.	int	
COLLECTOR_ID	ID of the PERF_COLLECTOR.	int	

TABLE 286 PM_WIDGET_TIME_SERIES_ENTRY (Continued)

Field	Definition	Format	Size
TARGET_TYPE	0 - Device 1 - Port	smallint	
TARGET_ID	Stores device ID if taret_TYPE is Device, or interface DB ID if target TYPE is port.	int	
MEASURE_ID	Measure table DB ID.	int	
MEASURE_INDEX	Index value for a MIB variable. For scalar value it will be empty.	varchar	256

TABLE 287 PM_WIDGET_TOP_N_COLLECTOR_ENTRY

Field	Definition	Format	Size
WIDGET_ID	The ID of the widget definition.	int	
COLLECTOR_ID	ID of the PERF_COLLECTOR.	int	
MEASURE_ID	Measure table DB ID.	int	
DIRECTION	The direction of the port measure. 0 - default (not used) 1 - receiving 2 -transmitting	smallint	

TABLE 288 PM_WIDGET_USER_ENTRY

Field	Definition	Format	Size
WIDGET_ID	The ID of the widget definition.	int	
USER_ID	ID of the user who is using the widget definition.	int	

TABLE 289 POE_THRESHOLD

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
TYPE	This field indicates if the threshold is defined for product and port level measure. • 0 = product level • 1 = port level	smallint	
DEVICE_ID	This is the foreign key reference key to the Device Table.	int	
INTERFACE_ID	This is the foreign key reference key to the Interface Table.	int	
ENABLED	Flag to indicate of defined threshold is enabled or not. • 0 = disabled • 1 = enabled	smallint	
VALUE	Value of the measure at which threshold is defined.	double precision	
INTERVAL	Time interval at which threshold is triggered.	int	
MEASURE	Product and port level poe measure definition.	smallint	

TABLE 289 POE_THRESHOLD (Continued)

Field	Definition	Format	Size
CONDITION	Condition like ><= to the defined threshold value at which threshold is triggered • 0 > (Greater Than) • 1 >= (Greater Than or Equal) • 2 < (Less Than) • 3 < = (Less Than or Equal) • 4 = (Equal to) • 5 != (Not Equal To)	smallint	
SEVERITY	Severity level of defined threshold on port and product Poe measures.	int	

TABLE 290 POE_THRESHOLD_EVENT

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
TIME_STAMP	This field indicates the time at which a particular threshold was triggered.	bigint	
THRESHOLD_ID	This is the foreign key reference key to the POE_THRESHOLD Table.	int	
EVENT_VALUE	Value of the measure at which threshold was triggered.	double precision	

TABLE 291 POLICY_RULE

Field	Definition	Format	Size
ID	Primary key for the table.	int	
NAME	Rule name.	varchar	255
DESCRIPTION	Rule description.	varchar	1024
TYPE	Policy Monitor rule type. For e.g. 1-zoning status check, 2-orphaned zone check, 3-fan in ratio check, 4- event registration check... 10-Configuration Rule, etc.	smallint	
CATEGORY	Policy Monitor rule category. For example, 0 - pre-defined, 1 - user-defined for configuration rule check.	smallint	

TABLE 292 POLICY_RULE_MAP

Field	Definition	Format	Size
ID	Primary key for the table.	int	
DEPLOYMENT_CONFIGURATION_ID	Foreign key reference to DEPLOYMENT_CONFIGURATION.ID.	int	
POLICY_RULE_ID	Foreign key reference to POLICY_RULE.ID.	int	
ATTRIBUTES	Attributes for pre-canned rules, this is name value pair string, use & as delimiter. For example minConn=2&maxConn=5.	varchar	255

TABLE 293 PORT_BOTTLENECK_CONFIG

Field	Definition	Format	Size
SWITCH_PORT_ID	The database ID of the switch port that the configuration belongs to.	int	
BOTTLENECK_DETECT_ENABLED	Flag indicates if bottleneck detection is enabled or not. The default value is 0.	smallint	
ALERTS_ENABLED	Flag indicates if bottleneck detection alerts is enabled or not.The default value is -1.	smallint	
CONGESTION_ THRESHOLD	Value of bottleneck detection congestion threshold in percent. The default value is -1.	double precision	
LATENCY_THRESHOLD	Value of bottleneck detection latency threshold in percent. The default value is -1.	double precision	
LATENCY_SEVERITY	The factor by which throughput must drop in a second in order for that second to be considered affected by latency bottlenecking. Range (1 to 1000).	int	
LATENCY_TIME	The minimum fraction of a second that must be affected by latency in order for that second to be considered affected by latency bottlenecking. Range (0 to 1).	double precision	
WINDOW_	Value of bottleneck detection latency window in millisecond. The default value is 0.	int	
QUIET_TIME	Value of bottleneck detection quiet time in millisecond. The default value is 0.	int	
CREATION_TIME	Creation time of the record.	timestamp	
LAST_UPDATE_TIME	Last update time of the record.	timestamp	

TABLE 294 PORT_BOTTLENECK_STATUS

Field	Definition	Format	Size
SWITCH_PORT_ID	The database ID of the switch port that the status belongs to.	int	
STATUS	Flag indicates bottleneck status of the switch port.	smallint	

TABLE 295 PORT_COMMISSION_CIMOM_SERVER

Field	Definition	Format	Size
ID	Primary key for the table.	int	
DESCRIPTION	User defined description of the CIMOM Server.	varchar	1024
NETWORK_ADDRESS	IPv4 or IPv6 address or Host name of the CIMOM server.	varchar	64
CIM_NAMESPACE	Name of the namespace where this CIM_FCPort CIM Class is located.	varchar	256
PORT	Port number which CIMOM server is listening.	int	
SSL_ENABLED	Protocol used for connecting CIMOM server. Default protocol will be HTTPS. If HTTPS is not reachable fall back to HTTP. Supported values 0 - HTTP, 1 - HTTPS	int	
USER_ID	User Id to be used for authenticating CIMOM Server.	varchar	128

TABLE 295 PORT_COMMISSION_CIMOM_SERVER (Continued)

Field	Definition	Format	Size
PASSWORD	Password to be used for authenticating. Stored in encrypted format.	varchar	512
STATUS	Status before and after contacting the CIMOM Server. Possible values are 0 - OK, 1- Not Contacted Yet , 2 - Credentials Updated, 3 - Credentials Failed, 4 - Not Reachable.	int	
LAST_CONTACTED_TIME	Last time CIMOM server contacted. This will be updated when we test the reachablity of the CIMOM Server and when we perform port decommission/recommission.	timestamp	
ERROR_MESSAGE	Detailed error message. Applicable when communication to CIMOM Server failed.	varchar	2048

TABLE 296 PORT_FENCING_POLICY

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
NAME	Name of the policy. The length of the field should be 62 because M-Model switch supports only maximum 62 characters.	varchar	62
TYPE	• 0 = ISL Protocol • 1 = Link • 2 = Security	smallint	
THRESHOLD_LIMIT	Threshold Limits for M-Model Switch.	int	
THRESHOLD_DURATION	Duration In minutes for M-Model Switch.	int	
DEFAULT_POLICY	• 1 = the default port fencing policies. • 0 = the non-default policies. The default port fencing policies are: For ISL - Default Protocol Error Policy For Link Violation type - Default Link Level Policy For Security - Default Security Policy	smallint	
B_THRESHOLD_LIMIT	Threshold Limits for B-Model Switch (Not Supported).	int	
B_THRESHOLD_DURATION	Duration in minutes for B-Model Switch (Not Supported).	int	

TABLE 297 PORT_FENCING_POLICY_MAP

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
POLICY_ID	Foreign key to ID column of PORT_FENCING_POLICY table.	int	
LEVEL	• 0 = All Fabric • 1 = Fabric • 2 = Core Switch Group • 3 = Switch • 4 = Port Type • 5 = Port List	smallint	

TABLE 297 PORT_FENCING_POLICY_MAP (Continued)

Field	Definition	Format	Size
SUB_LEVEL	• 1 = E_Port • 2 = F_Port • 3 = FL_Port, Fabric WWN, Switch WWN	char	23
NODE	WWN of Node which policy assigned.	char	23
INHERITANCE	Directly assigned or inherited from root level. • 0 = Directly assigned • 1 = Indirectly assigned	smallint	

TABLE 298 PORT_PROFILE

Field	Definition	Format	Size
ID	Auto generated id for the created profile	int	
SWITCH_ME_ID	Incase of a VCS discovery in M/C mode this is the cluster meid. Incase of VCS discovery in F/C mode, this is a member ID. Incase of a VDX this is a member ID	int	
NAME	Name of the port profile	varchar	255
SWITCH_PORT_MODE	Mode for vlan configuration it can be 0=access 1= trunk 2= converged	smallint	
STATE	Profile state 0=created 1=activate	smallint	
ACL_PROFILE	If port Profile has an acl profile or not. 0=NO 1=YES	smallint	
QOS_PROFILE	If port Profile has an qos profile or not. 0=NO 1=YES	smallint	
VLAN_PROFILE	If port Profile has an vlan profile or not.0=NO 1=YES	smallint	
VLAN_DETAILS	This column lists the way vlan is configured 0=NONE 1=ALL 2=SELECTED 3=EXC EPT	smallint	
DEFAULT_PROFILE	This flag determines if this profile is a default profile.0=NO 1=YES	smallint	
ACL_NAME	Name of the mapped ACL	varchar	255
ACTIVATED	Profile activated 0= false 1=true	smallint	
FCOE_PROFILE	If port Profile has an fcoe profile or not. • 0=NO • 1=YES	smallint	
FCOE_MAP_NAME	Name of the FCoE Map.	varchar	255

TABLE 299 PORT_PROFILE_DOMAIN

Field	Definition	Format	Size
ID	Sequence number of the records.	int	
ME_ID	Foreign Key Reference to ID field of MANAGED_ELEMENT table.	int	

TABLE 299 PORT_PROFILE_DOMAIN

Field	Definition	Format	Size
NAME	Name of the port profile domain.	varchar	255
DEFAULT_DOMAIN	This flag determines if this domain is a default domain. 0 - NO 1 - YES	smallint	

TABLE 300 PORT_PROFILE_DOMAIN_MAP

Field	Definition	Format	Size
PROFILE_DOMAIN_ID	Foreign Key Reference to ID field of PORT_PROFILE_DOMAIN table.	int	
PROFILE_ID	Foreign Key Reference to ID field of PORT_PROFILE table.	int	

TABLE 301 PORT_PROFILE_INTERFACE_MAP

Field	Definition	Format	Size
ID	Auto generated ID for the created profile	int	
PROFILE_ID	DB id of the port profile	int	
SWITCH_ME_ID	Managed element id of the cluster and its cluster members and a stand alone calisto	int	
INTERFACE_ID	ID of the interface table	int	
SWITCH_PORT_ID	Db id of the Switch port with matching interface	int	

TABLE 302 PORT_PROFILE_MAC_MAP

Field	Definition	Format	Size
ID	Auto generated ID for the created profile	int	
PROFILE_ID	DB id of the port profile	int	
MAC	Mac address mapped to the port profile	varchar	32
NAME	User assigned name to the mac	varchar	256

TABLE 303 PORT_PROFILE_QOS_MAP

Field	Definition	Format	Size
ID	Auto-generated ID for the created profile	int	
PROFILE_ID	DB ID of the port profile	int	
DCB_MODE	If the mode is dcb or non dcb. 1 : DCB.0: NON-DCB	smallint	
ETHERNET_MODE	This integer indicates if pause of priority flow control is set.0: PAUSE 1: PFC	smallint	
PAUSE_TX	Is PAUSE TX is enabled 0=NO 1=YES	smallint	
PAUSE_RX	Is PAUSE RX is enabled 0=NO 1=YES	smallint	
COS_COS	Name of the cos 2 cos map set in the NON DCB mode	varchar	256

TABLE 303 PORT_PROFILE_QOS_MAP

Field	Definition	Format	Size
TRAFFIC_CLASS	Name of the traffic class map set in the NON DCB mode	varchar	256
CEE_MAP	Name of the cee map set in the DCB mode	varchar	256
COS	Default COS value for QoS Profile can range from 0-7 if set	int	
TRUST_COS	Is trust cos enabled 0=NO 1=YES	smallint	

TABLE 304 PORT_PROFILE_QOS_PFC_MAP

Field	Definition	Format	Size
ID	Auto generated id for the created profile	int	
PROFILE_ID	DB id of the port profile	int	
COS0_TX	TX setting for this cos field 0: NO 1: YES	smallint	
COS0_RX	RX setting for this cos field 0: NO 1: YES	smallint	
COS1_TX	TX setting for this cos field 0: NO 1: YES	smallint	
COS1_RX	RX setting for this cos field 0: NO 1: YES	smallint	
COS2_TX	TX setting for this cos field 0: NO 1: YES	smallint	
COS3_TX	TX setting for this cos field 0: NO 1: YES	smallint	
COS3_RX	RX setting for this cos field 0: NO 1: YES	smallint	
COS4_TX	TX setting for this cos field 0: NO 1: YES	smallint	
COS4_RX	RX setting for this cos field 0: NO 1: YES	smallint	
COS5_TX	TX setting for this cos field 0: NO 1: YES	smallint	
COS5_RX	RX setting for this cos field 0: NO 1: YES	smallint	
COS2_RX	RX setting for this cos field 0: NO 1: YES	smallint	
COS6_TX	TX setting for this cos field 0: NO 1: YES	smallint	
COS6_RX	RX setting for this cos field 0: NO 1: YES	smallint	
COS7_TX	TX setting for this cos field 0: NO 1: YES	smallint	
COS7_RX	RX setting for this cos field 0: NO 1: YES	smallint	

TABLE 305 PORT_PROFILE_VLAN_MAP

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
PROFILE_ID	DB id of the port profile.	int	
VLANID	Configured vlan id on the switch.	int	
VLAN_TYPE	Type of this vlan, 0 : access 1: trunk.	int	

TABLE 305 PORT_PROFILE_VLAN_MAP

Field	Definition	Format	Size
MAC_GROUP_DB_ID	Nullable Foreign Key Reference to ID field of MAC_GROUP table. In case of VLAN_TYPE 3, MAC_GROUP table entry created with empty GROUP_ID with TYPE 3 and MAC_GROUP_MEMBER have the mac address details. In case of VLAN_TYPE 4, MAC_GROUP table entry created with valid GROUP_ID and TYPE(3).	int	
CTAG_ID	This will be populated only if VLAN_TYPE is 6 and 7. This as an Incoming customer tag (c-tag) associated with a GVLAN and its applicable only for trunk mode. If the TLS (Transparent LAN Service) is enabled in the device, a pre-defined range of values are used for C-Tag.	text	

TABLE 306 PORT_VLAN

Field	Definition	Format	Size
VLAN_DB_ID	Database ID of the VLAN instance which is associated with the port.	int	
STP	STP value for VLAN. Possible values are 0-Disabled, 1-STP, 2-RSTP, 3-MSTP, 4-PVST and 5-RPVST.	num	(1,0)
TVF	0 means Disabled, 1 means Enabled. When TVF is enabled, packets are allowed to be forwarded without any form of CPU intervention including MAC learning and MAC destination lookups. When it is disabled (VLAN CPU Protection), it allows traffic intended for pure Layer2.	smallint	
VLAN_ID	The existing Data type short has been modified to integer. Hence it supports 16 bit additionally.	smallint	
QOS	Quality of service for port VLAN.	smallint	
GLOBAL_VLAN_DB_ID	Database ID of the GLOBAL_VLAN instance which is associated with the port.	int	
STP_INSTANCE_ID	Database ID of the STP_INSTANCE instance which is associated with the port.	int	
ADMIN_STATUS	• 0 = Disabled • 1 = Enabled	smallint	
FCOE_ENABLED	Signifies whether this VLAN is the default FCoE VLAN on the DCB switch.	smallint	
PVLAN_TYPE	pvlan_type value for vlan.0- Normal VLAN. The following are PVLAN Types applicable for NOS4.0 and above.1- Primary PVLAN, 2- RSPAN, 3 -TLS..	int	

TABLE 306 PORT_VLAN (Continued)

Field	Definition	Format	Size
PRIMARY_VLAN_ID	Private VLAN domain is built with one primary VLAN and one or more secondary VLANs. This column represents primary VLAN ID associated with this secondary Isolated/Community VLAN (if PVLAN_TYPE column value is 2 or 3) in private VLAN domain. For primary VLAN (if PVLAN_TYPE column value is 1) in private VLAN domain and normal VLAN (if PVLAN_TYPE column value is 0) , then default value (i.e 0) will be populated.	int	
TLS_ID	It represents Transparent LAN Service id and its supported range is 1-1000 in GVLAN. The TLS and VLAN are one-one mapping.	int	

TABLE 307 PRIVILEGE

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
NAME	Privilege Name.	varchar	128
AREA	Privilege Area. 0= Application 1= SAN 2= IP	smallint	

TABLE 308 PRODUCT_APP

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
MENU_TEXT	Name of the product menu.	varchar	256
PROP1_KEY	First condition name to be satisfied by a selected product to launch a particular tool.	varchar	256
PROP1_VALUE	First condition value to be satisfied by a selected product to launch a particular tool.	varchar	256
PROP2_KEY	Second condition name to be satisfied by a selected product to launch a particular tool.	varchar	256
PROP2_VALUE	Second condition value to be satisfied by a selected product to launch a particular tool.	varchar	256
TOOL_ID	The tool to be used for launching the application.	int	
PARAMETERS	Link to that application.	varchar	256
IP_SELECTED	Selected IP Address option.	smallint	
WWN_SELECTED	Selected WWN option.	smallint	

TABLE 309 PROTOCOL_VLAN

Field	Definition	Format	Size
VLAN_DB_ID	Database ID of the VLAN instance which is associated with the protocol.	int	
PROTOCOL	Protocol for VLAN. Possible values are 1-IP, 2-IPX, 3-AppleTalk, 4-DECnet, 5-NetBIOS, 6-Other and 7-IPv6.	num	(4,0)

TABLE 310 QRTZ_BLOB_TRIGGERS

Field	Definition	Format	Size
TRIGGER_NAME*	Name of the trigger.	varchar	80
TRIGGER_GROUP*	Name of the trigger group.	varchar	80
BLOB_DATA	The Scheduler info.	bytea	

TABLE 311 QRTZ_CALENDARS

Field	Definition	Format	Size
CALENDAR_NAME*	Name of the Calendar.	varchar	80
CALENDAR	Calendar object.	bytea	

TABLE 312 QRTZ_CRON_TRIGGERS

Field	Definition	Format	Size
TRIGGER_NAME*	Name of the trigger.	varchar	80
TRIGGER_GROUP*	Name of the trigger group.	varchar	80
CRON_EXPRESSION	The CRON trigger Expression (ex:"0 0 12 * * ?" - meaning:Fire at 12pm (noon) every day).	varchar	80
TIME_ZONE_ID	Given "cron" expression resolved with respect to the TimeZone.	varchar	80

TABLE 313 QRTZ_FIRED_TRIGGERS

Field	Definition	Format	size
ENTRY_ID*	Fired instance ID.	varchar	95
TRIGGER_NAME	Name of the trigger.	varchar	80
TRIGGER_GROUP	Name of the trigger group.	varchar	80
IS_VOLATILE	Whether the job should not be persisted in the JobStore for re-use after the program restarts.	boolean	
INSTANCE_NAME	Trigger instance name.	varchar	80
FIRED_TIME	The trigger fired time.	num	(13,0)
STATE	The fired trigger job state.	varchar	16
JOB_NAME	Name of the job.	varchar	80
JOB_GROUP	Name of the job group.	varchar	80

TABLE 313 QRTZ_FIRED_TRIGGERS (Continued)

Field	Definition	Format	size
IS_STATEFUL	Whether the job implements the interface StatefulJob.	boolean	
REQUESTS_RECOVERY	True or false.	boolean	

TABLE 314 QRTZ_JOB_DETAILS

Field	Definition	Format	Size
JOB_NAME*	Name of the job.	varchar	80
JOB_GROUP*	Name of the job group.	varchar	80
DESCRIPTION	Description of the job (optional).	varchar	120
JOB_CLASS_NAME	The instance of the job that will be executed.	varchar	128
IS_DURABLE	Whether the job should remain stored after it is orphaned.	boolean	
IS_VOLATILE	Whether the job should not be persisted in the JobStore for re-use after program restarts.	boolean	
IS_STATEFUL	Whether the job implements the interface StatefulJob.	boolean	
REQUESTS_RECOVERY	Instructs the scheduler whether or not the job should be re-executed if a "recovery" or "fail-over" situation is encountered.	boolean	
JOB_DATA	To persist the job-related and application-related informations.	bytea	

TABLE 315 QRTZ_JOB_LISTENERS

Field	Definition	Format	Size
JOB_NAME*	Name of the job.	varchar	80
JOB_GROUP*	Name of the job group.	varchar	80
JOB_LISTENER*	Job listener action class instance.	varchar	80

TABLE 316 QRTZ_LOCKS

Field	Definition	Format	Size
LOCK_NAME*	Resource identification name assigned by user.	varchar	40

TABLE 317 QRTZ_PAUSED_TRIGGER_GRPS

Field	Definition	Format	Size
TRIGGER_GROUP*	Name of the trigger group.	varchar	80

TABLE 318 QRTZ_SCHEDULER_STATE

Field	Definition	Format	Size
INSTANCE_NAME*	Instance of the scheduler.	varchar	80
LAST_CHECKIN_TIME	Last fired time in milliseconds.	num	(13,0)

TABLE 318 QRTZ_SCHEDULER_STATE (Continued)

Field	Definition	Format	Size
CHECKIN_INTERVAL	Repeat interval.	num	(13,0)
RECOVERER	Misfire instruction.	varchar	80

TABLE 319 QRTZ_SIMPLE_TRIGGERS

Field	Definition	Format	size
TRIGGER_NAME*	Name of the trigger	varchar	80
TRIGGER_GROUP*	name of the trigger group	varchar	80
REPEAT_COUNT	number of times to repeat	num	(13,0)
REPEAT_INTERVAL	interval for first and second job	num	(13,0)
TIMES_TRIGGERED	Number of times the corresponding trigger fired	num	(13,0)

TABLE 320 QRTZ_JTRIGGER_LISTENERS

Field	Definition	Format	Size
TRIGGER_NAME*	Name of the trigger.	varchar	80
TRIGGER_GROUP*	Name of the trigger group.	varchar	80
TRIGGER_LISTENER*	The listener action.	varchar	80

TABLE 321 QRTZ_TRIGGERS

Field	Definition	Format	Size
TRIGGER_NAME*	Name of the trigger.	varchar	80
TRIGGER_GROUP*	Name of the trigger group.	varchar	80
JOB_NAME	Name of the job.	varchar	80
JOB_GROUP	Name of the job group.	varchar	80
IS_VOLATILE	Whether the trigger should be persisted in the JobStore for re-use after program restarts.	boolean	
DESCRIPTION	A description for the trigger instance - may be useful for remembering/displaying the purpose of the trigger, though the description has no meaning to Quartz.	varchar	120
NEXT_FIRE_TIME	The next fire time in milliseconds.	num	(13,0)
PREV_FIRE_TIME	The previous fired time in milliseconds.	num	(13,0)
TRIGGER_STATE	The state of the trigger (viz. Error, wait,etc.)	varchar	16
TRIGGER_TYPE	The type of the trigger (Simple,cron).	varchar	8
START_TIME	The job start time.	num	(13,0)
END_TIME	The job end time (-1 means infinite).	num	(13,0)
CALENDAR_NAME		varchar	80
MISFIRE_INSTR	Instructs the scheduler to execute the misfired job.	smallint	
JOB_DATA	Persists the job-related info.	bytea	

TABLE 322 QUERY_BASED_DEVICE_GROUP

Field	Definition	Format	Size
DEVICE_GROUP_ID		int	
QUERY_TEXT		varchar	4096
GROUP_CRITERIA	Holds the dynamic device group criteria XML value.	varchar	4096

TABLE 323 QUORUM_CARD_GROUP_MAPPING

Field	Definition	Format	Size
ID*		int	
ENCRYPTION_GROUP_ID	Foreign key reference to the ENCRYPTION_GROUP for which an authorization card is registered.	int	
SMART_CARD_ID	Foreign key reference to the SMART_CARD that is registered as an authorization card for the encryption group.	int	

TABLE 324 RAS_LOG

Field	Definition	Format	Size
MSG_ID*	Message ID of the event.	varchar	15
MODULE_ID	Module ID of the event.	varchar	10
SEVERITY	Severity of the event.	varchar	10
CAUSE	Probable root cause for the event.	varchar	4096
ACTION	Recommended action for the event.	varchar	4096
OLD_MSG_ID	Old message ID.	varchar	45

TABLE 325 RECIPIENT_TYPE

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
TYPE	Type of the recipient (Syslog or SNMP).	varchar	20

TABLE 326 RECOVERY_CARD_GROUP_MAPPING

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
ENCRYPTION_GROUP_ID	Foreign key reference to the ENCRYPTION_GROUP for which a recovery card is registered.	int	
SMART_CARD_ID	Foreign key reference to the SMART_CARD that is registered as a recovery card for the encryption group.	int	
POSITION_	The position of the card within the recovery card set. 1 = first card, 2 = second card, etc.	int	

TABLE 327 REPORT_TYPE

Field	Definition	Format	Size
ID*	Meta Data for available reports.	int	
NAME	Report name.	varchar	128
DESCRIPTION	Report type description.	varchar	256

TABLE 328 REPORT_TEMPLATE

Field	Definition	Format	Size
ID	The primary key of the table.	int	
NAME	Name of the report and the report names must be descriptive. For example, Wired Device Report.	varchar	256
TITLE	The title of the report that briefly describes the report contents. This title will also be used for the report header and menu item. Title should be unique. For example, Wired Products List.	varchar	256
CREATED_TIME	Timestamp of when the report was created.	timestamp	
CREATED_BY	Foreign key to the user table, to identify which user created the report.	int	
REPORT_TYPE	0 = Precanned template which will not be deleted or edited, 1 = Editable report which can be deleted as well, 2 = Not Editable report but can be deleted.	int	
REPORT_DEFINITION	XML representation of the report.	text	

TABLE 329 REPORT_DRILLDOWN_TEMPLATE

Field	Definition	Format	Size
ID*	The primary key of the table.	int	
REPORT_TEMPLATE_ID	References the ID column in the REPORT_TEMPLATE table.	int	
NAME	Name of the report. Names should be descriptive so users will know exactly what kind of report they will be running or scheduling. E.g. Wired Device Report.	varchar	256
REPORT_DRILLDOWN_DEFINITION	XML representation of the report.	text	

TABLE 330 RESOURCE_FABRIC_MAP

Field	Definition	Format	Size
RESOURCE_GROUP_ID*	Resource group ID.	int	
FABRIC_ID*	Fabric ID, which is in the resource group.	int	

TABLE 331 RESOURCE_GROUP

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	

TABLE 331 RESOURCE_GROUP (Continued)

Field	Definition	Format	Size
NAME	Resource group name.	varchar	128
DESCRIPTION	Resource group description.	varchar	512

TABLE 332 RESOURCE_HOST_MAP

Field	Definition	Format	Size
RESOURCE_GROUP_ID	Resource Group ID	int	
HOST_ID	HOST_ID,which is in the resource group	int	

TABLE 333 ROLE

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
NAME	Role name.	varchar	128
DESCRIPTION	Role description.	varchar	512
HIDDEN	Field to identify whether the role is Hidden from users or not. Values: • 0= Not Hidden • 1= Hidden Currently, only "All Users" Role is hidden and other roles are visible to user. Default value is 0.	smallint	

TABLE 334 ROLE_PRIVILEGE_MAP

Field	Definition	Format	Size
ROLE_ID*	User role ID.	int	
PRIVILEGE_ID*	Privilege ID.	int	
PERMISSION	Privilege permission: 1 = RO 2 = RW 0 = No privilege Default value is 0.	smallint	

TABLE 335 RULE_BLOCK_MAP

Field	Definition	Format	Size
POLICY_RULE_ID	Foreign key reference to POLICY_RULE.ID.	int	
CONFIG_BLOCK_ID	Foreign key reference to CONFIG_BLOCK.ID.	int	

TABLE 336 RULE_CONDITION_MAP

Field	Definition	Format	Size
POLICY_RULE_ID	Foreign key reference to POLICY_RULE.ID.	int	
CONFIG_CONDITION_ID	Foreign key reference to CONFIG_CONDITION.ID.	int	

TABLE 337 RULE_LOGICAL_EXPRESSION_MAP

Field	Definition	Format	Size
POLICY_RULE_ID	Policy rule ID.	int	
LOGICAL_EXPRESSION_XML	Configuration Rule Logical Expression XML.	text	

TABLE 338 SAN

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
NAME	Name of this SAN.	varchar	256
CONTACT	Contact person for this SAN.	varchar	256
LOCATION	Location of this SAN.	varchar	256
DESCRIPTION	Description.	varchar	256
STATS_COLLECTION	1 = statistics collection is enabled; otherwise, 0. Default value is 0.	smallint	
CREATION_TIME	time at which this record was created. Default value is 'now()'.	timestamp	
LAST_UPDATE_TIME	time when this was last updated. Default value is 'now()'.	timestamp	

TABLE 339 SAN_CONNECTION

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
SOURCE_SWITCH_ID	Foreign key to VIRTUAL_SWITCH table. This is the virtual switch ID of AG	int	
SOURCE_PORT_ID	Foreign key to SWITCH_PORT table. This is the switch port id of N-port	int	
SOURCE_PORT_WWN	WWN of the AG N port	varchar	32
SOURCE_PORT_TYPE	Type of source port	varchar	16
SOURCE_USER_PORT_NUMBER	User port number of AG N port	smallint	
DESTINATION_SWITCH_ID	Foreign key to VIRTUAL_SWITCH table. This is the virtual switch ID of edge switch	int	
DESTINATION_PORT_ID	Foreign key to SWITCH_PORT table. This is the switch port id of F-port	int	
DESTINATION_PORT_WWN	WWN of the F port	varchar	23
DESTINATION_PORT_TYPE	Type of destination port	varchar	16
DESTINATION_USER_PORT_NUMBER	User port number of F-port	smallint	
FABRIC_ID	Foreign key to FABRIC table	int	
TRUSTED	Indicates if the connection is trusted	smallint	
MISSING	Indicates if the connection is missing	smallint	

TABLE 339 SAN_CONNECTION (Continued)

Field	Definition	Format	Size
MISSING_TIME	Timestamp when the connection went missing	timestamp	
LAST_UPDATE_TIME	Last update time for this record	timestamp	
CREATION_TIME	Creation timestamp	timestamp	

TABLE 340 SCOM_HOST

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
HOST	The FQDN or the ip address of the host	varchar	256
DOMAIN	The domain of the SCOM server host	varchar	256
USER_NAME	The domain user to login into the SCOM Server	varchar	64
PASSWORD	The password to login into the SCOM Server	varchar	64
VERSION	The version of SCOM. Default is 6.1.7221.0 which is SCOM 2007 R2. The default value is '6.1.7221.0' .	varchar	32
TOKEN_ID	Unique ID for each SCOM host	varchar	32
STATUS	Status of Plug-in registration to the SCOM server where 0-registered, 1-unregistered, 2-authentication failed, 3-not reachable	int	

TABLE 341 SECURITY_POLICY

Field	Definition	Format	Size
VIRTUAL_SWITCH_ID *	DB ID of virtual_switch.	int	
POLICY_NUMBER*	IPSec Policy Number. The number can range from 1 to 32.	smallint	
POLICY_TYPE*	Type of the Policy. The possible values are IKE or IPSec	smallint	
ENCRYPTION_ALGORITHM	Encryption Algorithm for the policy.The following are the possible Encryption: NONE,DES,3DES,AES-128,AES-256,AES-CM-128 or AES-CM-256.	varchar	32
AUTHENTICATION_ALGORITHM	Authentication Algorithm for the policy: NONE SHA-1 MD5 AES-XCBC	varchar	32
PERFECT_FORWARD_POLICY_ENABLED	Perfect Forward Secrecy for the policy. The possible values are 0 or 1.	smallint	
DIFFIE_HELLMAN_GROUP	Diffie-Hellman Group used in PFS negotiation.	smallint	
SECURITY_ASSOC_LIFE	Association lifetime in seconds.	double precision	
SECURITY_ASSOC_LIFE_IN_MB	Security association lifetime in megabytes.	double precision	

TABLE 342 SELECTED_FLYOVER_PROPERTY

Field	Definition	Format	Size
PROPERTY_ID*	Refers to Flyover_Property ID from AVAILABLE_FLYOVER_PROPERTY table.	int	
USER_NAME*	The name of the user who selected the property to be shown on flyover.	varchar	128
POSITION_	The user preferred position of the selected flyover property.	int	

TABLE 343 SENSOR

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
CORE_SWITCH_ID		int	
SENSOR_ID	Identifies the sensor device , requested by SMIA and values filled in by Switch Asset Collector. Maps to Device Id in the html page. The default value is -1.	int	
CURRENT_READING	Identifies the current temperature reading sensor, requested by SMIA and values filled in by Switch Asset Collector, Maps to value field in the html page. The default value is -1.	bigint	
TYPE	The default value is -1.	int	
SUB_TYPE	The default value is -1.	int	
DESCRIPTION	Provides the description of the temperature sensor, requested by SMIA and values filled in by Switch Asset Collector	varchar	128
STATUS	provides the status of the sensor, requested by SMIA and values filled in by Switch Asset Collector,Values could be 0 or 1. 0 means faulty and 1 is ok.The default value is -1.	int	
OPERATIONAL_STATUS	provides the operational status of the sensor, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above. The default value is -1.	int	
PART_NUMBER	provides the part number of the sensor, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above	varchar	64
SERIAL_NUMBER	provides the serial number of the sensor, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above	varchar	64
VERSION	provides the version of the sensor, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above	varchar	32

TABLE 343 SENSOR (Continued)

Field	Definition	Format	Size
CREATION_TIME	provides the record creation time, standard columns for Management application and values filled in by Switch Asset Collector	timestamp	
LAST_UPDATE_TIME	provides the record last updated time, standard columns for Management application and values filled in by Switch Asset Collector	timestamp	
FRU_TYPE	provides the type of the sensor, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above. The values represents FAN,PS, SLOT etc. The default value is -1.	int	
UNIT_NUMBER	provides the unit number of the sensor, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above . This the gives the index of the unit. For SLOT FRU, this will be slot number. For FAN fru, this will be fan number. The default value is -1.	int	
STATE	provides the state of the sensor, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above. This gives the value whether the FRU is On or Off . The default value is -1.	int	

TABLE 344 SFLOW_CHECKPOINT

Field	Definition	Format	Size
TABLE_TO_DROP	Staging child tables previously checkpointed (indicating that their aggregation was completed).	varchar	40

TABLE 345 SFLOW_HOUR_SUMMARY

Field	Definition	Format	Size
SLNUM	This column is used to store a counter value to identify the total row count.	bigserial	
TIME_IN_SECONDS	Data collection time in seconds.	int	
DEVICE_ID	ID of the product which sends the sflow traffic.	int	
IN_UNIT	Unit number of the incoming traffic interface. Default value is 0.	smallint	
IN_SLOT	Slot number of the incoming traffic interface.	smallint	
IN_PORT	Port number of the incoming traffic interface.	smallint	
OUT_UNIT	Unit number of the outgoing traffic interface. Default value is 0.	smallint	
OUT_SLOT	Slot number of the outgoing traffic interface.	smallint	
OUT_PORT	Port number of the outgoing traffic interface.	smallint	
IN_VLAN	Vlan ID of the incoming traffic interface.	smallint	
OUT_VLAN	Vlan ID of the outgoing traffic interface.	smallint	

TABLE 345 SFLOW_HOUR_SUMMARY

Field	Definition	Format	Size
IN_PRIORITY	Priority ID of the incoming traffic interface.	smallint	
OUT_PRIORITY	Priority ID of the outgoing traffic interface.	smallint	
SRC_MAC	MAC address of the source in the received sFlow packet.	byte	
DEST_MAC	MAC address of the destination in the received sFlow packet.	byte	
L3_SRC_ADDR	L3 address of the source in the received sFlow packet.	byte	
L3_DEST_ADDR	L3 address of the destination in the received sFlow packet.	byte	
L3_PROTOCOL	L3 protocol value in the received sFlow packet. For example, ARP.	int	
IP_TOS	Type of service id in the received sFlow packet.	smallint	
L4_PROTOCOL	L4 protocol value in the received sFlow packet. For example, IGP	smallint	
L4_SRC_PORT	L4 source port number in the received sFlow packet.	int	
L4_DEST_PORT	L4 destination port number in the received sFlow packet.	int	
SRC_SUBNET_BITS	Subnet value of the incoming traffic interface.	smallint	
DEST_SUBNET_BITS	Subnet value of the outgoing traffic interface.	smallint	
LOCAL_AS	Second AS number of the received sFlow packet in case of BGP traffic.	bigint	
SRC_AS	Source AS number of the received sFlow packet in case of BGP traffic.	bigint	
SRC_PEER_AS	Peer AS number of the received sFlow packet in case of BGP traffic.	bigint	
SFLOW_IP_ROUTE_INFO_ID	route_info_id of the received sFlow packet in case of BGP traffic.	int	
IP_FLOW_LABEL	IP flow label value in the received sFlow packet.	int	
SRC_USER	Name of the Source user in the received sFlow packet.	int	
DEST_USER	Name of the destination user in the received sFlow packet.	int	
FRAMES	Number of frames transmitted through the sFlow sample collected.	bigint	
BYTES	Number of bytes transmitted through the sFlow sample collected.	bigint	
TCP_FLAGS	TCP flag value of the received sFlow packet.	smallint	

TABLE 345 SFLOW_HOUR_SUMMARY

Field	Definition	Format	Size
IN_PORT_TYPE	This column is used to store the port type of the incoming traffic interface. For VCS switch the value of • 0 means its edge port. • 1 means its trill port. For other devices Default value is 0.	smallint	
OUT_PORT_TYPE	This column is used to store the port type of the outgoing traffic interface. For VCS switch the value of • 0 means its edge port. • 1 means its trill port. For other devices Default value is 0.	smallint	

TABLE 346 SFLOW_IP_ROUTE_INFO

Field	Definition	Format	Size
SFLOW_IP_ROUTE_INFO_ID	This column is the primary key for IP routing information.	int	
LOCAL_PREF	Local preference value of routing information in the received sFlow packet.	int	
LAST_USED_TIME	Last used time of the routing information.	int	
DST_AS_PATH	Routing path information in the received sFlow packet.	varchar	2048
COMMUNITIES	Communities value in the received sFlow packet.	varchar	1024

TABLE 347 SFLOW_MINUTE_BGP

Field	Definition	Format	Size
SLNUM	This column is used to store a counter value to identify the total row count.	bigserial	
TIME_IN_SECONDS	Data collection time in seconds.	int	
DEVICE_ID	ID of the product which sends the sflow traffic.	int	
SRC_AS	Source AS number of the received sFlow packet in case of BGP traffic.	bigint	
SFLOW_IP_ROUTE_INFO_ID	route_info_id of the received sFlow packet in case of BGP traffic.	int	
IN_VLAN	Vlan ID of the incoming traffic interface.	smallint	
OUT_VLAN	Vlan ID of the outgoing traffic interface.	smallint	
FRAMES	Number of frames transmitted through the sflow sample collected.	bigint	
BYTES	Number of bytes transmitted through the sflow sample collected.	bigint	

TABLE 347 SFLOW_MINUTE_BGP (Continued)

Field	Definition	Format	Size
IN_PORT_TYPE	Port type of the incoming traffic interface. For VCS member the value of, • 0 means its edge port. • 1 means its fabric port. For other devices Default value is 0.	smallint	
OUT_PORT_TYPE	Port type of the outgoing traffic interface. For VCS member the value of, • 0 means its edge port • 1 means its fabric port. For other devices Default value is 0.	smallint	

TABLE 348 SFLOW_MINUTE_BGP_SLNUM

Field	Definition	Format	Size
MAX_SLNUM	Maximum row count.	bigint	

TABLE 349 SFLOW_MINUTE_L3_SLNUM

Field	Definition	Format	Size
MAX_SLNUM	Maximum row count.	bigint	

TABLE 350 SFLOW_MINUTE_MAC

Field	Definition	Format	Size
SLNUM	This column is used to store a counter value to identify the total row count.	bigserial	
TIME_IN_SECONDS	Data collection time in seconds.	int	
DEVICE_ID	ID of the product which sends the sflow traffic.	int	
FRAMES	Number of frames transmitted through the sflow sample collected.	bigint	
BYTES	Number of bytes transmitted through the sflow sample collected.	bigint	
IN_VLAN	Vlan ID of the incoming traffic interface.	smallint	
OUT_VLAN	Vlan ID of the outgoing traffic interface.	smallint	
SRC_MAC	MAC address of the Source in the received sFlow packet.	bytea	
DEST_MAC	MAC address of the destination in the received sFlow packet.	bytea	
IN_PORT_TYPE	Port type of the incoming traffic interface. For VCS member the value of, • 0 means its edge port • 1 means its fabric port. For other devices Default value is 0.	smallint	

TABLE 350 SFLOW_MINUTE_MAC (Continued)

Field	Definition	Format	Size
OUT_PORT_TYPE	Port type of the outgoing traffic interface. For VCS member the value of, • 0 means its edge port • 1 means its fabric port. For other devices Default value is 0	smallint	
L3_SRC_ADDR	This column is used to store the L3 address of the source in the received sFlow packet.	bytea	
L3_DEST_ADDR	This column is used to store the L3 address of the destination in the received sFlow packet.	bytea	

TABLE 351 SFLOW_MINUTE_MAC_SLNUM

Field	Definition	Format	Size
MAX_SLNUM	Maximum row count.	bigint	

TABLE 352 SFLOW_MINUTE_SUMMARY

Field	Definition	Format	Size
SLNUM	This column is used to store a counter value to identify the total row count.	bigserial	
TIME_IN_SECONDS	Data collection time in seconds.	int	
DEVICE_ID	ID of the product which sends the sflow traffic.	int	
FRAMES	Number of frames transmitted through the sflow sample collected.	bigint	
BYTES	Number of bytes transmitted through the sflow sample collected.	bigint	
IN_PORT_TYPE	Port type of the incoming traffic interface. For VCS member the value of, • 0 means its edge port • 1 means its fabric port. For other devices Default value is 0.	smallint	
OUT_PORT_TYPE	Port type of the outgoing traffic interface. For VCS member the value of, • 0 means its edge port • 1 means its fabric port. For other devices Default value is 0	smallint	

TABLE 353 SFLOW_MINUTE_VLAN

Field	Definition	Format	Size
SLNUM	This column is used to store a counter value to identify the total row count.	bigserial	
TIME_IN_SECONDS	Data collection time in seconds.	int	
DEVICE_ID	ID of the product which sends the sflow traffic.	int	
FRAMES	Number of frames transmitted through the sFlow sample collected.	bigint	

TABLE 353 SFLOW_MINUTE_VLAN (Continued)

Field	Definition	Format	Size
BYTES	Number of bytes transmitted through the sFlow sample collected.	bigint	
IN_VLAN	Vlan ID of the incoming traffic interface.	smallint	
OUT_VLAN	Vlan ID of the outgoing traffic interface.	smallint	
IN_PORT_TYPE	Port type of the incoming traffic interface. For VCS member the value of, • 0 means its edge port. • 1 means its fabric port. For other devices Default value is 0.	smallint	
OUT_PORT_TYPE	Port type of the outgoing traffic interface. For VCS member the value of, • 0 means its edge port. • 1 means its fabric port. For other devices Default value is 0.	smallint	

TABLE 354 SFLOW_MINUTE_VLAN_SLNUM

Field	Definition	Format	Size
MAX_SLNUM	Maximum row count.	bigint	

TABLE 355 SFLOW_REPORT_L3_SOURCE

Field	Definition	Format	Size
SFLOW_REPORT_L3_SOURCE_ID	Primary key autogenerated ID.	int	
REPORT_DEFINITION_ID	Report definition ID.	int	
ADDRESS_GROUP_ID	ACL network group IDs mapped with a report definition.	int	
IP_SUBNET_DEFINITION_ID	Subnet IDs mapped with a Report definition.	int	

TABLE 356 SFLOW_REPORT_L4_SOURCE

Field	Definition	Format	Size
SFLOW_REPORT_L4_SOURCE_ID	Primary key autogenerated ID.	int	
REPORT_DEFINITION_ID	Report definition ID.	int	
SERVICE_PORT_DEFINITION_ID	Service port Id mapped with a report definition.	int	
SERVICE_GROUP_ID	Service group Id mapped with a report definition.	int	

TABLE 357 SFLOW_STAGING

Field	Definition	Format	Size
SLNUM	This column is used to store a counter value to identify the total row count.	bigserial	
TIME_IN_SECONDS	Data collection time in seconds.	int	
DEVICE_ID	ID of the product which sends the sflow traffic.	int	

TABLE 357 SFLOW_STAGING (Continued)

Field	Definition	Format	Size
IN_UNIT	Unit number of the incoming traffic interface. Default value is 0.	smallint	
IN_SLOT	Slot number of the incoming traffic interface.	smallint	
IN_PORT	Port number of the incoming traffic interface.	smallint	
OUT_UNIT	Unit number of the outgoing traffic interface. Default value is 0.	smallint	
OUT_SLOT	Slot number of the outgoing traffic interface.	smallint	
OUT_PORT	Port number of the outgoing traffic interface.	smallint	
IN_VLAN	Vlan ID of the incoming traffic interface.	smallint	
OUT_VLAN	Vlan ID of the outgoing traffic interface.	smallint	
IN_PRIORITY	Priority ID of the incoming traffic interface.	smallint	
OUT_PRIORITY	Priority ID of the outgoing traffic interface.	smallint	
SRC_MAC	MAC address of the source in the received sFlow packet.	bytea	
DEST_MAC	MAC address of the destination in the received sFlow packet.	bytea	
L3_SRC_ADDR	L3 address of the source in the received sFlow packet.	bytea	
L3_DEST_ADDR	L3 address of the destination in the received sFlow packet.	bytea	
L3_PROTOCOL	L3 protocol value in the received sFlow packet. For example, ARP.	int	
IP_TOS	Type of service ID in the received sFlow packet.	smallint	
L4_PROTOCOL	L4 protocol value in the received sFlow packet. For example, IGP.	smallint	
L4_SRC_PORT	L4 source port number in the received sFlow packet.	int	
L4_DEST_PORT	L4 destination port number in the received sFlow packet.	int	
SRC_SUBNET_BITS	Subnet value of the incoming traffic interface.	smallint	
DEST_SUBNET_BITS	Subnet value of the outgoing traffic interface.	smallint	
LOCAL_AS	Second AS number of the received sFlow packet in case of BGP traffic.	bigint	
SRC_AS	Source AS number of the received sFlow packet in case of BGP traffic.	bigint	
SRC_PEER_AS	Peer AS number of the received sFlow packet in case of BGP traffic.	bigint	
SFLOW_IP_ROUTE_INFO_ID	route_info_id of the received sFlow packet in case of BGP traffic.	int	
IP_FLOW_LABEL	IP flow label value in the received sFlow packet.	int	
SRC_USER	Name of the source user in the received sFlow packet.	int	

TABLE 357 SFLOW_STAGING (Continued)

Field	Definition	Format	Size
DEST_USER	Name of the destination user in the received sFlow packet.	int	
FRAMES	Number of frames transmitted through the sflow sample collected.	bigint	
BYTES	Number of bytes transmitted through the sflow sample collected.	bigint	
TCP_FLAGS	Tcp flag value of the received sFlow packet.	smallint	
IN_PORT_TYPE	This column is used to store the port type of the incoming traffic interface. For VCS switch the value of 0 means its edge port, and 1 means its trill port. For other devices Default value is 0.	smallint	
OUT_PORT_TYPE	This column is used to store the port type of the outgoing traffic interface. For VCS switch the value of 0 means its edge port, and 1 means its trill port. For other devices Default value is 0.	smallint	

TABLE 358 SFLOW_STAGING_SLNUM

Field	Definition	Format	Size
MIN_SLNUM	Maximum row count.	bigint	

TABLE 359 SMART_CARD

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
CARD_TYPE	Indicates how this smart card is configured: 0 = authorization card. The default value is 0.	smallint	
CARD_INFO	Additional smart card details. For recovery set cards, the details include the recovery set size and the card''s position within the set; e.g., 2 of 5	varchar	64
CARDCN_ID	A unique name for the card, derived from the card''s serial number and usage	varchar	64
FIRST_NAME	Optional first name of the person responsible for this card.	varchar	64
LAST_NAME	Optional last name of the person responsible for this card	varchar	64
NOTES	User-supplied notes about the card.	varchar	256
PUBLIC_CERTIFICATE	The public key certificate of the card, in PEM format. Used to validate the card and set up a secure communications channel to the card.	varchar	4096
CERTIFICATE_LABEL	User-supplied name for the card''s public key certificate	varchar	256

TABLE 359 SMART_CARD (Continued)

Field	Definition	Format	Size
GROUP_NAME	The name of the Encryption Group used to initialize the card. For recovery set cards, this identifies which group"s master key is backed up on the card.	varchar	64
CREATION_TIME	The date and time that the card was initialized. For recovery set cards, this is the date and time the master key was written to the card. The default value is 'now()'.	timestamp	

TABLE 360 SMIA_SAN_NAME

Field	Definition	Format	Size
NAME	'This will be the principal switch WWN of the fabric.';	varchar	24
ELEMENT_NAME	User friendly name to identify the SAN	varchar	32
IS_PRIMARY_FABRIC	This value will indicate whether principal switch WWN has primary ownership or not. In case of simple FC fabric, the value will be always 1. In case of Meta SAN, Fabric with highest principal switch WWN will have primary ownership (value 1) and other fabric entries within the same SAN will have value as 0.	int	

TABLE 361 SNAPSHOT_PRODUCT_STATUS

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
DEPLOYMENT_STATUS_ID	Foreign Key references DEPLOYMENT_STATUS_ID (id). Identifies the execution cycle for the deployment.	int	
MANAGED_ELEMENT_ID	Associates for which target the status applies to.	int	
SNAPSHOT_TYPE	Indicates the type of snapshot: • 1-Pre snapshot • 2-Post snapshot	int	
SNAPSHOT_TIME	Time when this pre/post snapshot occurred.		
MESSAGE	Detailed message for snapshot report.	text	

TABLE 362 SNMP_CREDENTIALS

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
VIRTUAL SWITCH_ID	Virtual switch ID for which this instance of the SNMP credentials apply.	int	
RECIPIENT_ID	Recipient in the MESSAGE_RECIPIENT table.	int	
POR)_NUMBER	Port number of the SNMP agent on the switch for get and set requests.	smallint	
RETRY_COUNT	Number of times to retry if get/set request to the SNMP agent times out. Default value is 3.	smallint	

TABLE 362 SNMP_CREDENTIALS (Continued)

Field	Definition	Format	Size
TIMEOUT	Timeout value in seconds for a get/set request to the SNMP agent. Default value is 5.	smallint	
VERSION	SNMP agent version running on the switch, as in SNMPv1 or SNMPv3.	varchar	6
READ_COMMUNITY_ STRING	The SNMP Read-Only Community String is like a password. It is sent along with each SNMP Get-Request and allows (or denies) access to a device. The default value is "public". This is applicable if the agent is configured to operate in SNMPv1.	varchar	64
WRITE_COMMUNITY_ STRING	The SNMP Write-Only Community String is like a password. It is sent along with each SNMP Set-Request and allows (or denies) access to a device. The default value is "private". This is applicable if the agent is configured to operate in SNMPv1.	varchar	64
USER_NAME	A human readable string representing the name of the user. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64
CONTEXT_NAME	Text ID associated with the user, used by the SNMP agent to provide different views. This is applicable if the agent is configured to operate in SNMPv3.	varchar	128
AUTH_PROTOCOL	An indication of whether messages sent or received on behalf of this user can be authenticated and if so, which authentication protocol to use. The supported values for this field are: usmNoAuthProtocol, usmHMACMD5AuthProtocol, and usmHMACSHAAuthProtocol. This is applicable if the agent is configured to operate in SNMPv3.	varchar	16
AUTH_PASSWORD	The localized secret key used by the authentication protocol for authenticating messages. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64
PRIV_PROTOCOL	An indication of whether messages sent or received on behalf of this user can be encrypted and if so, which privacy protocol to use. The current values for this field are: usmNoPrivProtocol and usmDESPrivProtocol. This is applicable if the agent is configured to operate in SNMPv3.	varchar	16
PRIV_PASSWORD	The localized secret key used by the privacy protocol for encrypting and decrypting messages. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64

TABLE 363 SNMP_DATA

Field	Definition	Format	Size
ID	Primary key column.	serial	
MIB_OBJECT_ID	MIB Object ID.	int	

TABLE 363 SNMP_DATA (Continued)

Field	Definition	Format	Size
TARGET_TYPE	Target type of the SNMP collector data. The target type for, • device level collector is 0 • port level collector it is 1.	num	(2,0)
TARGET_ID	Target id of the SNMP collector data. for device level collector it will use deviceId, and for port level it will use interfaceId.	int	
VALUE	Value of the OID retrieved from the corresponding target.	double	
TIME_IN_SECONDS	Time, in seconds, at which the record was inserted.	int	
COLLECTOR_ID	Correspoding collector table ID.	int	
MIB_INDEX	Index value for a MIB varaible. For scalar value it will be empty.	varchar	256

TABLE 364 SNMP_DATA_1DAY

Field	Definition	Format	Size
ID	Primary key autogenerated ID.	int	
MIB_OBJECT_ID	The DB ID of MIB_OBJECT.	int	
TARGET_TYP	Target or source type can be, • device - 0 or • interface or ports - 1	num	(2,0)
TARGET_ID	DB ID of the target which can be device or interface.	int	
VALUE	Aggregated value inserted during the aging process.	double precision	
TIME_IN_SECONDS	Time, in seconds, at which the record was inserted.	int	
COLLECTOR_ID	DB ID of the collector object used for collection.	int	
MIB_INDEX	MIB index used for collection if applicable.	char	256

TABLE 365 SNMP_DATA_2HOUR

Field	Definition	Format	Size
ID	The DB ID of MIB_OBJECT.	int	
MIB_OBJECT_ID	The DB ID of MIB_OBJECT.	int	
TARGET_TYPE	Target or source type can be, • device - 0 or • interface or ports - 1	num	(2,0)
TARGET_ID	DB ID of the target which can be device or interface.	int	
VALUE	Aggregated value inserted during the aging process.	double precision	
TIME_IN_SECONDS	Time, in seconds, at which the record was inserted.	int	
COLLECTOR_ID	DB ID of the collector object used for collection.	int	
MIB_INDEX	MIB index used for collection if applicable.	char	256

TABLE 366 SNMP_DATA_30MIN

Field	Definition	Format	Size
ID	Primary key autogenerated ID	int	
MIB_OBJECT_ID	MIB OID used for collection	int	
TARGET_TYPE	Target or source type can be, • device - 0 or • interface or ports - 1	num	(2,0)
TARGET_ID	DB Id of the target which can be device or interface	int	
VALUE	Value collected by the engine	double precision	
TIME_IN_SECONDS	Time at which collection occured in seconds	int	
COLLECTOR_ID	DB Id of the collector object used for collection	int	
MIB_INDEX	MIB index used for collection if applicable	char	256

TABLE 367 SNMP_EXPR_DATA

Field	Definition	Format	Size
ID	Primary key column.	serial	
EXPRESSION_ID	MIB object ID.	int	
TARGET_TYPE	Target type of the SNMP collector data. Th target type for, • device level collector is 0, • for port level collector is 1.	smallint	
TARGET_ID	Target ID of the SNMP collector data. for device level collector it will use deviceId, for port level it will use interfaceId.	int	
VALUE	Value of the OID retrieved from the corresponding target.	double	
TIME_IN_SECONDS	Time when value of the OID was retrieved from the corresponding target.	int	
COLLECTOR_ID	Correspoding collector table ID.	int	

TABLE 368 SNMP_EXPR_DATA_1DAY

Field	Definition	Format	Size
ID	Primary key autogenerated ID.	int	
EXPRESSION_ID	DB ID of the expression object used for collection.	int	
TARGET_TYPE	Target or source type can be, • device - 0 or • interface or ports - 1	smallint	
TARGET_ID	DB Id of the target which can be device or interface.	int	
VALUE	Aggregated value inserted during the aging process.	double precision	

TABLE 368 SNMP_EXPR_DATA_1DAY (Continued)

Field	Definition	Format	Size
TIME_IN_SECONDS	Time, in seconds, at which the record was inserted in seconds.	int	
COLLECTOR_ID	DB ID of the collector object used for collection.	int	

TABLE 369 SNMP_EXPR_DATA_30MIN

Field	Definition	Format	Size
ID	Primary key autogenerated ID	int	
EXPRESSION_ID	DB ID of the expression object used for collection	int	
TARGET_TYPE	Target/Source type can be device:0 or interface/ports:1'	smallint	
TARGET_ID	DB Id of the target which can be device or interface	int	
VALUE	Value collected by the engine'	double precision	
TIME_IN_SECONDS	Time at which collection occured in seconds	int	
COLLECTOR_ID	DB Id of the collector object used for collection	int	

TABLE 370 SNMP_EXPRESSION

Field	Definition	Format	Size
EXPRESSION_ID	Primary key column.	serial	
NAME	Name of the expression.	varchar	64
DESCRIPTION	Description of the expression.	varchar	512
EQUATION	Equation of the expression.	varchar	1024
UNIT	Unit that is used for displaying the chart.	varchar	64
IS_TRANSIENT	Explicitly identified whether expressions is used for Real time collector or not. A transient expression will not be allowed for user editing.	numeric	(1,0)

TABLE 371 SNMP_PROFILE

Field	Definition	Format	Size
NAME*	A text string representing a set of SNMP agent profile. When created, one or more virtual switches could refer to this profile for its SNMP credentials unless a unique set of SNMP credentials has been defined in SNMP_CREDENTIAL.	varchar	256
PORT_NUMBER	Port number of the SNMP agent on the switch for get and set requests	smallint	
RETRY_COUNT	Number of times to retry if get/set request to the SNMP agent times out. Default value is 3.	smallint	
TIMEOUT	Timeout value in seconds before for a get/set request to the SNMP agent. Default value is 5.	smallint	

TABLE 371 SNMP_PROFILE (Continued)

Field	Definition	Format	Size
VERSION	SNMP agent version running on the switch as in SNMPv1 and SNMPv3	varchar	6
READ_COMMUNITY_STRING	The SNMP Read-Only Community String is like a password. It is sent along with each SNMP Get-Request and allows (or denies) access to device. The default value is "public". This is applicable if the agent is configured to operate in SNMPv1.	varchar	64
WRITE_COMMUNITY_STRING	The SNMP Write-Only Community String is like a password. It is sent along with each SNMP Set-Request and allows (or denies) access to a device. The default value is "private". This is applicable if the agent is configured to operate in SNMPv1	varchar	64
USER_NAME	A human-readable string representing the name of the user. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64
CONTEXT_NAME	A text ID associated with the user, used by SNMP agent to provide different views. This is applicable if the agent is configured to operate in SNMPv3.	varchar	128
AUTH_PROTOCOL	An indication of whether or not messages sent or received on behalf of this user can be authenticated and if so, which authentication protocol to use. The supported values for this field are: usmNoAuthProtocol, usmHMACMD5AuthProtocol, and usmHMACSHAAuthProtocol. This is applicable if the agent is configured to operate in SNMPv3.	varchar	16
AUTH_PASSWORD	The localized secret key used by the authentication protocol for authenticating messages. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64
PRIV_PROTOCOL	An indication of whether or not messages sent or received on behalf of this user can be encrypted and if so, which privacy protocol to use. The current values for this field are: usmNoPrivProtocol and usmDESPrivProtocol. This is applicable if the agent is configured to operate in SNMPv3.	varchar	16
PRIV_PASSWORD	The localized secret key used by the privacy protocol for encrypting and decrypting messages. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64
SNMP_INFORMS_ENABLED	To denote whether SNMP informs option is enabled or disabled Default value is 0.	smallint	

TABLE 372 SNMP_TRAP_CREDENTIAL

Field	Definition	Format	Size
ID	PK for the table to uniquely identify the record	int	
VERSION	to identify the version of Credentials: v1v2c and v3 are the values	varchar	6
COMMUNITY_STRING	to decode the v1/v2c traps	varchar	64
USER_NAME	user access name for v3 trap	varchar	64
AUTH_PROTOCOL	authentication protocol used for v3 traps	varchar	16
AUTH_PASSWORD	authentication password for v3 traps	varchar	64
PRIV_PROTOCOL	privacy protocol used for v3 traps	varchar	16
PRIV_PASSWORD		varchar	64
POSITION_	order of credentials to authenticate v1/v2c or v3 traps	int	

TABLE 373 SNMP_V3_FORWARDING_CREDENTIAL

Field	Definition	Format	Size
ID*		int	
USER_NAME	USM user name.	varchar	64
CONTEXT_NAME	USM context name.	VARCHAR	128
AUTH_PROTOCOL	Authorization protocol.	VARCHA	16
AUTH_PASSWORD	Authorization password.	VARCHAR	64
PRIV_PROTOCOL	Privilege protocol.	VARCHAR	16
PRIV_PASSWORD	Privilege password.	VARCHAR	64

TABLE 374 SOURCE_OBJECT_TYPE

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
TYPE_NAME	Type of the object to which the event applies, such as Fabric, Switch or Port.	char	64
DESCRIPTION	Description of the object	varchar	255

TABLE 375 SSL_CERTIFICATE

Field	Definition	Format	Size
SSL_CERTIFICATE_ID		int	
NAME		varchar	255
LOCATION		varchar	255
FILE_NAME		varchar	255
KEY_ID		int	
CERT_TYP		num	(2,0)
START_TIME		num	(20,0)

TABLE 375 SSL_CERTIFICATE (Continued)

Field	Definition	Format	Size
EXPIRATION_TIME		num	(20,0)
FORMAT		num	(2,0)
DESCRIPTION		varchar	1024
NOTIFICATION_TIME	The time stamp (long format) of the last expiration notification sent	num	(20,0)
NOTIFICATION_SENT	The status of last notification sent. Possible values: Unknown -0, Good 1, Expiring 2, Expired 3	num	(2,0)
NOTIFICATION_REPEAT	Indicates whether repeat expiration notification is enabled for this certificate or not. Possible values: Repeat Disabled - 0, Repeat Enabled - 1	num	(2,0)
SYNC_DEVICE	Indicates whether this certificate is in sync with device or not. Possible values: Need Deploy 0, Imported 1, Deployed 2, Unknown 3.	num	(2,0)
CERTIFICATE	The content of the ssl certificate.	txt	
USER_ID	This field will be populated when the Management application user creates certificate or import certificates from file. User can view this certificate not bound to any vip in SSL certificate dialog	int	

TABLE 376 SSL_CERTIFICATE_VIP_SERVER_MAP

Field	Definition	Format	Size
SSL_CERTIFICATE_ID	Foreign key to SSL_CERTIFICATE_ID in ssl_certificate table	int	
VIP_SERVER_ID	The column holds ID of VIP Server. It is Foreign Key and refers to ID column of VIP_SERVER table	int	

TABLE 377 SSL_KEY

Field	Definition	Format	Size
ssl_key_id		int	
name		varchar	255
location		varchar	255
file_name		varchar	255
key_type		varchar	2
encryption_type		varchar	2
password		varchar	255
description		varchar	1024
strength	The strength of the private key in bits.	int	

TABLE 377 SSL_KEY (Continued)

Field	Definition	Format	Size
private_key	Content of the private key.	txt	
USER_ID	This field will be populated when the Management application user creates certificate or import certificates from file. User can view this certificate not bound to any vip in SSL certificate dialog.	int	

TABLE 378 SSL_KEY_PASSWORD

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
KEY_PASSWORD_ALIAS	Key Password Alias is the alias name used for the encrypted key password. This alias name is used to identify the password in client UI.	varchar	16
KEY_PASSWORD	SSL keys are protected by passwords, and these passwords are used during key import operation from device. The key password is stored encrypted in the tables.	varchar	256

TABLE 379 STATS_AGING

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
FIVE_MIN_VALUE	Configured maximum samples value for the five minute table.	int	
THIRTY_MIN_VALUE	Configured maximum samples value for the thirty minute table.	int	
TWO_HR_VALUE	Configured maximum samples value for the two hour table.	int	
ONE_DAY_VALUE	Configured maximum samples value for the one day table.	int	
MAX_SAMPLES_VALUE	The maximum number of samples value, i.e., 3456.	int	
INTERPOLATE	Whether interpolation is enabled or disabled.	smallint	
POLICY_TYPE	The type of the aging ploicy. • 100 - Default aging (1 day 5 mins samples, 3 days 30 mins samples,7 days 2 hrs sample and 2 years 1 day samples) • 101 - 5 mins to 1 day aging(8 days 5 mins samples and 90 days of 1 day samples)	smallint	
ACTIVE	The active state of the policy.	smallint	

TABLE 380 STP_PORT

Field	Definition	Format	Size
STP_PORT_ID	Prmiary key Identifier.	int	
STP_INSTANCE_ID	Foreign Key Reference to STP_INSTANCE table.	int	
STP	If MSTP is enabled, the value will be 1 else 0.	numeric	(1,0)

TABLE 380 STP_PORT

Field	Definition	Format	Size
INTERFACE_ID	Foreign Key Reference to INTERFACE table	int	
PATH_COST	Port Path Cost.	bigint	
PRIORITY	Port Priority.	bigint	
LINK_TYPE	Link Type. 1- Shared 2 - P2P.	numeric	(1,0)
PORT_FAST	Port Fast. 0 - Disabled 1 - Enabled	numeric	(1,0)
BPDU_FILTER	BPDU Filter. 0 - Disabled 1 - Enabled	numeric	(1,0)
BPDU_GUARD	BPDU guard. 0 - Disabled 1 - Enabled	numeric	(1,0)
EDGE_PORT	Edge port. 0 - Disabled 1 - Enabled	numeric	(1,0)
AUTO_EDGE	Auto edge. 0 - Disabled 1 - Enabled	numeric	(1,0)
ROOT_GUARD	Root guard. 0 - Disabled 1 - Enabled	numeric	(1,0)
HELLO_TIME	Number of seconds between generation of config BPDUs on CIST.	smallint	
VLAN_ID	The PVST and RPVST values needs to mapped with the VLAN.	int	

TABLE 381 STP_INSTANCE

Field	Definition	Format	Size
STP_INSTANCE_ID		int	
INSTANCE_TYPE		num	(2,0)
INSTANCE_ID		num	(4,0)
DEVICE_ID		int	
STP_MODE		num	(2,0)
FORWARD_DELAY		num	(2,0)
MAX_AGE		num	(2,0)
HELLO_TIME		num	(2,0)
PRIORITY		num	(6,0)
STP_VERSION		num	(2,0)

TABLE 381 STP_INSTANCE (Continued)

Field	Definition	Format	Size
RE_ENABLE_PORT_INTERVAL	FOS/NOS Field. Re enable port interval.	int	
RE_ENABLE_PORT_STATE	FOS/NOS Field. Re enable port state.	smallint	
PATH_COST		bigint	
STP	Possible values: • 0 - Disabled • 1 - Enabled	smallint	
CISCO_INTER_OP	Cisco Interoperability Enabled/Disabled.	num	(1,0)
TX_HOLD_COUNT	Transmit HoldCount of the Bridge	smallint	
MAX_HOPS	MST max hop count (1-40)	smallint	
REGION	MST Region.	varchar	255
REVISION	Revision Number for Configuration information.	smallint	

TABLE 382 SWITCH_BOTTLENECK_CONFIG

Field	Definition	Format	Size
VIRTUAL_SWITCH_ID	The database ID of the switch that the configuration belongs to	int	
BOTTLENECK_DETECT_ENABLED	Flag indicates if bottleneck detection is enabled or not	smallint	
ALERTS_ENABLED	Flag indicates if bottleneck detection alerts is enabled or not	smallint	
CONGESTION_THRESHOLD	Value of bottleneck detection congestion threshold in percent	double precision	
LATENCY_THRESHOLD	Value of bottleneck detection latency threshold in percent	double precision	
WINDOW_	Value of bottleneck detection latency window in millisecond	int	
QUIET_TIME	Value of bottleneck detection quiet time in millisecond	int	
CREATION_TIME	Creation time of the record	timestamp	
LAST_UPDATE_TIME	Last update time of the record	timestamp	
LATENCY_SEVERITY	The factor by which throughput must drop in a second in order for that second to be considered affected by latency bottlenecking. Range (1 to 1000).	int	
LATENCY_TIME	The minimum fraction of a second that must be affected by latency in order for that second to be considered affected by latency bottlenecking. Range (0 to 1).	double precision	

TABLE 383 SWITCH_CONFIG

Field	Definition	Format	Size
ID*		int	
NAME	Name of the switch configurations uploaded from the switch either on demand or through scheduler	varchar	64
SWITCH_ID	ID of the switch from which the configuration has been uploaded.	int	
CORE_SWITCH_ID		int	
BACKUP_DATE_TIME	The date/time stamp at which the configuration has been uploaded.	timestamp	
CONFIG_DATA	The actual switch configuration data.	text	
CEE_CONFIG_DATA	Switch configuration data for CEE	text	
KEEP_COPY	The column value (1) helps to preserve the configuration even after the expiration of its age.	smallint	
CREATED_BY	The column value helps to figure out who triggered the configuration upload operation.	varchar	64
CONFIG_TYPE	Configuration Type • FC=0 • CEE_RUNNING=1 • CEE_STARTUP=2 • INVALID=-1 Default value is 0.	smallint	
COMMENTS	Brief comments about this configuration.	varchar	256

TABLE 384 SWITCH_CONFIG_DETAIL

Field	Definition	Format	Size
SWITCH_CONFIG_ID		int	
IP_ADDRESS	IP Address of the switch for which the configuration was uploaded either on demand or schedule.	varchar	128
WWN	WWN of the switch for which the configuration was uploaded either on demand or schedule.	char	23
PHYSICAL_SWITCH_WWN	CORE WWN of the switch for which the configuration was uploaded either on demand or schedule.	char	23
MODEL_NUMBER	Model Number of the switch for which the configuration was uploaded either on demand or schedule.	varchar	32

TABLE 385 SWITCH_LICENSE

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
CORE_SWITCH_ID	Refers to the entry in the CORE_SWITCH table.	int	
LICENSE_KEY	Stores the license key obtained from the switch.	varchar	256

TABLE 386 SWITCH_MODEL

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
SWBD_TYPE	Switch type number, universally used by all the Management application module implementation.	smallint	
SUBTYPE	Switch subtype. At present no subtypes for existing model records are defined. Default value is 0.	smallint	
DESCRIPTION	Model description, such as FC link speed, port count and whether multi-card (director) class switch or other type of switch. Default is 'Not Available'.	varchar	256
MODEL	Switch model string.	varchar	32
REMARK	Remarks, such as an internal project name.	varchar	64
SYS_OID	This will represent the sys_oid for each product type.	varchar	255
PRODUCT_FAMILY	This represents the product family that each OID belongs to.	varchar	128
BRIEF_PRODUCT_FAMILY	Shorter name for the product family.	varchar	32
SPEED	Switch max speed. Value 0 represents NotAvailable.	smallint	
MULTI_CP_CAPABLE	Switch is multi cp cabable or not. 0 means single CP and 1 means multi.	smallint	
MIN_IMAGE_VERSION	Supported min firmware version.	varchar	64
MAX_IMAGE_VERSION	Supported max firmware version.	varchar	64

TABLE 387 SWITCH_PORT

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
VIRTUAL_SWITCH_ID	DB ID of virtual_switch to which this port belongs.	int	
WWN	WWN of the port.	char	23
NAME	User friendly name of the port.	char	32
SLOT_NUMBER	Slot number. Default value is 0.	int	
PORT_NUMBER	The logical port number of the user port. There is no assumption of any relation to the physical location of a port within a chassis.	smallint	
USER_PORT_NUMBER	User port number. Unique port number in a chassis.	smallint	
PORT_ID	Port ID of this port.	varchar	8
PORT_INDEX	Number used for identifying port in zoning.	smallint	
AREA_ID	Area number the port is assigned to.	smallint	
MAC_ADDRESS	MAC address of this port.	varchar	64
PORT_MOD	Stores the port module type. Not applicable if port doesn't have a GBIC installed.	varchar	64

TABLE 387 SWITCH_PORT (Continued)

Field	Definition	Format	Size
TYPE	Port type. The specific mode currently enabled for the port. The port type could be U-Port, F-Port, E-Port etc.	varchar	16
FULL_TYPE	Refers to the full type of the port, U-Port, F-Port etc.	varchar	128
STATUS	Refers to the Status of the port. Eg. No Light, No Module, Mod_inv, Online etc.	varchar	64
HEALTH	Refers to the Health of the port. Eg. Unmonitored, Healthy, Offline , Error etc.	varchar	16
STATUS_MESSAGE	Any additional port level status similar to what is seen in CLI, like Segmented, Speed Mismatch, Trunk master etc are stored here.	varchar	255
PHYSICAL_PORT	Indicates if the port is physical port. It will be 0 for virtual ports Eg. Ports created by LISLs.	smallint	
LOCKED_PORT_TYPE	Indicates the locked port type of the port. Ports can be locked down so that they can come up only in that mode.	varchar	16
CATEGORY	Denotes the category of the switch. 1 denotes FC port and 2 denotes gige port.	smallint	
PROTOCOL	The protocol used by the port. FC, FCIP etc.	varchar	16
SPEED	Actual speed at which the port is currently operating.	varchar	64
SPEEDS_SUPPORTED	The supported port speed as a list of comma separated values.	varchar	32
MAX_PORT_SPEED	The maximum speed the port is capable of supporting, in bits per second.	int	
DESIRED_CREDITS	How many BB credits are desired for the port.	int	
BUFFER_ALLOCATED	How many BB credits are allocated for the port.	int	
ESTIMATED_DISTANCE	The estimated physical distance of the connection between ports.	int	
ACTUAL_DISTANCE	The physical distance of the connection on the port in relation to the other port.	int	
LONG_DISTANCE_SETTING	Whether long distance enabled.	int	
DEGRADED_PORT	Denotes if the port is in a degraded state. Has value as N/A for ports that are not online.	varchar	16
REMOTE_NODE_WWN	Node WWN of the attached port.	varchar	255
REMOTE_PORT_WWN	WWN of the attached port.	varchar	255
LICENSED	1 = the port is licensed; otherwise, 0.	smallint	
SWAPPED	1 = port is swapped; otherwise, 0.	smallint	
TRUNKED	1 = port is trunked; otherwise, 0.	smallint	
TRUNK_MASTER	1 = the port is trunk master; otherwise, 0.	smallint	
PERSISTENT_DISABLE	1 = port is persistently disabled.	smallint	
FICON_SUPPORTED	1 = FICON is supported; otherwise, 0.	smallint	
BLOCKED	1 = port is blocked; otherwise, 0.	smallint	

TABLE 387 SWITCH_PORT (Continued)

Field	Definition	Format	Size
PROHIBIT_PORT_NUMBERS	Indicates the ports prohibited with the current port as configured in the allow prohibit matric (PDCM).	varchar	1024
PROHIBIT_PORT_COUNT	The count of prohibited ports.	smallint	
NPIV	Whether NPIV mode is enabled.	smallint	
NPIV_CAPABLE	Instance NPIV mode capability: 1 = indicates port has NPIV capability 2 = NPIV license is enabled	smallint	
NPIV_ENABLED	Whether NPIV mode is enabled.	smallint	
FC_FAST_WRITE_ENABLED	1 = FC fast write is enabled.	smallint	
ISL_RRDY_ENABLED	Denotes if ISL receiver ready is enabled.	smallint	
RATE_LIMIT_CAPABLE	Denotes if the port is capable of Rate Limiting.	smallint	
RATE_LIMITED	Denotes if the port has Rate Limiting Enabled.	smallint	
QOS_CAPABLE	Indicates if the port is QOS capable.	smallint	
QOS_ENABLED	Indicates if the port is QOS enabled.	smallint	
TUNNEL_CONFIGURED	Denotes if the port has a fcip tunnel configured.	smallint	
FCIP_TUNNEL_UP	Denotes if the fcip tunnel that is configured is up.	smallint	
FCR_FABRIC_ID	Stores the FCR fabric ID. Applicable if the port is configured as an EX port.	smallint	
FCR_INTEROP_MODE	The interop mode of the FCR fabric. Applicable if the port is an EX port.	smallint	
CALCULATED_STATUS	The calculated status of the port. Eg. Healthy, Down, Marginal etc.	varchar	64
USER_DEFINED_VALUE1	User defined value used for annotation.	varchar	256
USER_DEFINED_VALUE2	User defined value used for annotation.	varchar	256
USER_DEFINED_VALUE3	User defined value used for annotation.	varchar	256
KIND	Stores the port kind from the NVP portKind.	varchar	32
STATE	The state of the port whether it is online or offline	varchar	64
PREVIOUS_STATUS	This table can hold the same values as STATUS column. But this will be holding the previous status of the PORT. These values to be populated by switch asset collector.	varchar	64
AUTO_DISABLE_CONFIGURED	To represent auto disable configuration state (set by user). Default value is 0.	smallint	
AUTO_DISABLED	To represent auto disabled status (set by switch). Default value is 0.	smallint	
OCCUPIED	Default value is 0.	smallint	
LAST_UPDATE	Last update time stored as long value. Elapsed time from 1970 in milliseconds.	bigint	
PORT_BIT_MASK	F-Port trunk bit mask value. Default value is 0.	int	

TABLE 387 SWITCH_PORT (Continued)

Field	Definition	Format	Size
LOGICAL_PORT_NUMBER	F-Port trunk logical port number. Default value is -1.	smallint	
DEFAULT_AREA_ID	Default Area id of F-Port trunk port. Default value is -1.	smallint	
LOGICAL_PORT_WWN	Logical port WWN of F-Port trunk group.	char	23
PREVIOUS_TYPE	This fields copies the old state of the port type. The field could be used to track the state change information for the switch port type. SwitchAssetCollector sets this field during the collection time. SMIA requested this information but could be used by any module which needs to track the type state change.	varchar	16
LATENCY_DETECT_SUPPORTED	Whether the port supports latency detection. 1 means true and 0 means false	smallint	
PREVIOUS_STATE	Fields copies the old state of the port . The field could be used to track the state change information for the switch port . SwitchAssetCollector sets this field during the collection time. SMIA requested this information but could be used by any module which needs to track the state change.	varchar	64
EPORT_DISABLED	Represents the eportDisabled field from switch.html. Values populated by SwitchAssetcollector during the collection time. Possible values includes 0 and 1. Default value is -1.	smallint	
SPEED_NEGOTIATED	This column indicates if the port speed is negotiated or not. If port speed is negotiated then value is 1 else it will be 0. Default value is -1.	smallint	
MAX_FRAME_MONITOR	Maximum frame monitor supported for switch port.	int	
MAX_FRAME_MONITOR_OFFSET	Maximum offset supported in fame monitor for switch port.	int	
	Contains the features supported as a bit mask at port level.	int	
IDENTIFIER	Switch port identifier extracted from interface name	char	80
PORT_CAPABILITIES	'List of capabilities of this port specified as bit mask. Each bit would represent capability like FEC, Encryption and compression, NPIV etc.';	int	
XISL_PORT_LIST	This field is applicable only for logical ports created for LISLs. It denotes the list of XISL ports associated with the current logical port. Will be blank for non-logical ports.	varchar	256

TABLE 387 SWITCH_PORT (Continued)

Field	Definition	Format	Size
PORT_COMMISSION_STATE	Indicates whether port decommission/recommission was in progress or completed, based on this status we will show the decommission/recommission icon on ports and Indicates the Decommissioned/Recommissioned status of the ports which was performed from the Management application. None - 0, Decommission In Progress - 1 , Decommissioned - 2, Recommission In Progress - 3, Recommissioned - 4. If the decommission is performed through CLI or other Management application server then the state would be None (0).	int	
FEATURES_ENABLED	Holds as a bit mask the features that are enabled . Refer FEATURES_ACTIVE for the active/inactive status of a feature. Each bit would represent features like Encryption, compression etc.' The bit mask and their corresponding Features are defined as an enum in the domain model class - SwitchPort.java.	int	
FEATURES_ACTIVE	Holds as a bit mask the features that are active. Please note that this is different from the enabled value which is found in the FEATURES_ENABLED column. Each bit would represent features like Encryption, compression etc. The bit mask and their corresponding Features are defined as an enum in the domain model class - SwitchPort.java.	int	
DISABLED_REASON	The Switch Port disabled reason.	varchar	1024
FENCED	1 means port is fenced.	smallint	
MASTER_PORT_NUMBER	This column will have the trunk master port number for the trunk members. For trunk master, it will have its own port number. For non-trunk ports, it will have the default value -1.	int	
SPEED_TYPE	Stores the speed type of the port. It contains one of the following values: • 1 - Indicates speed is in Mbps. • 2 - Indicates speed is in Gbps.	int	

TABLE 388 SWITCH_PORT_PERFORMANCE

Field	Definition	Format	Size
PORT_ID	Primary key of the Switch Port.	int	
SWITCH_ID	Primary key of Virtual Switch which this port is present	int	
TX	The number of octets or bytes that have been transmitted by this port. One second periodic polling of the port. This value is saved and compared with the next polled value to compute net throughput. Note, for Fibre Channel, ordered sets are not included in the count	double precision	

TABLE 388 SWITCH_PORT_PERFORMANCE (Continued)

Field	Definition	Format	Size
RX	The number of octets or bytes that have been received by this port. One second periodic polling of the port. This value is saved and compared with the next polled value to compute net throughput. Note, for Fibre Channel, ordered sets are not included in the count	double precision	
TX_UTILIZATION	The computed value of TX based on speed of port	double precision	
RX_UTILIZATION	'The computed value of RX based on speed of port	double precision	
LINK_FAILURE	Count of link failures. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8). Note, this is a Fibre Channel only stat	double precision	
TX_LINK_RESETS	Count of Link resets. This is the number of LRs received. Note, this is a Fibre Channel only stat	double precision	
RX_LINK_RESETS	Count of Link resets. This is the number LRs transmitted. Note, this is a Fibre Channel only stat	double precision	
SYNC_LOSSES	Count of instances of synchronization loss detected at port. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8). Note, this is a Fibre Channel only stat.	double precision	
SIGNAL_LOSSES	Count of instances of signal loss detected at port. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8). Note, this is a Fibre Channel only stat	double precision	
SEQUENCE_ERRORS	Count of primitive sequence protocol errors detected at this port. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8). Note, this is a Fibre Channel only stat	double precision	
INVALID_TRANSMISSIONS	Count of invalid transmission words received at this port. This count is part of the Link Error Status Block (LESB). FC-PH 29.8). Note, this is a Fibre Channel only stat	double precision	
CRC_ERRORS	Count of frames received with invalid CRC. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8). Loop ports should not count CRC errors passing through when monitoring. Note, this is a Fibre Channel only stat.'	double precision	
LAST_UPDATE_TIME	Time when this stats record was updated	timestamp	
FAKE_PORT	Denotes whether the port is a fake port created by the Management application for drawing connections or a real one obtained during collection from the switch. 1 denotes a fake port and 0 denotes a real port.	smallint	
SPEED_TYPE	Stores the speed type of the port. It will contain one of the following values: 1 - indicates speed is in Mbps 2 - indicates speed is in Gbps	int	

TABLE 389 SWITCH_THRESHOLD_SETTING

Field	Definition	Format	Size
SWITCH_ID*	References the ID in CORE_SWITCH table.	int	
POLICY_ID*	References the ID in THRESHOLD_POLICY table.	int	
STATUS	The status of applied to the switch.	smallint	
OVERRIDDEN	Policy is overridden or not overridden.	smallint	
DESCRIPTION	Description about the status of policy applied to the switch.	varchar	100

TABLE 390 SYSTEM_CARD_ENGINE_MAPPING

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
ENCRYPTION_ENGINE_ID	Foreign key reference to the ENCRYPTION_ENGINE for which a system card is registered	int	
SMART_CARD_ID	Foreign key reference to the SMART_CARD that is registered as a system card for the encryption engine.	int	

TABLE 391 SYSTEM_PROPERTY

Field	Definition	Format	Size
NAME*	The name of the property.	char	64
VALUE	The value for the property.	varchar	2048

TABLE 392 TARGET_TYPE

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
TYPE	Type of the target device. Some possible values are • Switch • Device • Port • Host • Port Group • Product Group • VLAN • Fabric	varchar	64

TABLE 393 THIRD_PARTY_DEVICE

Field	Definition	Format	Size
DEVICE_ID	Primary key for this table.	int	
DEVICE_TYPE	Type of the third party device. As of now, we have two types Wireless Location Manager and LANcope device.	varchar	64

TABLE 394 THRESHOLD_MEASURE

Field	Definition	Format	Size
MEASURE_ID*	References the ID In PM_MEASURE table, where all measures are defined.	int	
HIGH_BOUNDARY	Configured high boundary threshold value for measure ID.	int	
LOW_BOUNDARY	Configured low boundary threshold value for measure ID.	int	
BUFFER_SIZE	Configured buffer size for measure ID.	int	
POLICY_ID*	References the ID in THRESHOLD_POLICY table.	int	

TABLE 395 THRESHOLD_POLICY

Field	Definition	Format	Size
ID*		int	
NAME	Name of the policy.	varchar	100
TYPE	Type of the policy.	varchar	20
DESCRIPTION	Description about the policy.	varchar	100

TABLE 396 TIME_SERIES_DATA

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when value of the measure retrieved from the corresponding target.	int	
TARGET_TYPE	Target type of the PM collector data. For device level collector the target type is 0, for port level it is 1.	smallint	
MEASURE_ID	ID of the measure.	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId, for port level it will use interfaceId.	int	
COLLECTOR_ID	ID of the data_collector.	int	
MEASURE_INDEX	'Stores the index_map value in case of anexpression.	varchar	256
ME_ID	ME_ID of the target.	int	
VALUE	30 mins aggregated data.	double precision	

TABLE 397 TIME_SERIES_DATA_1DAY

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when the record is inserted.	int	
TARGET_TYPE	Target type of the PM collector data. For device level collector the target type is 0, for port level it is 1.	smallint	
MEASURE_ID	ID of the measure.	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId, for port level it will use interfaceId.	int	

TABLE 397 TIME_SERIES_DATA_1DAY (Continued)

Field	Definition	Format	Size
COLLECTOR_ID	ID of the data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
VALUE	30 mins aggregated data.	double precision	

TABLE 398 TIME_SERIES_DATA_2HOUR

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when the record is inserted.	int	
TARGET_TYPE	Target type of the PM collector data. For device level collector the target type is 0, for port level it is 1.	smallint	
MEASURE_ID	ID of the measure.	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId, for port level it will use interfaceId.	int	
COLLECTOR_ID	ID of the data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
VALUE	30 mins aggregated data.	double precision	

TABLE 399 TIME_SERIES_DATA_30MIN

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when the record is inserted.	int	
TARGET_TYPE	Target type of the PM collector data. For device level collector the target type is 0, for port level it is 1.	smallint	
MEASURE_ID	ID of the measure.	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId, for port level it will use interfaceId.	int	
COLLECTOR_ID	ID of the data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
VALUE	30 mins aggregated data.	double precision	

TABLE 400 TIME_SERIES_DATA_1

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when value of the measure retrieved from the corresponding target.	int	
TARGET_TYPE	Target type of the PM collector data. For IP_DEVICE(0), IP_PORT(1), IP_TRUNK(2), FOS_DEVICE(3), FC_PORT(4), GE_PORT(5), TE_PORT(6), HBA_PORT(7), CNA_PORT(8), VIRTUAL_FCOE_PORT(9), FCIP_TUNNEL(10), EE_MONITOR(11), IP_DEVICE_GROUP(12), IP_PORT_GROUP(13), VIRTUAL_GROUP(14), TRILL_TRUNK(15), ALL_SAN_PRODUCTS(16).	smallint	
MEASURE_ID	ID of the measure (MIB/Expression).	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId/virtualSwitchId, for port level it will use interfaceId/switchPortId/ fcipTunnelId/devicePortId.	int	
COLLECTOR_ID	DB ID of the pm_data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
SUM_VALUE	Named after SUM_VALUE to be consistent with column names in aggregated data tables. Stores the delta changes for counter values between two samples, only used for counter values, 0 for all other types of measures.	double precision	

TABLE 401 TIME_SERIES_DATA_1_1DAY

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when value of the measure retrieved from the corresponding target.	int	
TARGET_TYPE	Target type of the PM collector data. For IP_DEVICE(0), IP_PORT(1), IP_TRUNK(2), FOS_DEVICE(3), FC_PORT(4), GE_PORT(5), TE_PORT(6), HBA_PORT(7), CNA_PORT(8), VIRTUAL_FCOE_PORT(9), FCIP_TUNNEL(10), EE_MONITOR(11), IP_DEVICE_GROUP(12), IP_PORT_GROUP(13), VIRTUAL_GROUP(14), TRILL_TRUNK(15), ALL_SAN_PRODUCTS(16).	smallint	
MEASURE_ID	ID of the measure (MIB/Expression).	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId/virtualSwitchId, for port level it will use interfaceId/switchPortId/ fcipTunnelId/devicePortId.	int	
COLLECTOR_ID	DB ID of the pm_data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
VALUE	Stores One day aggregated data.	double precision	

TABLE 401 TIME_SERIES_DATA_1_1DAY (Continued)

Field	Definition	Format	Size
MIN_VALUE	Minimum value in 2 hour table while aggregating 1 day data.	double precision	
MAX_VALUE	Maximum value in 2 hour table while aggregating 1 day data.	double precision	

TABLE 402 TIME_SERIES_DATA_1_2HOUR

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when value of the measure retrieved from the corresponding target.	int	
TARGET_TYPE	Target type of the PM collector data. For IP_DEVICE(0), IP_PORT(1), IP_TRUNK(2), FOS_DEVICE(3), FC_PORT(4), GE_PORT(5), TE_PORT(6), HBA_PORT(7), CNA_PORT(8), VIRTUAL_FCOE_PORT(9), FCIP_TUNNEL(10), EE_MONITOR(11), IP_DEVICE_GROUP(12), IP_PORT_GROUP(13), VIRTUAL_GROUP(14), TRILL_TRUNK(15), ALL_SAN_PRODUCTS(16).	smallint	
MEASURE_ID	ID of the measure (MIB/Expression).	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId/virtualSwitchId, for port level it will use interfaceId/switchPortId/ fcipTunnelId/devicePortId.	int	
COLLECTOR_ID	DB ID of the pm_data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
VALUE	Stores the 2 hours aggregated data.	double precision	
MIN_VALUE	Minimum value in 30 min table while aggregating 2 hours of data.	double precision	
MAX_VALUE	Maximum value in 30 min table while aggregating 2 hours of data.	double precision	

TABLE 403 TIME_SERIES_DATA_1_30MIN

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when value of the measure retrieved from the corresponding target.	int	
TARGET_TYPE	Target type of the PM collector data. For IP_DEVICE(0), IP_PORT(1), IP_TRUNK(2), FOS_DEVICE(3), FC_PORT(4), GE_PORT(5), TE_PORT(6), HBA_PORT(7), CNA_PORT(8), VIRTUAL_FCOE_PORT(9), FCIP_TUNNEL(10), EE_MONITOR(11), IP_DEVICE_GROUP(12), IP_PORT_GROUP(13), VIRTUAL_GROUP(14), TRILL_TRUNK(15), ALL_SAN_PRODUCTS(16).	smallint	
MEASURE_ID	ID of the measure (MIB/Expression).	int	

TABLE 403 TIME_SERIES_DATA_1_30MIN (Continued)

Field	Definition	Format	Size
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId/virtualSwitchId, for port level it will use interfaceId/switchPortId/ fcipTunnelId/devicePortId.	int	
COLLECTOR_ID	DB ID of the pm_data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
VALUE	Stores the 30 minutes aggregated data.	double precision	
MIN_VALUE	Minimum value in raw performance statistics table while aggregating 30 minutes of data.	double precision	
MAX_VALUE	Maximum value in raw performance statistics table while aggregating 30 minutes of data.	double precision	

TABLE 404 TIME_SERIES_DATA_2

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when value of the measure retrieved from the corresponding target.	int	
TARGET_TYPE	Target type of the PM collector data. For IP_DEVICE(0), IP_PORT(1), IP_TRUNK(2), FOS_DEVICE(3), FC_PORT(4), GE_PORT(5), TE_PORT(6), HBA_PORT(7), CNA_PORT(8), VIRTUAL_FCOE_PORT(9), FCIP_TUNNEL(10), EE_MONITOR(11), IP_DEVICE_GROUP(12), IP_PORT_GROUP(13), VIRTUAL_GROUP(14), TRILL_TRUNK(15), ALL_SAN_PRODUCTS(16).	smallint	
MEASURE_ID	ID of the measure (MIB/Expression).	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId/virtualSwitchId, for port level it will use interfaceId/switchPortId/ fcipTunnelId/devicePortId.	int	
COLLECTOR_ID	DB ID of the pm_data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
SUM_VALUE	Named after SUM_VALUE to be consistent with column names in aggregated data tables. Stores the delta changes for counter values between two samples, only used for counter values, 0 for all other types of measures.	double precision	

TABLE 405 TIME_SERIES_DATA_2_1DAY

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when value of the measure retrieved from the corresponding target.	int	
TARGET_TYPE	Target type of the PM collector data. For IP_DEVICE(0), IP_PORT(1), IP_TRUNK(2), FOS_DEVICE(3), FC_PORT(4), GE_PORT(5), TE_PORT(6), HBA_PORT(7), CNA_PORT(8), VIRTUAL_FCOE_PORT(9), FCIP_TUNNEL(10), EE_MONITOR(11), IP_DEVICE_GROUP(12), IP_PORT_GROUP(13), VIRTUAL_GROUP(14), TRILL_TRUNK(15), ALL_SAN_PRODUCTS(16).	smallint	
MEASURE_ID	ID of the measure (MIB/Expression).	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId/virtualSwitchId, for port level it will use interfaceId/switchPortId/ fcipTunnelId/devicePortId.	int	
COLLECTOR_ID	DB ID of the pm_data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
VALUE	Stores One day aggregated data.	double precision	
MIN_VALUE	Minimum value in 2 hour table while aggregating 1 day data.	double precision	
MAX_VALUE	Maximum value in 2 hour table while aggregating 1 day data.	double precision	

TABLE 406 TIME_SERIES_DATA_2_2HOUR

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when value of the measure retrieved from the corresponding target.	int	
TARGET_TYPE	Target type of the PM collector data. For IP_DEVICE(0), IP_PORT(1), IP_TRUNK(2), FOS_DEVICE(3), FC_PORT(4), GE_PORT(5), TE_PORT(6), HBA_PORT(7), CNA_PORT(8), VIRTUAL_FCOE_PORT(9), FCIP_TUNNEL(10), EE_MONITOR(11), IP_DEVICE_GROUP(12), IP_PORT_GROUP(13), VIRTUAL_GROUP(14), TRILL_TRUNK(15), ALL_SAN_PRODUCTS(16).	smallint	
MEASURE_ID	ID of the measure (MIB/Expression).	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId/virtualSwitchId, for port level it will use interfaceId/switchPortId/ fcipTunnelId/devicePortId.	int	
COLLECTOR_ID	DB ID of the pm_data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	

TABLE 406 TIME_SERIES_DATA_2_2HOUR (Continued)

Field	Definition	Format	Size
VALUE	Stores the 2 hours aggregated data.	double precision	
MIN_VALUE	Minimum value in 30 min table while aggregating 2 hours of data.	double precision	
MAX_VALUE	Maximum value in 30 min table while aggregating 2 hours of data.	double precision	

TABLE 407 TIME_SERIES_DATA_2_30MIN

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when value of the measure retrieved from the corresponding target.	int	
TARGET_TYPE	Target type of the PM collector data. For IP_DEVICE(0), IP_PORT(1), IP_TRUNK(2), FOS_DEVICE(3), FC_PORT(4), GE_PORT(5), TE_PORT(6), HBA_PORT(7), CNA_PORT(8), VIRTUAL_FCOE_PORT(9), FCIP_TUNNEL(10), EE_MONITOR(11), IP_DEVICE_GROUP(12), IP_PORT_GROUP(13), VIRTUAL_GROUP(14), TRILL_TRUNK(15), ALL_SAN_PRODUCTS(16).	smallint	
MEASURE_ID	ID of the measure (MIB/Expression).	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId/virtualSwitchId, for port level it will use interfaceId/switchPortId/ fcipTunnelId/devicePortId.	int	
COLLECTOR_ID	DB ID of the pm_data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
VALUE	Stores the 30 minutes aggregated data.	double precision	
MIN_VALUE	Minimum value in raw performance statistics table while aggregating 30 minutes of data.	double precision	
MAX_VALUE	Maximum value in raw performance statistics table while aggregating 30 minutes of data.	double precision	

TABLE 408 TIME_SERIES_DATA_3

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when value of the measure retrieved from the corresponding target.	int	
TARGET_TYPE	Target type of the PM collector data.	smallint	
MEASURE_ID	ID of the measure (MIB/Expression).	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId/virtualSwitchId, for port level it will use interfaceId/switchPortId/ fcipTunnelId/devicePortId.	int	

TABLE 408 TIME_SERIES_DATA_3 (Continued)

Field	Definition	Format	Size
COLLECTOR_ID	DB ID of the pm_data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
VALUE	Stores the raw data received from the device.	double precision	
SUM_VALUE	Named after SUM_VALUE to be consistent with column names in aggregated data tables.Stores the delta changes for counter values between two samples, only used for counter values, 0 for all other types of measures.	double precision	

TABLE 409 TIME_SERIES_DATA_3_1DAY

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when value of the measure retrieved from the corresponding target.	int	
TARGET_TYPE	Target type of the PM collector data.	smallint	
MEASURE_ID	ID of the measure (MIB/Expression).	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId/virtualSwitchId, for port level it will use interfaceId/switchPortId/ fcipTunnelId/devicePortId.	int	
COLLECTOR_ID	DB ID of the pm_data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
VALUE	Stores One day aggregated data.	double precision	
MIN_VALUE	Minimum value in 2 hour table while aggregating 1 day data.	double precision	
MAX_VALUE	Maximum value in 2 hour table while aggregating 1 day data.	double precision	
SUM_VALUE	Named after SUM_VALUE to be consistent with column names in aggregated data tables.Stores the delta changes for counter values between two samples, only used for counter values, 0 for all other types of measures.	double precision	

TABLE 410 TIME_SERIES_DATA_3_2HOUR

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when value of the measure retrieved from the corresponding target.	int	
TARGET_TYPE	Target type of the PM collector data.	smallint	
MEASURE_ID	ID of the measure (MIB/Expression).	int	

TABLE 410 TIME_SERIES_DATA_3_2HOUR (Continued)

Field	Definition	Format	Size
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId/virtualSwitchId, for port level it will use interfaceId/switchPortId/ fcipTunnelId/devicePortId.	int	
COLLECTOR_ID	DB ID of the pm_data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
VALUE	Stores the 2 hours aggregated data.	double precision	
MIN_VALUE	Minimum value in 30 min table while aggregating 2 hours of data.	double precision	
MAX_VALUE	Maximum value in 30 min table while aggregating 2 hours of data.	double precision	
SUM_VALUE	Named after SUM_VALUE to be consistent with column names in aggregated data tables.Stores the delta changes for counter values between two samples, only used for counter values, 0 for all other types of measures.	double precision	

TABLE 411 TIME_SERIES_DATA_3_30MIN

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when value of the measure retrieved from the corresponding target.	int	
TARGET_TYPE	Target type of the PM collector data.	smallint	
MEASURE_ID	ID of the measure (MIB/Expression).	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId/virtualSwitchId, for port level it will use interfaceId/switchPortId/ fcipTunnelId/devicePortId.	int	
COLLECTOR_ID	DB ID of the pm_data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
VALUE	Stores the 30 minutes aggregated data.	double precision	
MIN_VALUE	Minimum value in raw performance statistics table while aggregating 30 minutes of data.	double precision	
MAX_VALUE	Maximum value in raw performance statistics table while aggregating 30 minutes of data.	double precision	
SUM_VALUE	Named after SUM_VALUE to be consistent with column names in aggregated data tables.Stores the delta changes for counter values between two samples, only used for counter values, 0 for all other types of measures.	double precision	

TABLE 412 TIME_SERIES_DATA_4

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when value of the measure retrieved from the corresponding target.	int	
TARGET_TYPE	Target type of the PM collector data.	smallint	
MEASURE_ID	ID of the measure (MIB/Expression).	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId/virtualSwitchId, for port level it will use interfaceId/switchPortId/ fcipTunnelId/devicePortId.	int	
COLLECTOR_ID	DB ID of the pm_data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
VALUE	Stores the raw data received from the device.	double precision	
SUM_VALUE	Named after SUM_VALUE to be consistent with column names in aggregated data tables.Stores the delta changes for counter values between two samples, only used for counter values, 0 for all other types of measures.	double precision	

TABLE 413 TIME_SERIES_DATA_4_1DAY

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when value of the measure retrieved from the corresponding target.	int	
TARGET_TYPE	Target type of the PM collector data.	smallint	
MEASURE_ID	ID of the measure (MIB/Expression).	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId/virtualSwitchId, for port level it will use interfaceId/switchPortId/ fcipTunnelId/devicePortId.	int	
COLLECTOR_ID	DB ID of the pm_data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
VALUE	Stores One day aggregated data.	double precision	
MIN_VALUE	Minimum value in 2 hour table while aggregating 1 day data.	double precision	
MAX_VALUE	Maximum value in 2 hour table while aggregating 1 day data.	double precision	
SUM_VALUE	Named after SUM_VALUE to be consistent with column names in aggregated data tables.Stores the delta changes for counter values between two samples, only used for counter values, 0 for all other types of measures.	double precision	

TABLE 414 TIME_SERIES_DATA_4_2HOUR

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when value of the measure retrieved from the corresponding target.	int	
TARGET_TYPE	Target type of the PM collector data.	smallint	
MEASURE_ID	ID of the measure (MIB/Expression).	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId/virtualSwitchId, for port level it will use interfaceId/switchPortId/ fcipTunnelId/devicePortId.	int	
COLLECTOR_ID	DB ID of the pm_data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
VALUE	Stores the 2 hours aggregated data.	double precision	
MIN_VALUE	Minimum value in 30 min table while aggregating 2 hours of data.	double precision	
MAX_VALUE	Maximum value in 30 min table while aggregating 2 hours of data.	double precision	
SUM_VALUE	Named after SUM_VALUE to be consistent with column names in aggregated data tables.Stores the delta changes for counter values between two samples, only used for counter values, 0 for all other types of measures.	double precision	

TABLE 415 TIME_SERIES_DATA_4_30MIN

Field	Definition	Format	Size
TIME_IN_SECONDS	Time when value of the measure retrieved from the corresponding target.	int	
TARGET_TYPE	Target type of the PM collector data.	smallint	
MEASURE_ID	ID of the measure (MIB/Expression).	int	
TARGET_ID	Target ID of the PM collector data. For device level collector it will use deviceId/virtualSwitchId, for port level it will use interfaceId/switchPortId/ fcipTunnelId/devicePortId.	int	
COLLECTOR_ID	DB ID of the pm_data_collector.	int	
MEASURE_INDEX	Stores the index_map value in case of an expression.	varchar	256
ME_ID	ME_ID of the target.	int	
VALUE	Stores the 30 minutes aggregated data.	double precision	
MIN_VALUE	Minimum value in raw performance statistics table while aggregating 30 minutes of data.	double precision	

TABLE 415 TIME_SERIES_DATA_4_30MIN (Continued)

Field	Definition	Format	Size
MAX_VALUE	Maximum value in raw performance statistics table while aggregating 30 minutes of data.	double precision	
SUM_VALUE	Named after SUM_VALUE to be consistent with column names in aggregated data tables.Stores the delta changes for counter values between two samples, only used for counter values, 0 for all other types of measures.	double precision	

TABLE 416 TOOL_APP

Field	Definition	Format	Size
TOOL_MENU_TEXT*	Text to be displayed for the Tool Menu.	varchar	256
TOOL_ID	A Tool in the TOOL_PATH table where the tools are defined.	int	
PARAMETERS	Default path for launching the tool.	varchar	256
KEY_STROKE	Short cut key stroke to the application.	varchar	30

TABLE 417 TOOL_PATH

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
TOOL_NAME	Name of the tool.	varchar	256
PATH	Path of the tool where installed or available.	varchar	1057
WORKING_FOLDER	Working folder for that application.	varchar	512

TABLE 418 TOPO_MAP_IMAGE

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
NAME	Image name in the foo.png format	varchar	256
IMAGE_OBJECT	'Image Object BLOB	bytea	

TABLE 419 TRILL

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
CLUSTER_ME_ID	The Management Element ID of the VCS Cluster in the VirtualSwitch	int	
SOURCE_ME_ID	The Management Element ID of the source VirtualSwitch.	int	
SOURCE_DOMAIN_ID	The source vcs member id	int	
SOURCE_PORT	The source port number as retrieved from the switch.	int	
SOURCE_PORT_NUMBER	The source port represented as a tuple of member/slot/port	char	30

TABLE 419 TRILL

Field	Definition	Format	Size
DEST_ME_ID	The Management Element ID of the destination VirtualSwitch.	int	
DEST_DOMAIN_ID	The destination vcs member id	int	
DEST_PORT	The dest port number as retrieved from the switch.	int	
DEST_PORT_NUMBER	The source port represented as a tuple of member/slot/port	char	30
COST	Cost for the given trill link	int	
TYPE	Type of the given trill link	smallint	
TRUSTED	Is this trill link trusted	smallint	
TRUNKED	Is this trill link part of a trunk	smallint	
CREATION_TIME	Time when the TRILL link record is created between source and destination.	timestamp	
MISSING	Is this trill link was discovered and is now missing	smallint	
MISSING_TIME	Time when the TRILL link is missing from the switch.	timestamp	
SOURCE_PORT_NAME	Switch port name for the source	char	30
DEST_PORT_NAME	Switch port name for the destination	char	30

TABLE 420 TRILL_TRUNK_GROUP

Field	Definition	Format	Size
ID	Primary key for this table. Serial number which is uniquely generated by DB.	int	
ME_ID	The Management Element ID of the VCS member in the VirtualSwitch	int	
MASTER_PORT_NUMBER	The master port represented as a tuple of member/slot/port	varchar	30

TABLE 421 TRILL_TRUNK_MEMBER

Field	Definition	Format	Size
GROUP_ID		int	
PORT_NUMBER	The source port represented as a tuple of member/slot/port	varchar	30

TABLE 422 TRUNK_GROUP_INTERFACE

Field	Definition	Format	Size
INTERFACE_ID		int	
VLAG	Specifies whether the lag is a vlag or not	smallint	

TABLE 423 TRUNK_GROUP_MEMBER

Field	Definition	Format	Size
TRUNK_GROUP_MEMBER_ID	Primary key for this table.	int	
INTERFACE_ID	Foreign key which refers INTERACE table.	int	
TRUNK_INTERFACE_ID	Foreign key which refers TRUNK_GROUP_INTERACE table.	int	
LAG_NAME	Lag name of the trunk.	varchar	64

TABLE 424 USER_

Field	Definition	Format	Size
ID *	Unique generated database identifier.	int	
NAME	User name.	varchar	128
DESCRIPTION	User description.	varchar	512
PASSWORD	User password.	varchar	512
EMAIL	User e-mail ID.	varchar	1024
NOTIFICATION_ENABLED	Flag for e-mail notification. Default value is 0.	smallint	
FULL_NAME	User''s Full Name.	varchar	512
PHONE_NUMBER	User''s Phone number.	varchar	32
INVALID_LOGIN_COUNT	This is a counter filed to identify the number of invalid login attempts. **NOTE:** After successful login this filed will be set to NULL. Default value is 0.	smallint	
LOCKED_OUT_DATETIME	The date time stamp when a user got locked out because of exceeding max number of invalid login attempts.	timestamp	
STATUS	User's account status: • 0=Disabled • 1=Enabled Default value is 1.	smallint	
SOURCE_OF_CREATION	To identify the source for creating the user account. • 0= User created through Management application Client • 1= User created when authenticated through external server. **NOTE:** At present there is no direct use of this field however this can be referred in future to build certain reports. Default value is 0.	smallint	
IP_PRODUCT_LOGIN_NAME	User CLI credential login user name.	varchar	256
IP_PRODUCT_LOGIN_PASSWORD	User CLI credential login password.	varchar	768

TABLE 424 USER_ (Continued)

Field	Definition	Format	Size
IP_PRODUCT_ENABLE_USER_NAME	User CLI credential enable user name.	varchar	256
IP_PRODUCT_ENABLE_PASSWORD	User CLI credential enable password.	varchar	768

TABLE 425 USER_AOR_MAP

Field	Definition	Format	Size
USER_NAME		varchar	128
AOR_ID	AOR ID where user has membership.	smallint	

TABLE 426 USER_DEFINED_DEVICE_DETAIL

Field	Definition	Format	Size
WWN	WWN of the device.	char	23
NAME	'Name of the device which is updated by the user.	varchar	256
TYPE	Type of the device (Initiator or Target.	varchar	32
IP_ADDRESS	IP address of the device which is updated by the user.	varchar	63
CONTACT	Contact detail of the device which is updated by the user.	varchar	256
LOCATION	Location of the device which is updated by the user.	varchar	256
DESCRIPTION	Description of the device which is updated by user.	varchar	256
USER_DEFINED_VALUE1	Value of the user defined property 1.	varchar	256
USER_DEFINED_VALUE2	Value of the user defined property 2.	varchar	256
USER_DEFINED_VALUE3	Value of the user defined property 3.	varchar	256

TABLE 427 USERDEFINED_NETWORK_SCOPE

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
NAME	Name of the Scope	varchar	128
USER_ID	Foreign Key USER_.ID. ID of the user who created the Custom Dashboard.	int	

TABLE 428 USERDEFINED_NETWORK_SCOPE_MEMBERSHIP

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
SCOPE_ID	Foreign Key USERDEFINED_NETWORK_SCOPE.ID. The ID of the user defined network scope to which this membership belongs.	int	

TABLE 428 USERDEFINED_NETWORK_SCOPE_MEMBERSHIP

Field	Definition	Format	Size
FABRIC_ID	Foreign Key FABRIC.ID. The ID of the fabric in the membership. This can be null if user does not include Fabric in his custom membership.	int	
PRODUCT_ME_ID	Foreign Key MANAGED_ELEMENT.ID. The ME ID of the device in the membership. This can be null if user does not include Switch in his custom membership.	int	
SWITCH_PORT_ID	Foreign Key SWITCH_PORT.ID. The ID of the switch Port in the membership. This can be null if user does not include Switch Port in his custom membership.	int	
INTERFACE_ID	Foreign Key INTERFACE. INTERFACE_ID. The ID of the Interface in the membership. This can be null if user does not include Interface in his custom membership.	int	
DEVICE_PORT_ID	Foreign Key DEVICE_PORT.ID. The ID of the Device Port in the membership. This can be null if user does not include Device Port in his custom membership.	int	

TABLE 429 USER_PREFERENCE

Field	Definition	Format	Size
USER_NAME *	User name whose preferences are saved. It corresponds to user_name in USER_table.	varchar	128
CATEGORY *	The name for a set of related preferences.	varchar	128
CONTENT	The set of preferences saved as name-value pairs.	text	

TABLE 430 USER_REALTIME_MEASURE_MAPPING

Field	Definition	Format	Size
ID	Primary Key.	int	
USER_ID	Foreign key reference to the user_ Table.	int	
EXPRESSION_ID	Foreign key reference to Measure Table.	int	
MIB_OBJECT_ID	Foreign key reference to Measure Table.	int	
MEASURE_TYPE	This identifies the collectible type. 0 for MIBs and 1 for Expressions.	int	

TABLE 431 USER_REALTIME_MEASURE_SETTING

Field	Definition	Format	Size
ID	Primary Key field for the user_realtime_measure_setting table	int	
USER_ID	This is the foreign key reference key to the user_ Table	int	
EXPRESSION_ID	This is the foreign key reference key to the snmp_expression Table	int	

TABLE 431 USER_REALTIME_MEASURE_SETTING (Continued)

Field	Definition	Format	Size
MIB_OBJECT_ID	This is the foreign key reference key to the mib_object Table	int	
TYPE	This identifies the collectible type. 0 for MIBs, 1 for Expressions	int	

TABLE 432 USER_RESOURCE_MAP

Field	Definition	Format	Size
USER_NAME*	User name.	varchar	128
RESOURCE_GROUP_ID*	Resource group name, which is mapped for the user.	int	

TABLE 433 USER_ROLE_MAP

Field	Definition	Format	Size
USER_NAME*	User name.	varchar	128
ROLE_ID*	Role ID, which is mapped for the user.	int	

TABLE 434 USER_STATE_MAP

Field	Definition	Format	Size
USER_NAME		varchar	128
STATE	Current user state. The possible values are: • 0 - Locked out by user manager • 1 - Locked Out Threshold Reached • 2 - Password Expired • 3 - Password History Policy Violated • 4 - Password Format Policy Violated **NOTE:** This numeric state value will be mapped to associated ENUM at DTO side	smallint	

TABLE 435 V_PORT_DETAIL

Field	Definition	Format	Size
DEVICE_PORT_ID	Primary key from the owner device port table.	int	
STATE	Flag to indicate whether port is online or offline	varchar	32
FCP_INITIATOR	The role of the virtual port; for example, FCP Initiator	varchar	256
SWITCH_IP	IP of the switch, the V port is connected to	varchar	128
VF_ID	VF ID for the V port	smallint	

TABLE 436 VCN_ICL

Field	Definition	Format	Size
VCN_ICL_ID	Virtual Cluster Node ICL DB ID.	int	
ICL_NAME	ICL name.	varchar	100

TABLE 436 VCN_ICL

Field	Definition	Format	Size
ICL_PORT_ID	ICL port foreign key.	int	
VCN_MEMBER_ID	Virtual Cluster Node member id foreign key.	int	

TABLE 437 VCN_MEMBER

Field	Definition	Format	Size
VCN_MEMBER_ID	Virtual Cluster Node member db id.	int	
CLUSTER_ID	Cluster id.	int	
CLUSTER_NAME	Cluster name.	varchar	100
CLUSTER_RBRIDGE_ID	Cluster rbridge id.	int	
SESSION_VLAN	Session VLAN id.	smallint	
KEEP_ALIVE_VLAN	Keep alive VLAN id.	smallint	
CLIENT_ISOLATION_MODE	Cluster isolation state: • Loose(0) • Strict(1).	smallint	
IS_CLIENTS_SHUTDOWN	Is MCT Client interfaces shutdown?	numeric	(1,0)
MEMBER_VLAN_RANGE	Configured member VLAN range.	varchar	256
ACTIVE_MEMBER_VLAN_RANGE	Active member VLAN range.	varchar	256
CLUSTER_DEPLOY_STATE	Cluster deployment state: • Deployed(0) • Undeployed(1).	smallint	
DEVICE_ID	Device id foreign key.	int	

TABLE 438 VCN_PEER

Field	Definition	Format	Size
VCN_PEER_ID	Virtual Cluster Node Peer db id.	int	
IP_ADDRESS	Peer ip address.	varchar	100
RBRIDGE_ID	Peer rbridge id.	int	
ICL_NAME	Cluster ICL name used for this peer.	varchar	100
FAST_FAILOVER_STATE	Cluster Peer fast failover state: • Disabled(0) • Enabled(1).	smallint	
KEEP_ALIVE_INTERVAL	Cluster Peer keep alive interval in seconds.	INET	
HOLD_TIME	Cluster Peer hold time in seconds.	int	
ACTIVE_MEMBER_VLAN_RANGE	Cluster Peer Active member VLAN range.	varchar	256
PEER_OPER_STATE	Cluster Peer operational state.	smallint	
PEER_DOWN_REASON	Cluster Peer down reason.	int	
PEER_UP_TIME	Cluster Peer up time.	int	

TABLE 438 VCN_PEER

Field	Definition	Format	Size
VCN_MEMBER_ID	Virtual Cluster Node member id foreign key.	int	
PEER_DEVICE_ID	Peer device id.	int	

TABLE 439 VCS_CLUSTER_MEMBER

Field	Definition	Format	Size
CLUSTER_ME_ID	The Management Element ID of the VCS Cluster in the VirtualSwitch.	int	
MEMBER_ME_ID	The Management Element ID of the cluster member in the VirtualSwitch.	int	
CREATION_TIME	Creation time of the record	timestamp	
TRUSTED	Describes whether the member is trusted. Possible values are 1 and 0. 1 means trusted and 0 means untrusted.	smallint	
MISSING	Describes whether the member is missing or not. Possible values are 1 and 0. 1 means missing and 0 means not missing	smallint	
MISSING_TIME	Time when the member gone missing.	timestamp	
STATE	Indicates the state of the member with respect to cluster. States can be Online, Offline, Rejoining etc.	varchar	64
FABRIC_STATUS	Stores the fabric level status of the node like Unknown and Online. Status is unknown when: • A node is going through a reboot or ISLs have not formed yet. • A node is not part of a cluster yet. Status is Online when: • A node is waiting to rejoin a cluster. • A node joins a cluster and all the ports are up and ISLs are formed.	varchar	64

TABLE 440 VCEM_PROFILE

Field	Definition	Format	Size
ID			
VERSION	Version of the VCEM server.	varchar	32
NETWORK_ADDRESS	The version number of the VCEM server.	varchar	128
PORT_NUMBER	The SOAP API port number on the VCEM server.	int	
USERNAME	The username to be used to logon to the VCEM server.	varchar	512
PASSWORD	The password to be used to logon to the VCEM server. Will be store encrypted.	varchar	512
DISCOVERY_STATUS	The current discovery status of the VCEM server (discovery pending, ,active, failed, deleted pending etc.).	smallint	

TABLE 440 VCEM_PROFILE (Continued)

Field	Definition	Format	Size
LAST_DISCOVERY_STATUS	The discovery status of the VCEM server in the previous discovery cycle.	smallint	
CREATION_TIME		timestamp	
LAST_UPDATE_TIME		timestamp	
LAST_FAILURE_TIMESTAMP	The time of the last failed collection.	timestamp	
LAST_SUCCESSFUL_TIMESTAMP	The time of the last successful collection.	timestamp	

TABLE 441 VIP_SERVER

Field	Definition	Format	Size
ID	Primary Key field for the VIP_SERVER	int	
TYPE	Even Policy Type • 0? Virtual Server • 1 ? Real Server	smallint	
DEVICE_ID	This is the foreign key reference key to the Device Table	int	
IP_ADDRESS	The IP Address for the Virtual Server or Real Server	varchar	128
NAME	The Name of Virtual Server or Real Server	varchar	256

TABLE 442 VIP_SERVER_BINDING

Field	Definition	Format	Size
ID	Primary Key field for the VIP_SERVER_BINDING	int	
DEVICE_ID	This is the foreign key reference key to the Device Table	int	
VIRTUAL_SERVER_IP_ADDRESS	The IP Address for the Virtual Server	varchar	128
VIRUTAL_SERVER_PORT	The Port number of the Virtual Server	int	
REAL_SERVER_IP_ADDRESS	The IP Address for the Real Server	varchar	128
REAL_SERVER_PORT	The Port Number for the Real Server	int	

TABLE 443 VIRTUAL_CIRCUIT_INTERFACE

Field	Definition	Format	Size
INTERFACE_ID		int	

TABLE 444 VIRTUAL_FCOE_PORT

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
VIRTUAL_SWITCH_ID	The unique id of switch the virtual fcoe port belongs to.	int	
PORT_WWN	WWN of port	varchar	64
PORT_SPEED	Will be 10G.	varchar	32
PORT_TYPE	Will be Virtual-FCoE-Port	varchar	16
ENABLED	Enabled/disabled	smallint	
STATUS	Status	varchar	64
TRUNK_INDEX	Trunk index	smallint	
PORT_NUMBER	Port number	smallint	
NAME	Name	varchar	64
SLOT_NUMBER	The Slot number in the switch to which this Virtual FCoE Port belongs	int	
VLAN_ID	Comma Separated values of the VLANs associated with this Virtual FCoE Port	varchar	64
DEVICE_COUNT	The number of devices associated with this Virtual FCoE Port. The default value is 0.	smallint	
PEER_MAC	The Peer FCF MAC if this Virtual FCoE Port is a FCoE VE-port	varchar	

TABLE 445 VIRTUAL_FCOE_PORT_MAC_MEMBER

Field	Definition	Format	Size
VIRTUAL_FCOE_PORT_ID	The unique id of virtual fcoe port the member belongs to	int	
MAC_ADDRESS	Mac address of member.	varchar	64

TABLE 446 VIRTUAL_FCOE_PORT_STAT

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
SWITCH_ID		int	
PORT_ID		int	
TX	The number of valid frames sent from the port	double precision	
RX	The number of valid frames received at this port	double precision	
TX_UTILIZATION	The computed value of TX based on speed of port (for MarchingAnts)	double precision	
RX_UTILIZATION	The computed value of RX based on speed of port (for MarchingAnts)	double precision	

TABLE 446 VIRTUAL_FCOE_PORT_STAT (Continued)

Field	Definition	Format	Size
CREATION_TIME	The time this stats record was created	timestamp	
ACTIVE_STATE	Used for error scenario	smallint	
LINK_FAILURES	Link failures	double precision	
TX_LINK_RESETS	TX Link resets	double precision	
RX_LINK_RESETS	RX link resets	double precision	
SYNC_LOSSES	Synchronization losses	double precision	
SIGNAL_LOSSES	Signal losses	double precision	
SEQUENCE_ERRORS	Sequence Errors	double precision	
INVALID_TX	Invalid transmissions	double precision	
CRC_ERRORS	Cyclic Redundancy check error	double precision	

TABLE 447 VIRTUAL_PORT_WWN_DETAILS

Field	Definition	Format	Size
ID	Unique generated database identifier.		
SWITCH_ID	If the VPWWN is constructed based on AG Node WWN and AG_Port_Index then this is id of connected switch.	int	
SWITCH_PORT_NUMBER	If the VPWWN is configured for AG , this value will have the default value(-1).	smallint	
AG_NODE_WWN	If the VPWWN is configured for Switch Port , this value will have the default value.	char	23
AG_PORT_NUMBER	If the VPWWN is configured for Switch Port , this value will have the default value.	smallint	
TYPE	Active WWN 0-Auto is the switch created VPWWN and User is user defined VPWWN'; 1-User	smallint	
STATUS	Enable or disable the VPWWN feature on switch port or AG-port. • 1-Enabled • 0-disabled	smallint	
USER_VPWWN	User created VPWWN.	char	23
AUTO_VPWWN	VPWWN created by Switch.	char	23

TABLE 447 VIRTUAL_PORT_WWN_DETAILS (Continued)

Field	Definition	Format	Size
DEVICE_PORT_WWN	Physical port WWN of the device for which VPWWN is assigned.	char	23
SLOT_NUMBER	Slot number of the switch, This will be -1 for AG.	smallint	

TABLE 448 VIRTUAL_SWITCH

Field	Definition	Format	Size
ID*	Primary key for the table.	int	
NAME	Stores the switch name.	varchar	64
WWN	WWN of the Switch.	char	23
VIRTUAL_FABRIC_ID	Virtaul fabric ID of the switch. A positive value will be stored if VF is enabled else -1.	smallint	
DOMAIN_ID	Domain ID of the switch.	smallint	
BASE_SWITCH	Indidates whether its a base switch. 1 is base switch and 0 is not.	smallint	
SWITCH_MODE	Stores the switch mode. • 0 is switch mode • 2 is ag mode.	smallint	
ROLE	Stores the role of the switch like Primary, Subordinate, Cluster etc.	varchar	32
FCS_ROLE	FCS role for the Switch . This is used only when FCS policy is turned on.	varchar	16
AD_CAPABLE	Stores the switch capability for Admin domain. • 1 is capable • 0 is not capable.	smallint	
FABRIC_IDID_MODE	Denotes if Insistent Domain ID mode is enabled.	smallint	
OPERATIONAL_STATUS	Stores the operational status of the switch.	varchar	128
MAX_ZONE_CONFIG_SIZE	Denotes the maximum supported zone DB size in bytes.	int	
CREATION_TIME	Creation time of the record.	timestamp	
LAST_UPDATE_TIME	Stores the timestamp of the last database update.	timestamp	
USER_NAME	Stores the telnet user name used to login to switch.	varchar	128
PASSWORD	Password used to login to the switch.	varchar	128
MANAGEMENT_STATE	Management state of the switch. This is a bit mask that indicates the switches manageability state, like switch not reachable, credentials invalid, not ready for manangement etc . • 0 means management state is Ok • non zero value will indicate manageability issues.	bigint	
STATE	Stores the switch state like Online, offline etc.	varchar	32
STATUS	Stores the status value here : UNKNOWN(0), MARGINAL(2),DOWN(3),HEALTHY(1).	varchar	32

TABLE 448 VIRTUAL_SWITCH (Continued)

Field	Definition	Format	Size
STATUS_REASON	Stores the status reason, which states the contributors for the status.	varchar	2048
USER_DEFINED_VALUE_1	User defined value used for annotation.	varchar	256
USER_DEFINED_VALUE_2	User defined value used for annotation.	varchar	256
USER_DEFINED_VALUE_3	User defined value used for annotation.	varchar	256
CORE_SWITCH_ID	Reference to Core Switch record.	int	
INTEROP_MODE	Interop mode for the switch. • 0 is native • 2 is McData • 3 is open fabric.	smallint	
CRYPTO_CAPABLE	Stores the switch capability for crypto support . • 1 is capable • 0 is not capable.	smallint	
FCR_CAPABLE	Stores the switch capability for FCR support . • 1 is capable • 0 is not capable.	smallint	
FCIP_CAPABLE	Stores the switch capability for FCIP support . • 1 is capable • 0 is not capable.	smallint	
FCOE_CAPABLE	If the switch supports FCoE. Default value is 0.	smallint	
L2_CAPABLE	If the switch supports L2.	smallint	
L3_CAPABLE	If the switch supports L3.	smallint	
LF_ENABLED	Logical Fabric Enabled/Disabled for a Virtual Switch. Default value is 0.	smallint	
DEFAULT_LOGICAL_SWITCH	Check to see whether virtual switch is a default logical switch or not. 1 is true and 0 is false. Default value is 0.	smallint	
FEATURES_SUPPORTED	Contains the features supported as a bit mask. Default value is 0.	int	
FMS_MODE	Stores FMS mode in FICON environment.	smallint	
DYNAMIC_LOAD_SHARING	Stores the switch capability for dynamic load sharing, • 1 is capable • 0 is not capable.	smallint	
PORT_BASED_ROUTING	Indicates whether the port based routing is present. • 1 is present • 0 is absent.	smallint	
IN_ORDER_DELIVERY	Indicates whether in order delivery is enabled or disabled. • 1 is enabled • 0 is disabled.	smallint	

TABLE 448 VIRTUAL_SWITCH (Continued)

Field	Definition	Format	Size
INSISTENT_DID_MODE	Indicates whether persistent domain ID is enabled on the switch. • 1 is enabled • 0 is disabled.	smallint	
LAST_SCAN_TIME	Stores the timestamp of the last scan time, the time which the switch was contacted for update.	timestamp	
DOMAIN_MODE_239	Stores the domain mode offset. Its only used in the mixed fabric (FOS+EOS).	smallint	
DOMAIN_ID_OFFSET	Stores the domain id offset value. Its only used in the mixed fabric (FOS+EOS).	smallint	
PREVIOUS_OPERATIONAL_STATUS	This table can hold the same values as OEPRATION_STATUS column. But this will be holding the previous OPERATIONAL_STATUS of the Virtual switch. These values to be populated by FCS during Fabric Refresh task	varchar	128
FCOE_LOGIN_ENABLED	The FCoE Login Management Status of the switch. Default value is 0.	smallint	
FCIP_CIRCUIT_CAPABLE	Whether the switch can create FCIP Circuits. 1 means true and 0 means false. Default value is 0.	smallint	
DISCOVERED_PORT_COUNT	Reflects the number of managed ports in the discovered switch. Default value is 0.	smallint	
LAST_PORT_MEMBERSHIP_CHANGE	Stores the timestamp of the last port member ship update.	bigint	
MAX_FCIP_TUNNELS	The maximun number of tunnels that can be created in this switch,-1 means not supported. Default value is -1.	int	
MAX_FCIP_CIRCUITS	The maximun number of circuits that can be created in this switch, -1 means not supported. Default value is -1.	int	
FCIP_LICENSED	FCIP Advanced Extension Licensing is available. 1 means licensed and 0 means not licensed, -1 means not supported. Default value is -1.	smallint	
ADDRESSING_MODE	This column to represent the logical switch addressing modes to assign Port Addresses, There are three different addressing modes supported. Fixed (0), Flat or 10 bit (1), Dynamic (2). Default value is -1.	smallint	
PREVIOUS_STATE	This fields copies the old state of the switch . The field could be used to track the state change information for the switch.These values to be populated by FCS during Fabric Refresh task.SMIA requested this information but could be used by any module which needs to track the state change	varchar	32

TABLE 448 VIRTUAL_SWITCH (Continued)

Field	Definition	Format	Size
MANAGED_ELEMENT_ID	A unique managed element ID for this virtual switch. Also a foreign key reference to the MANAGED_ELEMENT table.	int	
HIF_ENABLED	The HIF Enabled bit on the switch. Values are 1 for enabled and 0 for not enabled. -1 the default, stands for not supported and will be used for older firmwares. Default value is -1.	smallint	
CLUSTER_MODE	This column is used to determine whether VCS Cluster is in Standalone mode or Cluster mode. The values will be populated by the VCS collector during the discovery of the VCS switch. The default value of -1 means that its a non VCS device. Following Enum will be defined as NON_VCS(-1), STANDALONE(0), CLUSTER(1).	smallint	
VCS_ID	This column is used to store the VCS ID of the device. The value will be populated by the NosSwitchAssetCollector during the discovery of the VCS Cluster. The non zero value will be stored as VCS ID. Default value is -1.	smallint	
CLUSTER_TYPE	This column is used to determine whether VCS is in Fabric Cluster or Logical Chassis. The values are populated by the VCS collector during the discovery of the VCS switch. The default value -1 means that its a non-VCS device. Following are the values and their types: • 0 - Unknown • 1 - Standalone • 2 - Fabric Cluster • 3 - Logical Chassis	smallint	
SWITCH_ID	Represents the Switch embedded port destination identifier.	int	
MONITORED	To identify whether the switch is monitored or unmonitored. 0 is Unmonitored and 1 is Monitored.	int	
FEATURES_ENABLED	Holds as a bit mask the features that are active / enabled. Each bit would represent features like Lossless etc.	int	
MAPS_ENABLED_ACTIONS	Bitmask of Maps actions enabled on the switch. 0-None, 1-Raslog, 2-SNMP, 4-Email, 8-Fence Port, 16-SW Down, 32-SW Marginal	int	
FABRIC_STATUS	Stores the fabric level status of the node like Unknown and Online. Status is Unknown when: • A node is going through a reboot or ISLs have not formed yet. • A node is not part of a cluster yet. Status is Online when: • A node is waiting to rejoin a cluster. • A node joins a cluster and all the ports are up and ISLs are formed.	varchar	64

TABLE 449 VIRTUAL_SWITCH_CAPABILITY

Field	Definition	Format	Size
VIRTUAL-SWITCH_ID *	DB ID of virtual switch.	int	
CAPABILITY_ *	Name of capability detected on virtual switch.	varchar	256
ENABLED	1 = the capability is enabled on the virtual switch.	int	

TABLE 450 VIRTUAL_SWITCH_CHECKSUM

Field	Definition	Format	Size
VIRTUAL_SWITCH_ID *	DB ID of virtual switch.	int	
CHECKSUM_KEY *	Checksum key.	varchar	32
CHECKSUM	Checksum value.	varchar	16

TABLE 451 VIRTUAL_SWITCH_COLLECTION

Field	Definition	Format	Size
VIRTUAL_SWITCH_ID *	DB ID of virtual switch.	int	
COLLECTOR_NAME *	Collector name.	varchar	256
LAST_VIRTUAL_SW_ MODIFICATION	Last modified time on switch.	timestamp	

TABLE 452 VLAN

Field	Definition	Format	Size
VLAN_DB_ID	Unique database generated identifier.	int	
DEVICE_ID	Database ID of the DEVICE instance which is associated with the vlan.	int	
NAME	Name for vlan.	varchar	128
TABLE_SUBTYPE	Table subtype possible value is VLAN.	varchar	32

TABLE 453 VLAN_DYNAMIC_INTERFACE_MEMBER

Field	Definition	Format	Size
VLAN_INTERFACE_RELATION_ID	Database ID of the VLAN_INTERFACE_RELATION instance which is associated with the dynamic interface member.	int	

TABLE 454 VLAN_EXCLUDED_INTERFACE

Field	Definition	Format	Size
VLAN_INTERFACE_RELATION_ID	Database ID of the VLAN_INTERFACE_RELATION instance which is associated with the excluded interface member.	int	

TABLE 455 VLAN_INTERFACE_MEMBER

Field	Definition	Format	Size
VLAN_INTERFACE_RELATION_ID	Database ID of the VLAN_INTERFACE_RELATION instance which is associated with the interface member.	int	

TABLE 456 VLAN_INTERFACE_RELATION

Field	Definition	Format	Size
VLAN_INTERFACE_RELATION_ID	Unique database generated identifier.	int	
VLAN_DB_ID	Database ID of the VLAN instance which is associated with the interface.	int	
INTERFACE_ID	Database ID of the INTERFACE instance which is associated with the vlan.	int	
TABLE_SUBTYPE	Table subtype possible value is VLAN_INTERFACE_RELATION.		

TABLE 457 VLAN_INT_C_TAG_RELATION

Field	Definition	Format	Size
VLAN_INTERFACE_RELATION_ID	Foreign Key Reference to VLAN_INTERFACE_RELATION table.	int	
C_TAG_ID	This as an Incoming customer tag (c-tag) associated with a GVLAN and its applicable only for trunk mode. If the TLS (Transparent LAN Service) is enabled in the device, a pre-defined range of values are used for C-Tag.	text	

TABLE 458 VLAN_INT_MAC_GROUP_RELATION

Field	Definition	Format	Size
VLAN_INTERFACE_RELATION_ID	Foreign Key Reference to VLAN_INTERFACE_RELATION table.	int	
MAC_GROUP_DB_ID	Foreign key Reference to ID field of MAC_GROUP table.	text	

TABLE 459 VLAN_STATIC_INTERFACE_MEMBER

Field	Definition	Format	Size
VLAN_INTERFACE_RELATION_ID	Database ID of the VLAN_INTERFACE_RELATION instance which is associated with the static interface member.	int	

TABLE 460 VLL_DEVICE_RELATION

Field	Definition	Format	Size
MPLS_SERVICE_DEVICE_RELATION_DB_ID	Database ID inherited from MPLS_SERVICE_DEVICE_RELATION.	int	
VLL_DEVICE_RELATION.VLL_MODE	Represents the VLL mode. Possible values are Unknown-0, Raw-1 and Taggged-2.	int	

TABLE 461 VLL_ENDPOINT_RELATION

Field	Definition	Format	Size
MPLS_SERVICE_ENDPOINT_RELATION_DB_ID	Database ID inherited from MPLS_SERVICE_ENDPOINT_RELATION.	int	
PW_ENET_PW_INSTANCE	Represents the Index of Ethernet tables associated with this endpoint Instance.	int	
COS	This value indicates the Class Of Service for this endpoint. For VLL, this value is used to select the appropriate tunnel whose COS value is either same, or almost approaching this value. For VLL-local, this value is applied to the ingress packet of an endpoint. Allowed range is 0-7 and 255. 255 means COS is not explicitly configured.	smallint	

TABLE 462 VMOTION_EVENT

Field	Definition	Format	Size
ID	Uniquely identifies the vmotion event.	int	
SOURCE_HOST_NAME	The name of the source host at the time of the vmotion.	varchar	256
SOURCE_IP_ADDRESS	IP address of the source host at the time of the vmotion.	varchar	128
SOURCE_HOST_UUID	The uuid assigned by the hypervisor to the source host.	varchar	64
DEST_HOST_NAME	The name of the destination host at the time of the vmotion.	varchar	256
DEST_IP_ADDRESS	IP address of the destination host at the time of the vmotion.	varchar	128
DEST_HOST_UUID	The uuid assigned by the hypervisor to the destination host. This can be null in case of a failed vmotion.	varchar	64
SOURCE_DATACENTER_NAME	Source Datacenter name.	varchar	256
DEST_DATACENTER_NAME	Destination Dataccenter name. Can be null in case of a failed vmotion.	varchar	256
VM_UUID	Unique identifier for the VM to identify that VM across vmotions.	varchar	64
VM_NAME	User-assigned name for the VM.	varchar	80
VM_IP_ADDRESS	The primary IPv4 or IPv6 address used by the VM on the management LAN, if any.	varchar	32
VCENTER_HOST	The FQDN or the ip address of the vcenter.	varchar	256
VNIC_MACS	Comma separated vnic mac addresses.	varchar	256
START_TIME	Start time of the vmotion event.	timestamp	
END_TIME	End time of the vmotion event, could be null cause of a failed vmotion.	timestamp	

TABLE 462 VMOTION_EVENT (Continued)

Field	Definition	Format	Size
STATUS	VMotion event status. 0 = info, 1 = warning, 2 = failed.	smallint	
DRS_TRIGGERED	Identifies whether the events was due to DRS. 0 = No, 1 = Yes.	smallint	
USER_NAME	Identifies that user who initiated the vmotion.	varchar	80
DESCRIPTION	Event message that is received.	varchar	256

TABLE 463 VMOTION_PNIC_DETAILS

Field	Definition	Format	Size
ID	Identifies an entry for the source or destination pnic and the connected switch details.	int	
VMOTION_EVENT_ID	Foreign key to the vmotion_event table.	int	
PNIC_TYPE	Pnic type. 0 = source, 1 = destination, identifies if the pNIC is from the source or the destination host.	smallint	
PNIC_MAC	Physical Nic mac addresse of the connected Pnic on the host.	varchar	256
PORT_PROFILES	Comma separated PP Name-SwitchName for all the port profiles associated with the vNics that are being migrated as a result of the vmotion.	varchar	256
SWITCH_NAME	Switch names entry for connected switch to the pNic.	varchar	256
SWITCH_IP_ADDRESS	Switch ip addresses entries for connected switch to the pNic.	varchar	256

TABLE 464 VM_DATA_CENTER

Field	Definition	Format	Size
ID	Unique generated database identifier.		
NAME	Data center name.	varchar	256
VCENTER_ID	Id of the vCenter server managing this Data center.	int	
MOR_ID	The managed object reference number assigned by the hypervisor.	int	

TABLE 465 VM_DATASTORE_DETAILS

Field	Definition	Format	Size
ID	Primary key.	int	
DATACENTER_ID	Foreign to vm_data_center.	int	

TABLE 465 VM_DATASTORE_DETAILS

Field	Definition	Format	Size
NAME	Name of the datastore.	varchar	256
ACCESSIBLE	The connectivity status of this datastore. If this is set to false, meaning the datastore is not accessible, this datastores capacity and freespace properties cannot be validated. 0 = no 1 = yes.	smallint	
STATUS	Status of the datastore could be normal, enteringMaintenance, inMaintenance.	varchar	20
FILE_SYSTEM_TYPE	Type of file system volume, such as VMFS or NFS.	varchar	20
TOTAL_CAPACITY	Maximum capacity of this datastore, in bytes. This value is updated periodically by the server.	bigint	
FREE_SPACE	Available space of this datastore, in bytes. The server periodically updates this value.	bigint	
LAST_UPDATE_TIME	Time when the free-space and capacity values in DatastoreInfo and DatastoreSummary were updated.	timestamp	
RDM_SUPPORTED	Flag Indicates whether or not raw disk mappings can be created on this datastore. 0 = no 1 = yes.	smallint	
PERFILE_THIN_PROVISIONING_SUPPORTED	Flag indicating whether or not the per file thin provisioning is supported or not. 0 = no 1 = yes. When thin provisioning is used, backing storage is lazily allocated.	smallint	
STORAGE_IORM_SUPPORTED	Indicates whether the datastore supports Storage I/O Resource Management. 0 = no 1 = yes.	smallint	
DIRECTORY_HIERARCHY_SUPPORTED	Indicates whether or not directories can be created on this datastore. 0 = no 1 = yes.	smallint	
LOCATION	The unique locator for the datastore.	varchar	256
MOR_ID	The managed object reference number assigned by the hypervisor.	int	

TABLE 466 VM_DV_PORT

Field	Definition	Format	Size
VM_DV_SWITCH_ID	Foreign key to the VM_DVSWITCH table. The dvSwitch on which this port group exists.	int	
VM_DV_PORT_GROUP_ID	Foreign Key to the VM_DV_PORTGROUP table. The dvPortgroup in which this dvPort instance may exist (in case it's not a standalone port)	int	
NAME	The name of the port	varchar	256
DESCRIPTION	A description string of the port.	varchar	256

TABLE 466 VM_DV_PORT (Continued)

Field	Definition	Format	Size
CONFLICT	Whether the port is a conflict port. A port could be marked as conflict if an entity is discovered connecting to a port that is already occupied, or if the port is created by the host without conferring with Virtual Center Server. A conflict port will not have its runtime state persisted and the port can''t move away from the host, i.e no vMotion if a Virtual Machine is using a conflict port	smallint	
CONNECTEE_TYPE	The type of the connectee. One of: hostConsoleVnic hostVmkVnic pnic vmVnic	smallint	
CONNECTEE_ADDRESS_HINT	A hint on address info of the nic that connects to this port	varchar	256
MTU	The MTU of the port. Currently, this property can only be set at the switch level. Attempt to change it at the portgroup or port level will raise exception	int	
MAC_ADDRESS	The mac address that is used at this port	varchar	64
RUNTIME_LINK_UP_STATE	Whether the port is in linkUp status	varchar	128
RUNTIME_LINK_PEER	The name of the connected entity	varchar	128
RUNTIME_BLOCKED	Whether the port is blocked by switch implementation	smallint	
TRUNKING_MODE	True if the port VLAN tagging/stripping is disabled	smallint	
VLAN_IDS	The VLAN id of the port	varchar	256
PROXY_HOST_NAME	The host that services this port	varchar	256
KEY	The key for the port	varchar	64
MOR_ID	The managed object reference number assigned by the hypervisor	int	

TABLE 467 VM_DV_PORT_GROUP

Field	Definition	Format	Size
VM_DV_SWITCH_ID	Foreign Key to the vm_dvswitch table. The dvSwitch on which this port group exists	int	
NAME	The name of the portgroup.	varchar	256
NUM_PORTS	Number of ports in the portgroup	int	
TYPE	The type of portgroup. One of: earlyBinding ephemeral lateBinding	smallint	

TABLE 467 VM_DV_PORT_GROUP (Continued)

Field	Definition	Format	Size
DESCRIPTION	A description string of the portgroup	varchar	256
UPLINK_PORT_GROUP	Whether this portgroup is an uplink portgroup	smallint	
KEY	The key for the port group	varchar	64
MOR_ID	The managed object reference number assigned by the hypervisor	int	

TABLE 468 VM_DV_SWITCH

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
UUID	The generated UUID of the switch. Unique across VC inventory and instances	varchar	256
NAME	The name of the switch	varchar	256
MAX_PORTS	The maximum number of ports allowed in the switch, not including conflict ports	int	
DESCRIPTION	A description string of the switch	varchar	1024
PORT_COUNT	Current number of ports, not including conflict ports	int	
STANDALONE_PORT_COUNT	The number of standalone ports in the switch. Standalone ports are ports that don"t belong to any portgroup	int	
ADMIN_NAME	The name of the person that is responsible for the switch	varchar	256
ADMIN_CONTACT	The contact information for the person	varchar	256
BUILD	Build string for the server on which this call is made. For example, x.y.z-num. This string does not apply to the API	varchar	256
PRODUCT_NAME	Short form of the product name	varchar	256
VENDOR_NAME	Name of the vendor of this product	varchar	256
VERSION	Dot-separated version string. For example, "1.2"	varchar	256
FORWARDING_CLASS	Forwarding class of the distributed virtual switch	varchar	256
DV_PORT_GROUP_OPER_SUPPORTED	Whether this switch allow Virtual Center users to modify DVS configuration at portgroup level, except for host memeber, policy and scope operations	smallint	
DV_PORT_OPER_SUPPORTED	Whether this switch allow Virtual Center users to modify DVS configuration at port level, except for host memeber, policy and scope operations	smallint	

TABLE 468 VM_DV_SWITCH (Continued)

Field	Definition	Format	Size
DVS_OPER_SUPPORTED	Whether this switch allow Virtual Center users to modify DVS configuration at switch level, except for host memeber, policy and scope operations	smallint	
CREATION_TIME	The create time of the switch	timestamp	
UPLINK_PORT_NAME	The uniform name of uplink ports on each host	varchar	256
VM_DATA_CENTER_ID	A foreign key referencing VM_DATACENTER table instance to which this host is associated with	int	
MOR_ID	The managed object reference number assigned by the hypervisor	int	
IP_ADDRESS	The IP address currently assigned to the DV switch.	varchar	64
IPFIX_ENABLED	Whether netflow is enabled on the dvswitch, 0 implies false and 1 implies that its enabled.	smallint	
DISCOVERY_PROTOCOL	Neighbor discovery protocol 0 = CDP else 1 which is LLDP.	smallint	
DISCOVERY_OPERATION	Discovery operation default is 0 = listen, 1= advertise, 2 = both, 3 = none.	smallint	
CDP_ENABLED	Whether CDP is enabled on the dvswitch, 0 implies false and 1 implies that its enabled.	smallint	
VSPAN_ENABLED	Whether Port Mirroring is enabled on the dvswitch, 0 implies false and 1 implies that its enabled.	smallint	
MAXIMUM_MTU	The maximum transmission unit (MTU) associated with this distributed virtual switch in bytes.	int	

TABLE 469 VM_DV_SWITCH_HOST_MEMBER

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
VM_DV_SWITCH_ID	A foreign key referencing VM_DV_SWITCH (ID)	int	
VM_HOST_ID	A foreign key referencing VM_HOST (ID)	int	

TABLE 470 VM_FC_HBA

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
NODE_WWN	The world wide node name for the adapter	varchar	23
PORT_WWN	The world wide port name for the adapter	varchar	23

TABLE 470 VM_FC_HBA (Continued)

Field	Definition	Format	Size
PORT_TYPE	The type of the fiber channel port. One of : • Fabric • Loop • Point to point • Unknown	smallint	
SPEED	The current operating speed of the adapter in bits per second.	varchar	64
BUS	The host bus number	int	
DEVICE_NAME	The device name of host bus adapter	varchar	256
DRIVER	The name of the driver	varchar	256
MODEL	The model name of the host bus adapter	varchar	256
PCI	The Peripheral Connect Interface (PCI) ID of the device representing the host bus adapter	varchar	256
STATUS	The operational status of the adapter. Valid values include : online offline fault	smallint	
VM_HOST_ID	A foreign key referencing VM_HOST table instance to which this host is associated with	int	
MOR_ID	The managed object reference number assigned by the hypervisor	int	

TABLE 471 VM_FC_HBA_DEVICE_PORT_MAP

Field	Definition	Format	Size
DEVICE_PORT_ID	A foreign key referencing DEVICE_PORT table instance to which this host is associated with	int	
VM_FC_HBA_ID	A foreign key referencing VM_FC_HBA table instance to which this host is associated with	int	

TABLE 472 VM_HOST

Field	Definition	Format	Size
DEVIE_ENCLOSURE_ID	Identifies a server running a supported hypervisor. The ID value is the same as the ID of the corresponding DEVICE_ENCLOSURE record.	int	
NODE_WWN	The Node WWN for this host.	char	23
HYPERVISOR_NAME	Hypervisor name and version, such as VMware ESX Server v3.5.0	varchar	64
HYPERVISOR_TYPE	Numeric hypervisor type ID. 1 = VMware, 2 = Hyper-V. The default value is 0.	smallint	
CPU_COUNT	Number of CPUs in the server. The default value is 0.	int	

TABLE 472 VM_HOST (Continued)

Field	Definition	Format	Size
CPU_TYPE	Text summary of CPU hardware, such as: Intel(R) Xeon(TM) CPU 2.6 GHz	varchar	64
CPU_RESOURCES	Text summary of CPU resources, such as "20 GHz total, 15 GHz reserved". May be a different format for different VM vendors	varchar	64
MEM_RESOURCES	Text summary of memory resources, such as "7 GB total, 5 GB reserved". May be a different format for different VM vendors	varchar	64
LICENSE_SERVER	IP address or hostname of VM Hypervisor"s license server.	varchar	128
BOOT_TIME	Date and time that the host was last started	timestamp	
VM_DATACENTER_ID	A foreign key referencing VM_DATACENTER table instance to which this host is associated with.	int	
DVS_HOSTMEMBER_STATUS	• 1 - disconnected The host is in disconnected or not responding state. • 2 - down The host component is down. • 3 - outOfSync The switch configuration in the host component is not the same as the configuration in VirtualCenter server. • 4 - pending The host component is waiting to be initialized. • 5 - up The host component is up and running. • 6 - warning The host requires attention.	smallint	
DVS_PRODUCT_NAME	Short form of the product name of proxy switch module of a dvSwitch.	varchar	256
DVS_PRODUCT_VENDOR	Name of the vendor of this product.	varchar	256
DVS_PRODUCT_VERSION	Dot-separated version string. For example, "1.2".	varchar	256
CLUSTER_NAME	The name of the cluster of which this host is a member of.	varchar	256
MOR_ID	The managed object reference number assigned by the hypervisor.	int	
UUID	UUID to uniquely identify the host.	varchar	64

TABLE 473 VM_HOST_END_DEV_CONNECTIVITY

Field	Definition	Format	Size
VM_PHYSICAL_NIC_ID	A foreign key referencing VM_PHYSICAL_NIC (ID)	int	
INTERFACE_ID	A foreign key referencing INTERFACE (ID)	int	

TABLE 474 VM_HOST_PROXY_SWITCH

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
VM_HOST_ID	Foreign Key to the vm_host table	int	

TABLE 474 VM_HOST_PROXY_SWITCH (Continued)

Field	Definition	Format	Size
DVS_NAME	The name of the DistributedVirtualSwitch that the HostProxySwitch is part of	varchar	256
DVS_UUID	The uuid of the DistributedVirtualSwitch that the HostProxySwitch is a part of	varchar	256
KEY_	The proxy switch key	varchar	256
NUM_PORTS	The number of ports that this switch currently has	int	
NUM_PORTS_AVAILABLE	The number of ports that are available on this virtual switch	int	
UPLINK_PORT_NAMES	The list of ports that can be potentially used by physical nics. This property contains the names of such ports	varchar	256

TABLE 475 VM_HOST_PROXY_SWITCH_PNIC_SPEC

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
VM_HOST_PROXY_SWITCH_ID	Foreign Key to the vm_host_proxy_switch table	int	
PNIC_DEVICE	The physical NIC to be added in the switch	varchar	256
UPLINK_PORT_GROUP_KEY	The key of the portgroup to be connected to the physical NIC	varchar	256
UPLINK_PORT_KEY	The key of the port to be connected to the physical NICs	varchar	256
UPLINK_PORT_NAME	The name of the port to be connected to the physical NICs	varchar	256

TABLE 476 VM_HOST_VIRTUAL_NIC

Field	Definition	Format	Size
ID	Unique Auto Generated DB ID.	serial	
DEVICE_NAME	Device Name for the virtual NIC.	varchar	256
MAC	The media access control (MAC) address of the virtual network adapter	varchar	64
DHCP_ENABLED	The flag to indicate whether or not DHCP (dynamic host control protocol) is enabled. If this property is set to true, the ipAddress and the subnetMask strings cannot be set explicitly	smallint	
IP_ADDRESS	The IP address currently used by the network adapter. All IP addresses are specified using IPv4 dot notation	varchar	128
SUBNET_MASK	Subnet mask for the virtual NIC.	varchar	64
VM_STD_VSWITCH_PORT_GROUP_ID	Foreign Key to the VM_STD_VSWITCH_PORT_GROUP table. Port group with which this vmknic is associated	int	

TABLE 476 VM_HOST_VIRTUAL_NIC (Continued)

Field	Definition	Format	Size
VM_DV_PORT_ID	Foreign key to the vm_dv_port table. DV Port with which this vmknic is associated	int	
MTU	The MTU of the port	int	
VM_HOST_ID	FOREIGN KEY to the vm_host table	int	
MOR_ID	The managed object reference number assigned by the hypervisor	int	
PORT_GROUP_KEY	The key for the port group	varchar	256
BINARY_MAC	MAC address in binary format.	bytea	
BINARY_IP	IP address in binary format.	bytea	

TABLE 477 VM_NETWORK_SETTINGS

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
VLAN_TYPE	One of: Private VLAN Trunk VLAN Access VLAN	smallint	
VLAN_IDS	Single or range of VLANs configured on the port	varchar	256
BLOCKED	Whether this port is blocked, i.e. packet forwarding is stopped	int	
VM_STD_VSWITCH_PORT_GROUP_ID	ID of standard vSwitch port group	int	
VM_STANDARD_VIRTUAL_SWITCH_ID	ID of standard vSwitch	int	
VM_DV_SWITCH_ID	ID of distributed vSwitch	int	
VM_DV_PORT_GROUP_ID	ID of distributed vSwitch port group	int	
VM_DV_PORT_ID	ID of distributed vSwitch port	int	

TABLE 478 VM_NIC_TEAMING_POLICY

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
NOTIFY_SWITCHES	Flag to specify whether or not to notify the physical switch if a link fails. If this property is true, ESX Server will respond to the failure by sending a RARP packet from a different physical adapter, causing the switch to update its cache.	smallint	
POLICY	Network adapter teaming policy includes failover and load balancing, It can be one of the following: • loadbalance_ip: route based on ip hash. • loadbalance_srcmac: route based on source MAC hash. • loadbalance_srcid: route based on the source of the port ID. • failover_explicit: use explicit failover order.	smallint	

TABLE 478 VM_NIC_TEAMING_POLICY (Continued)

Field	Definition	Format	Size
REVERSE_POLICY	The flag to indicate whether or not the teaming policy is applied to inbound frames as well. For example, if the policy is explicit failover, a broadcast request goes through uplink1 and comes back through uplink2. Then if the reverse policy is set, the frame is dropped when it is received from uplink2. This reverse policy is useful to prevent the virtual machine from getting reflections.	smallint	
ROLLING_ORDER	The flag to indicate whether or not to use a rolling policy when restoring links. For example, assume the explicit link order is (vmnic9, vmnic0), therefore vmnic9 goes down, vmnic0 comes up. However, when vmnic9 comes backup, if rollingOrder is set to be true, vmnic0 continues to be used, otherwise, vmnic9 is restored as specified in the explicitly order.	smallint	
ACTIVE_NICS_ORDER	Comma separated list of active network adapters used for load balancing.	varchar	1056
STANDBY_NICS_ORDER	Standby network adapters used for failover.	varchar	1056
NIC_FAIL_CRITERIA_CHK_BEACON	Failover detection policy for this network adapter team. The bridge must be BondBridge for this property to be valid. The flag to indicate whether or not to enable this property to enable beacon probing as a method to validate the link status of a physical network adapter. checkBeacon can be enabled only if the VirtualSwitch has been configured to use the beacon. Attempting to set checkBeacon on a PortGroup or VirtualSwitch that does not have beacon probing configured for the applicable VirtualSwitch results in an error.	smallint	
VM_NETWORK_SETTINGS_ID	ID of network settings table.	int	
UNUSED_NICS_ORDER	Comma separated list of unused network adapters.	varchar	1056

TABLE 479 VM_PATH

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
HOST_ID	Identifies the host containing this path. This is a foreign key reference to VM_HOST.ID	int	
VM_ID	Identifies the VM using this path to a LUN. If the path is used by the host hypervisor instead of a VM, VM_ID is 0. When non-zero, this value matches VIRTUAL_MACHINE.ID	int	
STORAGE_ID	Identifies the LUN that is assigned to the VM. Not a foreign key, but the value matches VM_LUN.ID	int	
NAME	The VM-assigned name for this path. For VMware, this is the device name, such as vmhba0:0:1.	varchar	128

TABLE 479 VM_PATH (Continued)

Field	Definition	Format	Size
FABRIC_ID	Identifies the fabric that contains this path. Not a foreign key reference. Copied here for convenience. Determined by locating the HBA port WWN or target port WWN in the DEVICE_PORT table. Zero if the fabric is not managed. The default value is 0.	int	
HBA_PORT	The HBAs physical port WWN for this path	char	23
VM_PORT_WWN	The initiator port WWN used by the VM. If NPIV is used, this is a virtual port WWN assigned by the VM to this HBA port. If NPIV is not used, this WWN is the same as the HBA Port WWN	char	23
TARGET_PORT	The port WWN of the destination target.	char	23
ENABLED	'0 = path disabled, 1 = path enabled. The default value is 0.	smallint	
ACTIVE	0 = path inactive, 1 = path active. The default value is 0.	smallint	
PREFERRED	0 = not preferred, 1 = preferred path. The preferred path is used whenever available when the path policy is Fixed.The default value is 0.	smallint	
USAGE	Identifies how a VMware VM uses this LUN. 0 = NA (used for Hyper-V), 1 = VMFS (datastores), 2 = RDM (Raw Device Mapping). The default value is 0.	smallint	
HBA_NODE	The HBA physical node WWN for this path	char	23
VM_NODE_WWN	The initiator node WWN used by the VM. If NPIV is used, this is a virtual node WWN assigned to the VM. If NPIV is not used, this WWN is the same as the node WWN of one of the HBAs in the host.	char	23
TARGET_NODE	The node WWN of the destination target	char	23
HBA_NAME	The hypervisor device name of the HBA used in this path, such as vmhba1	varchar	64
FS_TYPE	This field will identify the filesystem type to be either: VMFS, NFS or RDM.	varchar	32

TABLE 480 VM_PHYSICAL_NIC

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
DEVICE_NAME	The device name of the physical network adapter.	varchar	256
DRIVER	The name of the driver	varchar	256
LINK_SPEED_MBPS	The bit rate on the link	int	

TABLE 480 VM_PHYSICAL_NIC (Continued)

Field	Definition	Format	Size
DUPLEX	The flag to indicate whether or not the link is capable of full-duplex ("true") or only half-duplex ("false").	smallint	
MAC_ADDRESS	The media access control (MAC) address of the physical network adapter.	varchar	17
PCI	Device hash of the PCI device corresponding to this physical network adapter.	varchar	256
WAKE_ON_LAN_SUPPORTED	Flag indicating whether the NIC is wake-on-LAN capable. 0 - false, 1 - true.	smallint	
DHCP_ENABLED	The flag to indicate whether or not DHCP (dynamic host control protocol) is enabled. If this property is set to true, the ipAddress and the subnetMask strings cannot be set explicitly. 0 - false, 1 - true.	smallint	
IP_ADDRESS	The IP address currently used by the network adapter. All IP addresses are specified using IPv4 dot notation. For example, "192.168.0.1". Subnet addresses and netmasks are specified using the same notation.	varchar	64
SUBNET_MASK	Subnet mask for the Physical NIC.	varchar	64
VM_HOST_ID	A foreign key referencing VM_HOST(ID).	int	
VM_STANDARD_VIRTUAL_SWITCH_ID	A foreign key referencing VM_STANDARD_VIRTUAL_SWITCH(ID).	int	
VM_DV_PORT_ID	A foreign key referencing VM_DV_PORT(ID).	int	
MOR_ID	The managed object reference number assigned by the hypervisor.	int	
BINARY_MAC	MAC address in binary format.	bytea	

TABLE 481 VM_SECURITY_POLICY

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
ALLOW_PROMISCUOUS	The flag to indicate whether or not all traffic is seen on the port. 0 - false, 1 - true	smallint	
FORGED_TRANSMITS	The flag to indicate whether or not the virtual network adapter should be allowed to send network traffic with a different MAC address than that of the virtual network adapter. 0 - false, 1 - true	smallint	
MAC_CHANGES	The flag to indicate whether or not the Media Access Control (MAC) address can be changed. 0 - false, 1 - true	smallint	
VM_NETWORK_SETTINGS_ID	ID of network settings table.	int	

TABLE 482 VM_STANDARD_VIRTUAL_SWITCH

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
NAME	The name of the virtual switch.	varchar	32
PORTS_COUNT	The number of ports that this virtual switch currently has.	int	
PORTS_AVAILABLE	The number of ports that are available on this virtual switch.	int	
MTU	The maximum transmission unit (MTU) associated with this virtual switch in bytes.	int	
BRIDGE_TYPE	The bridge specification describes how physical network adapters can be bridged to a virtual switch. One of: Auto Bridge - 0, Bond Bridge - 1, Simple Bridge - 2.	smallint	
VM_HOST_ID	References the ESX host in which this switch exists.	int	
MOR_ID	The managed object reference number assigned by the hypervisor.	int	

TABLE 483 VM_STANDARD_VSWITCH_PORT

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
MAC	The Media Access Control (MAC) address of network service of the virtual machine connected on this port.	varchar	64
TYPE	The type of component connected on this port. One of: • VMKernel • Service Console • Unknown • VM	smallint	
VM_STD_VSWITCH_PORT_GROUP_ID	Foreign Key to the VM_STD_VSWITCH_PORT_GROUP table. Port group in which this port exists.	int	
MOR_ID	The managed object reference number assigned by the hypervisor.	int	

TABLE 484 VM_STD_VSWITCH_PORT_GROUP

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
NAME	The name of the port group.	varchar	256

TABLE 484 VM_STD_VSWITCH_PORT_GROUP (Continued)

Field	Definition	Format	Size
VM_STANDARD_VIRTUAL__SWITCH_ID	Foreign Key to the vm_standard_virtual_switch table. The standard virtual swtich on which this port group exists.	int	
MOR_ID	The managed object reference number assigned by the hypervisor.	int	

TABLE 485 VM_STORAGE

Field	Definition	Format	Size
ID	Uniquely identifies this LUN.	serial	
HOST_ID	Identifies the server that accesses this LUN.	int	
NAME	The VM-assigned device name for this LUN, such as vmhba1:0:0. For VMware, this is the canonical name.	varchar	512
TARGET_NODE	The Node WWN or iSCSI target name for the storage device (target) that contains this LUN.	char	256
VENDOR	Vendor name, such as Seagate.	varchar	64
MODEL	Target model name, such as ST581.	varchar	64
SERIAL_NUMBER	The device''s serial number.	varchar	64
TYPE	0 = disk, 1 = tape.	smallint	
CAPACITY	For disks, the disk capacity in GB.	double precision	
STATUS	The status reported by the host. 0 = offline, 1 = online.	smallint	
PATH_POLICY	Determines how multiple paths to this LUN are used. 0 = fixed, 1 = Most Recently Used, 2 = Round Robin.	smallint	
UUID	Universal unique ID	varchar	
DATASTORE_URL	The unique locator for the datastore.	varchar	256
DATASTORE_NAME	Name of the datastore in case this LUN/NAS volume is exposed as an extent of a VMFS/NFS datastore.	varchar	256
ISCSI_TARGET_ADDRESS	IP address or host name of the iSCSI target.	varchar	256
ISCSI_TARGET_PORT	The TCP port of the storage device. If not specified, the standard default of 3260 is used.	varchar	10
NAS_REMOTE_HOST	The host that runs the NFS/CIFS server.	varchar	64
NAS_REMOTE_PATH	The remote path of NFS/CIFS mount point.	varchar	256
NAS_REMOTE_USER	In case of CIFS, the user name used while connecting to the server.	varchar	256
TARGET_PORT	Target Port WWN that the storage is connected to or the iSCSI target address.	varchar	256)

TABLE 486 VM_STORAGE_HBA_REMOTE_PORT_MAP

Field	Definition	Format	Size
VM_STORAGE_ID	A foreign key referencing VM_STORAGE (ID).	int	
HBA_REMOTE_PORT_ID	A foreign key referencing HBA_REMOTE_PORT (ID).	int	

TABLE 487 VM_TRAFFIC_SHAPING_POLICY

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
ENABLED	'The flag to indicate whether or not traffic shaper is enabled on the port. 0 - false, 1 - true	smallint	
AVERAGE_BANDWIDTH	The average bandwidth in bits per second if shaping is enabled on the port.	bigint	
BURST_SIZE	The maximum burst size allowed in bytes if shaping is enabled on the port.	bigint	
PEAK_BANDWIDTH	The peak bandwidth during bursts in bits per second if traffic shaping is enabled on the port.	bigint	
VM_NETWORK_SETTINGS_ID	ID of network settings table.	int	
TYPE	Type of traffic shaping policy, whether ingress or egress. 0 is ingress, 1 is egress traffic shaping policy.	smallint	

TABLE 488 VM_VCENTER

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
HOST	The FQDN or the ip address of the host.	varchar	256
PORT	The port of the VCENTER server on the host.	int	
USER_NAME	The username to login into the VCENTER.	varchar	64
PASSWORD	The password to login into the VCENTER.	varchar	512
VERSION	The version of VCENTER.	varchar	10
TOKEN_ID	The id to map the each VCENTER on the host.	varchar	64
PLUGIN_STATUS	Status of Plug-in registration to the vCenter server.	varchar	32
PLUGIN_ENABLED	Whether plug-in enabled or disabled.	smallint	
PLUGIN_FORWARD_EVENTS	Whether to forward events from Network Advisor to the vCenter server or not	smallint	
DISCOVERY_STATUS	vCenter server discovery status. Can be one of the below values: 1. Active 2. Failed - Authentication Failure 3. Failed - Not reachable	smallint	
DELETED_DISCOVERY	The vCenter server discovery has been deleted. Such a deleted vCenter server entry will not be discovered.	smallint	

TABLE 488 VM_VCENTER (Continued)

Field	Definition	Format	Size
MANAGED_ELEMENT_ID	A foreign key referencing MANAGED_ELEMENT(ID).	int	
FAULT_MONITORING_STATE	Flag to indicate whether fault monitoring is registered or not for a VM Host. Possible values are: 1.Not registered 2.Registered (Default)	smallint	
NAME	The name of the VCenter.	varchar	64
UUID	Unique identifier for vCenter server instance.	varchar	64

TABLE 489 VM_VCENTER_MEMBER

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
HOST_NAME	Hostname of VM host.	varchar	256
IP_ADDRESS	IP address of VM host.	varchar	128
STATUS	Discovery status of VM host. This can be one of the following: 1. Discovery Pending 2. Excluded 3. Conflict - Existing Host 4. Disconnected 5.Not responding.	smallint	
REASON	In case the status is 3 (Conflict - Existing host) then this field will be used to persist the hostname for conflicting user defined host.	varchar	1024
VM_VCENTER_ID	Id of the vCenter server managing this host.	int	
VM_HOST_ID	Foreign Key to the vm_host table.	int	

TABLE 490 VM_VIRTUAL_ETHERNET_ADAPTER

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
DISPLAY_LABEL	Display label for the virtual ethernet adapter.	varchar	256
DISPLAY_SUMMARY	Summary description.	varchar	256
KEY	This property is a unique key that distinguishes this device from other devices in the same virtual machine. Keys are immutable but may be recycled; that is, a key does not change as long as the device is associated with a particular virtual machine. However, once a device is removed, its key may be used when another device is added.	int	

TABLE 490 VM_VIRTUAL_ETHERNET_ADAPTER (Continued)

Field	Definition	Format	Size
ADDRESS_TYPE	MAC address type. Valid values for address type are: • Manual • Statically assigned MAC address. • Generated • Automatically generated MAC address. • Assigned • MAC address assigned by VirtualCenter.	smallint	
MAC_ADDRESS	MAC address assigned to the virtual network adapter. Clients can set this property to any of the allowed address types. The server might override the specified value for "Generated" or "Assigned" if it does not fall in the right ranges or is determined to be a duplicate.	varchar	64
WAKE_ON_LAN_ENABLED	Indicates whether wake-on-LAN is enabled on this virtual network adapter. Clients can set this property to selectively enable or disable wake-on-LAN.	smallint	
VIRTUAL_MACHINE_ID	Foreign Key to the vm_virtual_machine table. References the VM to which this vnic is attached.	int	
ADAPTER_TYPE	One of: • E1000 • Vmxnet • Pcnet32	smallint	
VM_STD_VSWITCH_PORT_GROUP_ID	Foreign Key to the VM_STD_VSWITCH_PORT_GROUP table. References the vSS port group to which the vnic may be associated with.	int	
VM_DV_PORT_ID	Foreign key to the vm_dv_port table. References dvPort to which this vnic is attached to.	int	
DV_PORT_KEY	The key of the port.	varchar	64
DV_PORT_GROUP_KEY	The key of portgroup.	varchar	64
DV_SWITCH_UUID	The UUID of the switch.	varchar	64
PORT_GROUP_NAME	The port group name.	varchar	256
MOR_ID	The managed object reference number assigned by the hypervisor.	int	
BINARY_MAC	MAC address in binary format.	bytea	
IP_ADDRESS	IPv4 address of VNIC.	varchar	32
BINARY_IP	IP address in binary format.	bytea	

TABLE 491 VM_VIRTUAL_MACHINE

Field	Definition	Format	Size
ID	Uniquely identifies the virtual machine	serial	
HOST_ID	Identifies the server that contains this VM	int	
HYPERVISOR_VM_ID	The VM number assigned by the hypervisor. Some hypervisors identify VMs by number as well as by name	int	
NAME	User-assigned name for the VM	varchar	80
DESCRIPTION	Optional user-entered notes describing the VM. (Annotation in VMware terminology.)	varchar	256
OS	Operating system name and version.	varchar	64
STATUS	VM status. 0 = stopped, 1 = running, 2 = suspended.	smallint	
VCPU_COUNT	Number of virtual CPUs used by the VM.	int	
CPU_RESOURCES	Summary of CPU resource configuration. Format may depend on VM vendor.	varchar	64
MEM_RESOURCES	Summary of memory resource configuration. Format may depend on VM vendor.	varchar	64
IP_ADDRESS	The primary IPv4 or IPv6 IP address used by the VM on the management LAN, if any. Primary is defined by the VM vendor.	varchar	32
HOSTNAME	The primary hostname assigned to this VM.	varchar	128
BOOT_TIME	The date and time the VM was last started.	timestamp	
DATASTORE_NAME	The user-assigned name for the VMs datastore. The datastore holds the VMs virtual disks, swap file, and configuration data.	varchar	80
DATASTORE_LOCATION	The location of the VMs datastore May be a SAN target disk or a locally-attached host disk folder. For VMware, this is a target LUN name.	varchar	64
NODE_WWN	The Node WWN for this VM. If NPIV is not being used, this will be the same as the Node WWN in the host"s DEVICE_ENCLOSURE record. If NPIV is being used, each VM has a unique Node WWN.	char	23
UUID		varchar	64
BINARY_IP	IP address in binary format.	bytea	
CONNECTION_STATE	The connectivity state of a virtual machine. • 0 = not available • 1 = connected • 2 = disconnected • 3 = inaccessible • 4 = invalid • 5 =orphaned	smallint	
COMMITTED_STORAGE	Used storage by a particular virtual machine.	varchar	64

TABLE 491 VM_VIRTUAL_MACHINE (Continued)

Field	Definition	Format	Size
UNCOMMITTED_STORAGE	Additional Provisioned storage for a particular virtual machine.	varchar	64
UNSHARED_STORAGE	Exclusive storage for a particular virtual machine.	varchar	64

TABLE 492 VM_VIRTUAL_MACHINE_DATASTORE_MAP

Field	Definition	Format	Size
VM_DATASTORE_DETAILS_ID	A foreign key referencing VM_DATASTORE_DETAILS(ID).	int	
VIRTUAL_MACHINE_ID	A foreign key referencing VM_VIRTUAL_MACHINE(ID).	int	
PROVISIONED_STORAGE	Additional storage space, in bytes, potentially used by the virtual machine on this datastore. Additional space may be needed for example when lazily allocated disks grow, or storage for swap is allocated when powering on the virtual machine.	bigint	
NOT_SHARED_STORAGE	Storage space, in bytes, occupied by the virtual machine on this datastore that is not shared with any other virtual machine.	bigint	
USED_STORAGE	Storage space, in bytes, on this datastore that is actually being used by the virtual machine.It includes space actually occupied by disks, logs, snapshots, configuration files etc. Files of the virtual machine which are present on a different datastore (e.g. a virtual disk on another datastore) are not included here.	bigint	

TABLE 493 VPLS_DEVICE_RELATION

Field	Definition	Format	Size
MPLS_SERVICE_DEVICE_RELATION_DB_ID	Database ID inherited from MPLS_SERVICE_DEVICE_RELATION.	int	
VPLS_CONFIG_INDEX	Represents the unique config index of VPLS endpoint.	int	
MAC_LIMIT	The maximum number of MAC address entries that can be learned for this VPLS Instance.	int	

TABLE 494 VPLS_ENDPOINT_RELATION

Field	Definition	Format	Size
MPLS_SERVICE_ENDPOINT_RELATION_DB_ID	Database ID inherited from MPLS_SERVICE_ENDPOINT_RELATION.	int	
ISID	The ISID value for that endpoint. Valid ISID value is between 256 (0x100) and 16777214 (0xFFFFFE). Default is 0 which indicates the endpoint is not configured with ISID.	int	

TABLE 495 VR_CONN_DOMAIN

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
VCEM_PROFILE_ID	Foreign key references the ID of the VCEM server that the domain belongs to.	int	
VR_CONN_DOMAIN_GROUP_ID	Nullable foreign key references the ID of the domain group that the domain may belong to.	int	
VCEM_ASSIGNED_ID	The ID assigned by the VCEM server.	bigint	
GUID		varchar	512
NAME		varchar	256
IP_ADDRESS		varchar	128
STATUS		varchar	256
FIRMWARE_VERSION		varchar	128
CREATION_TIME		timestamp	
LAST_UPDATE_TIME		timestamp	

TABLE 496 VR_CONN_DOMAIN_GROUP

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
VCEM_PROFILE_ID	Foreign key references the ID of the VCEM server that the domain group belongs to.	int	
VCEM_ASSIGNED_ID	The ID assigned by the VCEM server.	bigint	
NAME		varchar	256
STATUS		varchar	256
CREATION_TIME		timestamp	
LAST_UPDATE_TIME		timestamp	

TABLE 497 VR_CONN_FC_CONNECTION

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
VR_CONN_SERVER_PROFILE_ID	Foreign key references the ID of the server profile that the FC connection belongs to.	int	
PORT_NUMBER		smallint	
CONNECTION_BAY		smallint	
CREATION_TIME		timestamp	
LAST_UPDATE_TIME		timestamp	

TABLE 498 VR_CONN_MODULE

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
VR_CONN_DOMAIN_ID	Foreign key references the domain ID that the module belongs to.	int	
VCEM_ASSIGNED_ID	The ID assigned by VCEM.	varchar	256
WWN	The WWN of the module.	char	23
PRODUCT_NAME	The product name of the module.	varchar	256
SERIAL_NUMBER	The serial number of the module.	varchar	32
STATUS	The current status of the module.	varchar	256
LAST_STATUS	The previous status of the module.	varchar	256
IO_BAY	The bay number of the module.	int	
VENDOR	Subject to chnage. May not be able to differentiate module maker. Maker of the module. 0: unknown 1: Brocade 2: QLogic	int	
CREATION_TIME		timestamp	
LAST_UPDATE_TIME		timestamp	

TABLE 499 VR_CONN_MODULE_PORT

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
VR_CONN_MODULE_ID	The ID of the module that the port belongs to.	int	
WWN	The WWN of the Virtual Connect port.	char	23
POSITION_	The port number of the port within the module.	smallint	
FABRIC_NAME	The fabric name of the VCEM.	varchar	256
SPEED		varchar	64
STATUS		varchar	64
LAST_STATUS		varchar	64
REMOTE_NODE_WWN	The WWN of the connected remote switch.	char	23
CREATION_TIME		timestamp	
LAST_UPDATE_TIME		timestamp	

TABLE 500 VR_CONN_SERVER_PROFILE

Field	Definition	Format	Size
ID	Unique generated database identifier.	serial	
VCEM_PROFILE_ID	Foreign key references the ID of the VCEM server that the server profile belongs to.	int	
VR_CONN_DOMAIN_GROUP_ID	Nullable foreign key references the ID of the domain group that the server profile may belong to.	int	
VCEM_ASSIGNED_ID	The ID assigned by the VCEM server.	bigint	
NAME		varchar	256
BAY_NAME		varchar	256
BAY_NUMBER		smallint	
VIRTUAL_SERIAL_NUMBER		varchar	32
CREATION_TIME		timestamp	
LAST_UPDATE_TIME		timestamp	
BAY_ENCLOSURE_UUID	The UUID extracted from the enclosure object inside the bay object inside the server profile. The value matches the domain GUID.	varchar	512

TABLE 501 VR_CONN_WWN

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
VR_CONN_FC_CONNECTION_ID	Foreign key references the ID of the FC connection that the WWN belongs to	int	
PORT_ADDRESS	Port WWN	char	23
NODE_ADDRESS	Node WWN	char	23
SAN_NAME		varchar	256
CREATION_TIME		timestamp	
LAST_UPDATE_TIME		timestamp	

TABLE 502 WIRELESS_PRODUCT_DETAILS

Field	Definition	Format	Size
ID	The primary key of the table.	int	
DEVICE_ID	Each AP or Controller has an entry in the table. No other device will have entries here. The foreign key reference to device table.	int	
CONTROLLER_DEVICE_ID	The reference to the APs controller in device table. If APs controller gets deleted, the value sets to null. If the entry is controller the value is null.	int	
PROFILE_NAME	Profile name that the AP is using.	varchar	64

TABLE 502 WIRELESS_PRODUCT_DETAILS

Field	Definition	Format	Size
RF_DOMAIN_NAME	RF domain name set for the AP.	varchar	64
TIME_ZONE	Time zone set for the AP.	varchar	80
COUNTRY	Country set for the AP.	varchar	32
VLAN_FOR_CONTROL_TRAFFIC	VLAN for control traffic set for the AP.	varchar	512
CLIENT_COUNT	Number of wireless clients or stations that connected or associated to the AP.	int	

TABLE 503 WIRELESS_PRODUCT_RELATION

Field	Definition	Format	Size
ID	The primary key of the table.	int	
AP_DEVICE_ID	The foreign key reference to device table for AP.	int	
AP_INTERFACE_ID	The reference to the AP interface in interface table. In case the AP interface is not found or discovered, the value is null.	int	
CONNECTED_SWITCH_INTERFACE_ID	The reference to the switch interface in interface table which connected to the AP.	int	

TABLE 504 WT_ARCHIVE

Field	Definition	Format	Size
FIRMWARE_VERSION	Firmware version for which jar files are downloaded	varchar	128
JAR_LIST	List of jar files as comma separated string	varchar	256

TABLE 505 ZONE

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
ZONE_DB_ID	PK the owning ZONE_DB.	int	
NAME	The zone name.	varchar	64
TYPE	The zone type.	int	
SUB_TYPE	The zone subtype.	int	
ACTIVATE	For TI zones only, zone is activated. Default value is 0.	smallint	
CONFIGURED_FAILOVER	Configured Failover state of the TI Zone.	smallint	
CONFIGURED_ACTIVATE	Configured active state of the TI Zone.	smallint	
ENABLED_FAILOVER	Enabled Failover state of the TI Zone.	smallint	
ENABLED_ACTIVATE	Enabled Active state of the TI Zone.	smallint	

TABLE 506 ZONE_ALIAS

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
ZONE_DB_ID	PK of the owning ZONE_DB.	int	
NAME	The zone alias name.	varchar	64

TABLE 507 ZONE_ALIAS_IN_ZONE

Field	Definition	Format	Size
ZONE_ALIAS_ID*	PK of the zone alias.	int	
ZONE_ID*	PK of the zone.	int	23

TABLE 508 ZONE_ALIAS_MEMBER

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
TYPE	Zone alias member type: 2 = WWN 4 = D,P	smallint	
VALUE	Member value (D,P or WWN).	varchar	256
ZONE_ALIAS_ID	PK of the owning zone alias.	int	

TABLE 509 ZONE_DB

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
FABRIC_ID	PK of the owning fabric.	int	
NAME	Zone DB name for offline Zone DBs.	varchar	256
OFFLINE	Offline Zone DB (1 = offline).	smallint	
CREATED	Created timestamp.	timestamp	
LAST_MODIFIED	Last modified timestamp.	timestamp	
LAST_APPLIED	Last saved to switch timestamp.	timestamp	
CREATED_BY	Created by user name.	varchar	128
LAST_MODIFIED_BY	Last modified by user name.	varchar	128
LAST_APPLIED_BY	Last saved to switch user name.	varchar	128
DEFAULT_ZONE_STATUS	All access or no access when no active zone configuration.	smallint	
ZONE_TXN_SUPPORTED	Zoning commands support transaction.	smallint	
MCDATA_DEFAULT_ZONE	McData switch default zoning mode.	smallint	
MCDATA_SAFE_ZONE	McData switch safe zoning mode.	smallint	
ZONE_CONFIG_SIZE	Zone configuration string length.	int	
ZONE_AVAILABLE_SIZE	Available zone DB size in the switch. Default value is -1.	int	

TABLE 510 ZONE_DB_CONFIG

Field	Definition	Format	Size
ID	Unique generated database identifier.	int	
ZONE_DB_ID	PK of the owning zone DB	int	
DEFINED_CONTENT	Defined zone raw config string, wrapped with $ to prevent special char trimming	text	
ACTIVE_CONTENT	Active zone raw config string	text	
TI_ZONE_CONTENT	TI zone raw config string	text	

TABLE 511 ZONE_DB_CONTENT

Field	Definition	Format	Size
ID*		int	
ZONE_DB_ID	PK of the owning offline zone DB.	int	
CONTENT	Saved online content before offline was saved to switch.	text	
TI_CONTENT	TI_CONTENT saved online TI zone content before offline was saved to switch.	text	
DEFINED		text	
ACTIVE		text	

TABLE 512 ZONE_DB_USERS

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
ZONE_DB_ID	PK of the owning zone DB.	int	
USER_NAME	List of users currently editing this zone DB.	varchar	128

TABLE 513 ZONE_IN-ZONE_SET

Field	Definition	Format	Size
ZONE_SET_ID*	PK of the owning zone set.	INT	
ZONE_ID*	PK of the owning zone.	INT	

TABLE 514 ZONE_MEMBER

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
TYPE	Member type: 2 = WWN 4 = D,P	smallint	
VALUE	Member value (D,P or WWN).	varchar	256
ZONE_ID	PK of owning zone.	int	

TABLE 515 ZONE_SET

Field	Definition	Format	Size
ID*	Unique generated database identifier.	int	
ZONE_DB_ID	PK of owning zone DB.	int	
NAME	Zone set name.	varchar	64
ACTIVE	1 = active zone set 0 = otherwise.	smallint	

Views

ADAPTER_PORT_CONFIG_INFO

```
create or replace view ADAPTER_PORT_CONFIG_INFO as
select
    ADAPTER_PORT_CONFIG.ID,
    ADAPTER_PORT_CONFIG.NAME as CONFIG_NAME,
    ADAPTER_PORT_CONFIG.TYPE as TYPE,
    ADAPTER_PORT_CONFIG_PROPERTY.NAME as PROPERTY_NAME,
    ADAPTER_PORT_CONFIG_DETAILS.VALUE as PROPERTY_VALUE
from
    ADAPTER_PORT_CONFIG,
    ADAPTER_PORT_CONFIG_DETAILS,
    ADAPTER_PORT_CONFIG_PROPERTY
where
    ADAPTER_PORT_CONFIG.ID = ADAPTER_PORT_CONFIG_DETAILS.CONFIG_ID
    and ADAPTER_PORT_CONFIG_PROPERTY.ID= ADAPTER_PORT_CONFIG_DETAILS.PROPERTY_ID;
```

AG_CONNECTION_INFO

```
create or replace view AG_CONNECTION_INFO as
select
    AG_N_PORT.VIRTUAL_SWITCH_ID as SOURCE_SWITCH_ID,
    AG_N_PORT.ID as SOURCE_PORT_ID,
    AG_N_PORT.WWN as SOURCE_PORT_WWN,
    AG_N_PORT.TYPE as SOURCE_PORT_TYPE,
    AG_N_PORT.USER_PORT_NUMBER as SOURCE_USER_PORT_NUMBER,
    EDGE_F_PORT.VIRTUAL_SWITCH_ID as DESTINATION_SWITCH_ID,
    EDGE_F_PORT.ID as DESTINATION_PORT_ID,
    EDGE_F_PORT.WWN as DESTINATION_PORT_WWN,
    EDGE_F_PORT.TYPE as DESTINATION_PORT_TYPE,
    EDGE_F_PORT.USER_PORT_NUMBER as DESTINATION_USER_PORT_NUMBER
from
    SWITCH_PORT AG_N_PORT,
    SWITCH_PORT EDGE_F_PORT
where
    ((AG_N_PORT.REMOTE_PORT_WWN = EDGE_F_PORT.WWN)
        or (AG_N_PORT.REMOTE_PORT_WWN = EDGE_F_PORT.LOGICAL_PORT_WWN
            and EDGE_F_PORT.TRUNK_MASTER = 1))
    and AG_N_PORT.TYPE = 'N-Port';
```

BOOT_IMAGE_FILE_DETAILS_INFO

```
create or replace view BOOT_IMAGE_FILE_DETAILS_INFO as
select
    BOOT_IMAGE_FILE_DETAILS.BOOT_IMAGE_NAME,
    BOOT_IMAGE_FILE_DETAILS.MAJOR_VERSION,
    BOOT_IMAGE_FILE_DETAILS.MINOR_VERSION,
    BOOT_IMAGE_FILE_DETAILS.MAINTENANCE,
    BOOT_IMAGE_FILE_DETAILS.PATCH,
    BOOT_IMAGE_FILE_DETAILS.IMPORTED_DATE,
    BOOT_IMAGE_FILE_DETAILS.RELEASE_DATE,
    BOOT_IMAGE_FILE_DETAILS.RELEASE_NOTES_LOCATION,
    BOOT_IMAGE_FILE_DETAILS.LOCATION,
    BOOT_IMAGE_DRIVER_MAP.SUPPORTED_DRIVERS
from
    BOOT_IMAGE_FILE_DETAILS,
    BOOT_IMAGE_DRIVER_MAP
where
    BOOT_IMAGE_FILE_DETAILS.DRIVER_MAPPING_ID= BOOT_IMAGE_DRIVER_MAP.ID;
```

CNA_ETH_PORT_CONFIG_INFO

```
create or replace view CNA_ETH_PORT_CONFIG_INFO as
select
    CNA_PORT.ID,
    CNA_PORT.PORT_NUMBER,
    CNA_PORT.PORT_WWN,
    CNA_PORT.NODE_WWN,
    CNA_PORT.PHYSICAL_PORT_TYPE,
    CNA_PORT.NAME,
    CNA_PORT.MAC_ADDRESS,
    CNA_PORT.MEDIA,
    CNA_PORT.CEE_STATE,
    CNA_PORT.HBA_ID,
    CNA_ETH_PORT_CONFIG.CNA_ETH_PORT_ID as CNA_ETH_PORT_ID,
    CNA_ETH_PORT_CONFIG.ID as CNA_ETH_PORT_CONFIG_ID,
    CNA_ETH_PORT_CONFIG.CURRENT_MAC_ADDRESS,
    CNA_ETH_PORT_CONFIG.MAX_BANDWIDTH,
    CNA_ETH_PORT_CONFIG.PCIF_INDEX,
    CNA_ETH_PORT_CONFIG.MIN_BANDWIDTH,
    CNA_ETH_PORT_CONFIG.PORT_NUMBER as ETH_PORT_CONFIG_PORT_NUMBER,
    CNA_ETH_PORT_CONFIG.PORT_TYPE,
    CNA_ETH_PORT_CONFIG.CONFIGURATION_STATUS
from
    CNA_PORT
        left outer join CNA_ETH_PORT_CONFIG on CNA_PORT.ID =
CNA_ETH_PORT_CONFIG.CNA_PORT_ID;
```

CNA_PORT_DETAILS_INFO

```
create or replace view CNA_PORT_DETAILS_INFO as
select
    CNA_PORT.ID,
    CNA_PORT.PORT_NUMBER,
    CNA_PORT.PORT_WWN,
    CNA_PORT.NODE_WWN,
    CNA_PORT.PHYSICAL_PORT_TYPE,
```

```
    CNA_PORT.NAME,
    CNA_PORT.MAC_ADDRESS,
    CNA_PORT.MEDIA,
    CNA_PORT.CEE_STATE,
    CNA_PORT.HBA_ID,
    CNA_PORT.CREATION_TIME as CNA_PORT_CREATION_TIME,
    CNA_ETH_PORT.ID as ETH_PORT_ID,
    CNA_ETH_PORT.ETH_DEV,
    CNA_ETH_PORT.ETH_LOG_LEVEL,
    CNA_ETH_PORT.NAME as ETH_PORT_NAME,
    CNA_ETH_PORT.MAC_ADDRESS as ETH_MAC_ADDRESS,
    CNA_ETH_PORT.IOC_ID,
    CNA_ETH_PORT.HARDWARE_PATH,
    CNA_ETH_PORT.STATUS,
    CNA_ETH_PORT.CREATION_TIME as ETH_PORT_CREATION_TIME,
    CNA_ETH_PORT.CURRENT_MAC_ADDRESS as CURRENT_MAC_ADDRESS,
    CNA_ETH_PORT.MAX_BANDWIDTH,
    CNA_ETH_PORT.PCIF_INDEX,
    CNA_ETH_PORT.MAX_PCIF,
    CNA_ETH_PORT.MIN_BANDWIDTH,
    CNA_ETH_PORT.MTU,
    CNA_PORT.ALARM_WARNING
from
    CNA_PORT
        left outer join CNA_ETH_PORT on CNA_PORT.ID = CNA_ETH_PORT.CNA_PORT_ID;
```

CNA_PORT_INFO

```
create or replace view CNA_PORT_INFO as
select
    CNA_PORT.ID,
    CNA_PORT.PORT_NUMBER,
    CNA_PORT.PORT_WWN,
    CNA_PORT.NODE_WWN,
    CNA_PORT.PHYSICAL_PORT_TYPE,
    CNA_PORT.NAME,
    CNA_PORT.MAC_ADDRESS,
    CNA_PORT.MEDIA,
    CNA_PORT.CEE_STATE,
    CNA_PORT.HBA_ID,
    CNA_PORT.CREATION_TIME as CNA_PORT_CREATION_TIME,
    CNA_ETH_PORT.ID as ETH_PORT_ID,
    CNA_ETH_PORT.ETH_DEV,
    CNA_ETH_PORT.ETH_LOG_LEVEL,
    CNA_ETH_PORT.NAME as ETH_PORT_NAME,
    CNA_ETH_PORT.MAC_ADDRESS as ETH_MAC_ADDRESS,
    CNA_ETH_PORT.IOC_ID,
    CNA_ETH_PORT.HARDWARE_PATH,
    CNA_ETH_PORT.STATUS,
    CNA_ETH_PORT.CREATION_TIME as ETH_PORT_CREATION_TIME,
    HBA_PORT.DEVICE_PORT_ID,
    CNA_ETH_PORT.MTU,
    CNA_PORT.ALARM_WARNING
from
    CNA_PORT
        left outer join HBA_PORT on CNA_PORT.ID = HBA_PORT.CNA_PORT_ID
        left outer join CNA_ETH_PORT on CNA_PORT.ID = CNA_ETH_PORT.CNA_PORT_ID;
```

CORE_SWITCH_DETAILS_INFO

```
create or replace view CORE_SWITCH_DETAILS_INFO as
select
   CORE_SWITCH.ID,
   CORE_SWITCH.IP_ADDRESS,
   CORE_SWITCH.WWN,
   CORE_SWITCH.NAME,
   CORE_SWITCH.TYPE,
   CORE_SWITCH.MODEL,
   CORE_SWITCH.FIRMWARE_VERSION,
   CORE_SWITCH.VENDOR,
   CORE_SWITCH.MAX_VIRTUAL_SWITCHES,
   CORE_SWITCH.NUM_VIRTUAL_SWITCHES,
   CORE_SWITCH.REACHABLE,
   CORE_SWITCH.UNREACHABLE_TIME,
   CORE_SWITCH.OPERATIONAL_STATUS,
   CORE_SWITCH.CREATION_TIME,
   CORE_SWITCH.LAST_SCAN_TIME,
   CORE_SWITCH.LAST_UPDATE_TIME,
   CORE_SWITCH.SYSLOG_REGISTERED,
   CORE_SWITCH.CALL_HOME_ENABLED,
   CORE_SWITCH.SNMP_REGISTERED,
   CORE_SWITCH.USER_IP_ADDRESS,
   CORE_SWITCH.NIC_PROFILE_ID,
   CORE_SWITCH.MANAGING_SERVER_IP_ADDRESS,
   CORE_SWITCH.VF_ENABLED,
   CORE_SWITCH.VF_SUPPORTED,
   CORE_SWITCH.MANAGED_ELEMENT_ID as CORE_MANAGED_ELEMENT_ID,
   CORE_SWITCH_DETAILS.ETHERNET_MASK,
   CORE_SWITCH_DETAILS.FC_MASK,
   CORE_SWITCH_DETAILS.FC_IP,
   CORE_SWITCH_DETAILS.FC_CERTIFICATE,
   CORE_SWITCH_DETAILS.SW_LICENSE_ID,
   CORE_SWITCH_DETAILS.SUPPLIER_SERIAL_NUMBER,
   CORE_SWITCH_DETAILS.PART_NUMBER,
   CORE_SWITCH_DETAILS.CHECK_BEACON,
   CORE_SWITCH_DETAILS.TIMEZONE,
   CORE_SWITCH_DETAILS.MAX_PORT,
   CORE_SWITCH_DETAILS.CHASSIS_SERVICE_TAG,
   CORE_SWITCH_DETAILS.BAY_ID,
   CORE_SWITCH_DETAILS.TYPE_NUMBER,
   CORE_SWITCH_DETAILS.MODEL_NUMBER,
   CORE_SWITCH_DETAILS.MANUFACTURER,
   CORE_SWITCH_DETAILS.PLANT_OF_MANUFACTURER,
   CORE_SWITCH_DETAILS.SWITCH_SERIAL_NUMBER,
   CORE_SWITCH_DETAILS.ACT_CP_PRI_FW_VERSION,
   CORE_SWITCH_DETAILS.ACT_CP_SEC_FW_VERSION,
   CORE_SWITCH_DETAILS.STBY_CP_PRI_FW_VERSION,
   CORE_SWITCH_DETAILS.STBY_CP_SEC_FW_VERSION,
   CORE_SWITCH_DETAILS.EGM_CAPABLE,
   CORE_SWITCH_DETAILS.SUB_TYPE,
   CORE_SWITCH_DETAILS.PARTITION,
   CORE_SWITCH_DETAILS.MAX_NUM_OF_BLADES,
   CORE_SWITCH_DETAILS.VENDOR_VERSION,
   CORE_SWITCH_DETAILS.VENDOR_PART_NUMBER,
   CORE_SWITCH_DETAILS.RNID_SEQUENCE_NUMBER,
   CORE_SWITCH_DETAILS.CONTACT,
   CORE_SWITCH_DETAILS.LOCATION,
```

```
   CORE_SWITCH_DETAILS.DESCRIPTION,
   CORE_SWITCH_DETAILS.IP_ADDRESS_PREFIX,
   CORE_SWITCH_DETAILS.DOMAIN_NAME,
   CORE_SWITCH_DETAILS.FRAME_LOG_SIZE,
   CORE_SWITCH_DETAILS.FRAME_LOG_ENABLED,
   CORE_SWITCH_DETAILS.MAPS_ENABLED
from
   CORE_SWITCH LEFT OUTER JOIN CORE_SWITCH_DETAILS
   on CORE_SWITCH_DETAILS.CORE_SWITCH_ID = CORE_SWITCH.ID;
```

CRYPTO_HOST_LUN_INFO

```
create or replace view CRYPTO_HOST_LUN_INFO as
select
   LUN.CRYPTO_HOST_ID,
   LUN.ID CRYPTO_LUN_ID,
   LUN.LUN_NUMBER,
   LUN.CRYPTO_TARGET_CONTAINER_ID,
   LUN.SERIAL_NUMBER,
   LUN.ENCRYPTION_STATE,
   LUN.STATUS,
   LUN.REKEY_INTERVAL,
   LUN.VOLUME_LABEL_PREFIX,
   LUN.LAST_REKEY_DATE,
   LUN.LAST_REKEY_STATUS,
   LUN.LAST_REKEY_PROGRESS,
   LUN.CURRENT_VOLUME_LABEL,
   LUN.PRIOR_ENCRYPTION_STATE,
   LUN.ENCRYPTION_FORMAT,
   LUN.ENCRYPT_EXISTING_DATA,
   LUN.DECRYPT_EXISTING_DATA,
   LUN.KEY_ID,
   LUN.BLOCK_SIZE,
   LUN.TOTAL_BLOCKS,
   LUN.LUN_STATE,
   LUN.LUN_FLAGS,
   LUN.ENCRYPTION_ALGORITHM,
   LUN.KEY_ID_STATE,
   LUN.REKEY_SESSION_NUMBER,
   LUN.PERCENTAGE_COMPLETE,
   LUN.REKEY_ROLE,
   LUN.CURRENT_LBA,
   LUN.LUN_STATE_STRING,
   LUN.NEW_LUN,
   LUN.NEW_LUN_TYPE,
   LUN.DISABLE_WRITE_EARLY_ACK,
   LUN.DISABLE_READ_AHEAD,
   LUN.TIME_LEFT_FOR_AUTO_REKEY,
   CRYPTO_HOST.HOST_PORT_WWN,
   CRYPTO_HOST.HOST_NODE_WWN
    LUN.THIN_PROVISION_LUN
from
   CRYPTO_LUN LUN,
   CRYPTO_HOST
where
   LUN.CRYPTO_HOST_ID = CRYPTO_HOST.ID;
```

CRYPTO_TARGET_ENGINE_INFO

```
create or replace view CRYPTO_TARGET_ENGINE_INFO as
select
   CRYPTO_TARGET_CONTAINER.ID TARGET_CONTAINER_ID,
   CRYPTO_TARGET_CONTAINER.NAME,
   CRYPTO_TARGET_CONTAINER.VT_NODE_WWN,
   CRYPTO_TARGET_CONTAINER.VT_PORT_WWN,
   CRYPTO_TARGET_CONTAINER.FAILOVER_STATUS,
   CRYPTO_TARGET_CONTAINER.FAILOVER_STATUS_2,
   CRYPTO_TARGET_CONTAINER.DEVICE_STATUS,
   CRYPTO_TARGET_CONTAINER.DEVICE_TYPE,
   CRYPTO_TARGET_CONTAINER.TARGET_PORT_WWN,
   CRYPTO_TARGET_CONTAINER.TARGET_NODE_WWN,
   CRYPTO_TARGET_CONTAINER.CONTAINER_FIELD_DATA,
   CRYPTO_TARGET_CONTAINER.CONFIGURATION_STATUS,
   CRYPTO_TARGET_CONTAINER.FRONT_END_N_PORT_NUMBER,
   ENCRYPTION_ENGINE.STATUS ENCRYPTION_ENGINE_STATUS,
   ENCRYPTION_ENGINE.HA_CLUSTER_ID,
   ENCRYPTION_ENGINE.SYSTEM_CARD_STATUS,
   ENCRYPTION_ENGINE.WWN_POOLS_AVAILABLE,
   ENCRYPTION_ENGINE.STATE ENCRYPTION_ENGINE_STATE,
   ENCRYPTION_ENGINE.ID ENCRYPTION_ENGINE_ID,
   CRYPTO_SWITCH.SWITCH_ID SWITCH_ID,
   CRYPTO_SWITCH.ENCRYPTION_GROUP_ID ENCRYPTION_GROUP_ID
from
   CRYPTO_TARGET_CONTAINER,
   ENCRYPTION_ENGINE,
   CRYPTO_SWITCH
where
   CRYPTO_TARGET_CONTAINER.ENCRYPTION_ENGINE_ID = ENCRYPTION_ENGINE.ID
   and CRYPTO_SWITCH.SWITCH_ID = ENCRYPTION_ENGINE.SWITCH_ID;
```

DASHBOARD_PREFERENCES_INFO

```
CREATE VIEW dashboard_preferences_info AS
    select
   DASHBOARD.NAME as DASHBOARD_NAME,
   DASHBOARD.DESCRIPTION as DASHBOARD_DESC,
   DASHBOARD.CREATED_BY,
   DASHBOARD_CANVAS.NAME as CANVAS_NAME,
   DASHBOARD_CANVAS.DESCRIPTION as CANVAS_DESC,
   DASHBOARD_CANVAS_PREFERENCE.SCOPE_ID,
   DASHBOARD_CANVAS_PREFERENCE.SCOPE_TYPE,
   DASHBOARD_CANVAS_PREFERENCE.DASHBOARD_ID,
   DASHBOARD_CANVAS_PREFERENCE.DASHBOARD_CANVAS_ID,
   DASHBOARD_CANVAS_PREFERENCE.VISIBLE,
   DASHBOARD_CANVAS_PREFERENCE.TIME_SCOPE
from
  DASHBOARD,
  DASHBOARD_CANVAS,
  DASHBOARD_CANVAS_PREFERENCE
where
  DASHBOARD.ID = DASHBOARD_CANVAS_PREFERENCE.DASHBOARD_ID
  and DASHBOARD_CANVAS.ID = DASHBOARD_CANVAS_PREFERENCE.DASHBOARD_CANVAS_ID;
```

DEPLOYMENT_INFO

```
create or replace view DEPLOYMENT_INFO as
select
    DEPLOYMENT_CONFIGURATION.ID as ID,
    DEPLOYMENT_CONFIGURATION.NAME as NAME,
    DEPLOYMENT_CONFIGURATION.DESCRIPTION as DESCRIPTION,
    DEPLOYMENT_HANDLER.MODULE as MODULE,
    DEPLOYMENT_HANDLER.SUB_MODULE as SUB_MODULE,
    DEPLOYMENT_STATUS.DEPLOYMENT_TIME as DEPLOYMENT_TIME,
    DEPLOYMENT_CONFIGURATION.DEPLOY_OPTION as DEPLOYMENT_OPTION,
    DEPLOYMENT_STATUS.STATUS as STATUS,
    DEPLOYMENT_STATUS.DEPLOYED_BY as DEPLOYED_BY,
    DEPLOYMENT_CONFIGURATION.CREATED_BY as CREATOR,
    DEPLOYMENT_CONFIGURATION.SCHEDULE_ENABLED as SCHEDULE_ENABLED,
    DEPLOYMENT_CONFIGURATION.SNAPSHOT_ENABLED as SNAPSHOT_ENABLED,
    SCHEDULE_ENTRY.TYPE as FREQUENCY,
    DEPLOYMENT_CONFIGURATION.MANAGEMENT_FLAG,
    DEPLOYMENT_HANDLER.PRIVILEGE_ID,
    DEPLOYMENT_HANDLER.HANDLER_CLASS,
    DEPLOYMENT_HANDLER.CLIENT_ACTION_HANDLER_CLASS,
    DEPLOYMENT_STATUS.ID as STATUS_ID,
    DEPLOYMENT_HANDLER.MODULE_DISPLAYNAME,
    DEPLOYMENT_REPORT_TEMPLATE.HEADER,
    DEPLOYMENT_REPORT_TEMPLATE.FOOTER
from
    DEPLOYMENT_CONFIGURATION
        join DEPLOYMENT_HANDLER on DEPLOYMENT_CONFIGURATION.DEPLOYMENT_HANDLER_ID
= DEPLOYMENT_HANDLER.ID
        left outer join DEPLOYMENT_STATUS on
            (DEPLOYMENT_STATUS.DEPLOYMENT_TIME =
               (select
                    max(DEPLOYMENT_STATUS.DEPLOYMENT_TIME)
                from
                    DEPLOYMENT_STATUS
                where
                    DEPLOYMENT_STATUS.DEPLOYMENT_CONFIGURATION_ID =
DEPLOYMENT_CONFIGURATION.ID))
        left outer join SCHEDULE_ENTRY on
            SCHEDULE_ENTRY.IDENTITY = cast(DEPLOYMENT_CONFIGURATION.ID as
varchar(16))
            and SCHEDULE_ENTRY.TABLE_NAME = 'DEPLOYMENT_CONFIGURATION'
        left outer join DEPLOYMENT_REPORT_TEMPLATE on
DEPLOYMENT_REPORT_TEMPLATE.DEPLOYMENT_HANDLER_ID = DEPLOYMENT_HANDLER.ID;
```

DEPLOYMENT_LOG

```
create or replace view DEPLOYMENT_LOG as
select
    DEPLOYMENT_CONFIGURATION.ID,
    DEPLOYMENT_CONFIGURATION.NAME,
    DEPLOYMENT_CONFIGURATION.DESCRIPTION,
    DEPLOYMENT_HANDLER.MODULE,
    DEPLOYMENT_HANDLER.SUB_MODULE,
    DEPLOYMENT_STATUS.DEPLOYMENT_TIME,
    DEPLOYMENT_CONFIGURATION.DEPLOY_OPTION as DEPLOYMENT_OPTION,
    DEPLOYMENT_STATUS.STATUS, DEPLOYMENT_STATUS.DEPLOYED_BY,
    DEPLOYMENT_CONFIGURATION.CREATED_BY as CREATOR,
```

```
    DEPLOYMENT_CONFIGURATION.SCHEDULE_ENABLED,
    DEPLOYMENT_CONFIGURATION.SNAPSHOT_ENABLED,
    DEPLOYMENT_CONFIGURATION.MANAGEMENT_FLAG,
    DEPLOYMENT_HANDLER.PRIVILEGE_ID,
    DEPLOYMENT_HANDLER.HANDLER_CLASS,
    DEPLOYMENT_HANDLER.CLIENT_ACTION_HANDLER_CLASS,
    DEPLOYMENT_STATUS.ID as STATUS_ID,
    DEPLOYMENT_HANDLER.MODULE_DISPLAYNAME,
    DEPLOYMENT_STATUS.TRIGGER_SOURCE as TRIGGER_SOURCE,
    DEPLOYMENT_REPORT_TEMPLATE.HEADER,
    DEPLOYMENT_REPORT_TEMPLATE.FOOTER
from
    DEPLOYMENT_CONFIGURATION
        inner join DEPLOYMENT_HANDLER
            on DEPLOYMENT_CONFIGURATION.DEPLOYMENT_HANDLER_ID =
DEPLOYMENT_HANDLER.ID
        inner join DEPLOYMENT_STATUS
            on DEPLOYMENT_CONFIGURATION.ID =
DEPLOYMENT_STATUS.DEPLOYMENT_CONFIGURATION_ID
        left outer join DEPLOYMENT_REPORT_TEMPLATE on
DEPLOYMENT_REPORT_TEMPLATE.DEPLOYMENT_HANDLER_ID = DEPLOYMENT_HANDLER.ID;
```

DEVICE_CONNECTION_INFO

```
CREATE VIEW device_connection_info AS
    select
    DEVICE_CONNECTION.ID,
    DEVICE_CONNECTION.FABRIC_ID,
    DEVICE_CONNECTION.DEVICE_PORT_ID,
    DEVICE_CONNECTION.SWITCH_PORT_ID,
    DEVICE_CONNECTION.AG_PORT_ID,
    COALESCE(DEVICE_ENCLOSURE_MEMBER.ENCLOSURE_ID, HBA.HOST_ID) as
DEVICE_ENCLOSURE_ID,
    DEVICE_CONNECTION.CREATION_TIME,
    DEVICE_CONNECTION.LAST_UPDATED_TIME,
    DEVICE_PORT.NODE_ID,
    DEVICE_CONNECTION.MISSING,
    DEVICE_CONNECTION.MISSING_TIME,
    SWPORT.VIRTUAL_SWITCH_ID,
    DEVICE_CONNECTION.TRUSTED,
    AGPORT.VIRTUAL_SWITCH_ID as AG_SWITCH_ID,
    DEVICE_PORT.WWN as DEVICE_PORT_WWN,
    COALESCE(USERDEFINEDDETAILS.TYPE, DN.TYPE) as DEVICE_TYPE
from DEVICE_CONNECTION
    left join DEVICE_PORT on DEVICE_CONNECTION.DEVICE_PORT_ID = DEVICE_PORT.ID
    left join SWITCH_PORT SWPORT on DEVICE_CONNECTION.SWITCH_PORT_ID = SWPORT.ID
    left join SWITCH_PORT AGPORT on DEVICE_CONNECTION.AG_PORT_ID = AGPORT.ID
    left join HBA_PORT_DEVICE_PORT_MAP on DEVICE_PORT.ID =
HBA_PORT_DEVICE_PORT_MAP.DEVICE_PORT_ID
    left join HBA_PORT on HBA_PORT_DEVICE_PORT_MAP.HBA_PORT_ID =
HBA_PORT.DEVICE_PORT_ID
    left join HBA on HBA_PORT.HBA_ID = HBA.ID
    left join DEVICE_ENCLOSURE_MEMBER on DEVICE_PORT.ID =
DEVICE_ENCLOSURE_MEMBER.DEVICE_PORT_ID
    left join DEVICE_NODE DN on DEVICE_PORT.NODE_ID = DN.ID
    left join USER_DEFINED_DEVICE_DETAIL USERDEFINEDDETAILS on DN.WWN =
USERDEFINEDDETAILS.WWN;
```

EE_MONITOR_STATS_5MIN_INFO

```
create or replace view EE_MONITOR_STATS_5MIN_INFO as
select VIRTUAL_SWITCH.ID as VIRTUAL_SWITCH_ID,
  ME_ID,
  TARGET_ID as EE_MONITOR_ID,
  timestamp with time zone 'epoch' + TIME_IN_SECONDS * interval '1 second' as
CREATION_TIME,
  sum(case when MEASURE_ID = 208 then value else 0 end) as TX_UTILIZATION,
  sum(case when MEASURE_ID = 209 then value else 0 end) as RX_UTILIZATION,
  sum(case when MEASURE_ID = 210 then value else 0 end) as CRC_ERRORS
  from TIME_SERIES_DATA_1, VIRTUAL_SWITCH
  where ME_ID = MANAGED_ELEMENT_ID and COLLECTOR_ID = 16
  group by ME_ID, TARGET_TYPE, TARGET_ID, TIME_IN_SECONDS,VIRTUAL_SWITCH_ID order
by TIME_IN_SECONDS desc;
```

EE_MONITOR_STATS_30MIN_INFO

```
create or replace view EE_MONITOR_STATS_30MIN_INFO as
select VIRTUAL_SWITCH.ID as VIRTUAL_SWITCH_ID,
  ME_ID,
  TARGET_ID as EE_MONITOR_ID,
  timestamp with time zone 'epoch' + TIME_IN_SECONDS * interval '1 second' as
CREATION_TIME,
  sum(case when MEASURE_ID = 208 then value else 0 end) as TX_UTILIZATION,
  sum(case when MEASURE_ID = 209 then value else 0 end) as RX_UTILIZATION,
  sum(case when MEASURE_ID = 210 then value else 0 end) as CRC_ERRORS
  from TIME_SERIES_DATA_1_30MIN, VIRTUAL_SWITCH
  where ME_ID = MANAGED_ELEMENT_ID and COLLECTOR_ID = 16
  group by ME_ID, TARGET_TYPE, TARGET_ID, TIME_IN_SECONDS,VIRTUAL_SWITCH_ID order
by TIME_IN_SECONDS desc;
```

EE_MONITOR_STATS_2HOUR_INFO

```
create or replace view EE_MONITOR_STATS_2HOUR_INFO as
select VIRTUAL_SWITCH.ID as VIRTUAL_SWITCH_ID,
  ME_ID,
  TARGET_ID as EE_MONITOR_ID,
  timestamp with time zone 'epoch' + TIME_IN_SECONDS * interval '1 second' as
CREATION_TIME,
  sum(case when MEASURE_ID = 208 then value else 0 end) as TX_UTILIZATION,
  sum(case when MEASURE_ID = 209 then value else 0 end) as RX_UTILIZATION,
  sum(case when MEASURE_ID = 210 then value else 0 end) as CRC_ERRORS
  from TIME_SERIES_DATA_1_2HOUR, VIRTUAL_SWITCH
  where ME_ID = MANAGED_ELEMENT_ID and COLLECTOR_ID = 16
  group by ME_ID, TARGET_TYPE, TARGET_ID, TIME_IN_SECONDS,VIRTUAL_SWITCH_ID order
by TIME_IN_SECONDS desc;
```

EE_MONITOR_STATS_1DAY_INFO

```
create or replace view EE_MONITOR_STATS_1DAY_INFO as
select VIRTUAL_SWITCH.ID as VIRTUAL_SWITCH_ID,
  ME_ID,
  TARGET_ID as EE_MONITOR_ID,
```

```
  timestamp with time zone 'epoch' + TIME_IN_SECONDS * interval '1 second' as
CREATION_TIME,
  sum(case when MEASURE_ID = 208 then value else 0 end) as TX_UTILIZATION,
  sum(case when MEASURE_ID = 209 then value else 0 end) as RX_UTILIZATION,
  sum(case when MEASURE_ID = 210 then value else 0 end) as CRC_ERRORS
  from TIME_SERIES_DATA_1_1DAY, VIRTUAL_SWITCH
  where ME_ID = MANAGED_ELEMENT_ID and COLLECTOR_ID = 16
  group by ME_ID, TARGET_TYPE, TARGET_ID, TIME_IN_SECONDS,VIRTUAL_SWITCH_ID order
by TIME_IN_SECONDS desc;
```

TE_PORT_STATS_5MIN_INFO

```
create or replace view TE_PORT_STATS_5MIN_INFO as
select VIRTUAL_SWITCH.ID as VIRTUAL_SWITCH_ID,
  ME_ID,
  TARGET_ID as PORT_ID,
  timestamp with time zone 'epoch' + TIME_IN_SECONDS * interval '1 second' as
CREATION_TIME,
  sum(case when MEASURE_ID = 193 then value else 0 end) as
RECEIVE_OK_PERCENT_UTIL,
  sum(case when MEASURE_ID = 194 then value else 0 end) as
TRANSMIT_OK_PERCENT_UTIL,
  sum(case when MEASURE_ID = 196 then value else 0 end) as RECEIVE_OK,
  sum(case when MEASURE_ID = 195 then value else 0 end) as TRANSMIT_OK,
  sum(case when MEASURE_ID = 36 then value else 0 end) as RECEIVE_EOF,
  sum(case when MEASURE_ID = 40 then value else 0 end) as UNDERFLOW_ERRORS,
  sum(case when MEASURE_ID = 41 then value else 0 end) as OVERFLOW_ERRORS,
  sum(case when MEASURE_ID = 43 then value else 0 end) as ALIGNMENT_ERRORS,
  sum(case when MEASURE_ID = 42 then value else 0 end) as RUNT_ERRORS,
  sum(case when MEASURE_ID = 43 then value else 0 end) as TOO_LONG_ERRORS,
  sum(case when MEASURE_ID = 39 then value else 0 end) as CRC_ERRORS
  from TIME_SERIES_DATA_1, VIRTUAL_SWITCH
  where ME_ID = MANAGED_ELEMENT_ID and COLLECTOR_ID = 12
  group by ME_ID, TARGET_TYPE, TARGET_ID, TIME_IN_SECONDS,VIRTUAL_SWITCH_ID order
by TIME_IN_SECONDS desc;
```

TE_PORT_STATS_30MIN_INFO

```
create or replace view TE_PORT_STATS_30MIN_INFO as
select VIRTUAL_SWITCH.ID as VIRTUAL_SWITCH_ID,
  ME_ID,
  TARGET_ID as PORT_ID,
  timestamp with time zone 'epoch' + TIME_IN_SECONDS * interval '1 second' as
CREATION_TIME,
  sum(case when MEASURE_ID = 193 then value else 0 end) as
RECEIVE_OK_PERCENT_UTIL,
  sum(case when MEASURE_ID = 194 then value else 0 end) as
TRANSMIT_OK_PERCENT_UTIL,
  sum(case when MEASURE_ID = 196 then value else 0 end) as RECEIVE_OK,
  sum(case when MEASURE_ID = 195 then value else 0 end) as TRANSMIT_OK,
  sum(case when MEASURE_ID = 36 then value else 0 end) as RECEIVE_EOF,
  sum(case when MEASURE_ID = 40 then value else 0 end) as UNDERFLOW_ERRORS,
  sum(case when MEASURE_ID = 41 then value else 0 end) as OVERFLOW_ERRORS,
  sum(case when MEASURE_ID = 43 then value else 0 end) as ALIGNMENT_ERRORS,
  sum(case when MEASURE_ID = 42 then value else 0 end) as RUNT_ERRORS,
  sum(case when MEASURE_ID = 43 then value else 0 end) as TOO_LONG_ERRORS,
  sum(case when MEASURE_ID = 39 then value else 0 end) as CRC_ERRORS
```

```
  from TIME_SERIES_DATA_1_30MIN, VIRTUAL_SWITCH
  where ME_ID = MANAGED_ELEMENT_ID and COLLECTOR_ID = 12
  group by ME_ID, TARGET_TYPE, TARGET_ID, TIME_IN_SECONDS,VIRTUAL_SWITCH_ID order
by TIME_IN_SECONDS desc;
```

TE_PORT_STATS_2HOUR_INFO

```
create or replace view TE_PORT_STATS_2HOUR_INFO as
select VIRTUAL_SWITCH.ID as VIRTUAL_SWITCH_ID,
  ME_ID,
  TARGET_ID as PORT_ID,
  timestamp with time zone 'epoch' + TIME_IN_SECONDS * interval '1 second' as
CREATION_TIME,
  sum(case when MEASURE_ID = 193 then value else 0 end) as
RECEIVE_OK_PERCENT_UTIL,
  sum(case when MEASURE_ID = 194 then value else 0 end) as
TRANSMIT_OK_PERCENT_UTIL,
  sum(case when MEASURE_ID = 196 then value else 0 end) as RECEIVE_OK,
  sum(case when MEASURE_ID = 195 then value else 0 end) as TRANSMIT_OK,
  sum(case when MEASURE_ID = 36 then value else 0 end) as RECEIVE_EOF,
  sum(case when MEASURE_ID = 40 then value else 0 end) as UNDERFLOW_ERRORS,
  sum(case when MEASURE_ID = 41 then value else 0 end) as OVERFLOW_ERRORS,
  sum(case when MEASURE_ID = 43 then value else 0 end) as ALIGNMENT_ERRORS,
  sum(case when MEASURE_ID = 42 then value else 0 end) as RUNT_ERRORS,
  sum(case when MEASURE_ID = 43 then value else 0 end) as TOO_LONG_ERRORS,
  sum(case when MEASURE_ID = 39 then value else 0 end) as CRC_ERRORS
  from TIME_SERIES_DATA_1_2HOUR, VIRTUAL_SWITCH
  where ME_ID = MANAGED_ELEMENT_ID and COLLECTOR_ID = 12
  group by ME_ID, TARGET_TYPE, TARGET_ID, TIME_IN_SECONDS,VIRTUAL_SWITCH_ID order
by TIME_IN_SECONDS desc;
```

TE_PORT_STATS_1DAY_INFO

```
create or replace view TE_PORT_STATS_1DAY_INFO as
select VIRTUAL_SWITCH.ID as VIRTUAL_SWITCH_ID,
  ME_ID,
  TARGET_ID as PORT_ID,
  timestamp with time zone 'epoch' + TIME_IN_SECONDS * interval '1 second' as
CREATION_TIME,
  sum(case when MEASURE_ID = 193 then value else 0 end) as
RECEIVE_OK_PERCENT_UTIL,
  sum(case when MEASURE_ID = 194 then value else 0 end) as
TRANSMIT_OK_PERCENT_UTIL,
  sum(case when MEASURE_ID = 196 then value else 0 end) as RECEIVE_OK,
  sum(case when MEASURE_ID = 195 then value else 0 end) as TRANSMIT_OK,
  sum(case when MEASURE_ID = 36 then value else 0 end) as RECEIVE_EOF,
  sum(case when MEASURE_ID = 40 then value else 0 end) as UNDERFLOW_ERRORS,
  sum(case when MEASURE_ID = 41 then value else 0 end) as OVERFLOW_ERRORS,
  sum(case when MEASURE_ID = 43 then value else 0 end) as ALIGNMENT_ERRORS,
  sum(case when MEASURE_ID = 42 then value else 0 end) as RUNT_ERRORS,
  sum(case when MEASURE_ID = 43 then value else 0 end) as TOO_LONG_ERRORS,
  sum(case when MEASURE_ID = 39 then value else 0 end) as CRC_ERRORS
  from TIME_SERIES_DATA_1_1DAY, VIRTUAL_SWITCH
  where ME_ID = MANAGED_ELEMENT_ID and COLLECTOR_ID = 12
  group by ME_ID, TARGET_TYPE, TARGET_ID, TIME_IN_SECONDS,VIRTUAL_SWITCH_ID order
by TIME_IN_SECONDS desc;
```

SWITCH_INFO

```
CREATE VIEW switch_info AS
    select
   CORE_SWITCH.ID as PHYSICAL_SWITCH_ID,
   CORE_SWITCH.NAME as PHYSICAL_SWITCH_NAME,
   CORE_SWITCH.IP_ADDRESS,
   CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN,
   CORE_SWITCH.OPERATIONAL_STATUS as PHYSICAL_OPERATIONAL_STATUS,
   CORE_SWITCH.TYPE,
   CORE_SWITCH.MAX_VIRTUAL_SWITCHES,
   CORE_SWITCH.NUM_VIRTUAL_SWITCHES,
   CORE_SWITCH.FIRMWARE_VERSION,
   CORE_SWITCH.VENDOR,
   CORE_SWITCH.REACHABLE,
   CORE_SWITCH.UNREACHABLE_TIME,
   CORE_SWITCH.MODEL,
   CORE_SWITCH.SYSLOG_REGISTERED,
   CORE_SWITCH.SNMP_REGISTERED,
   CORE_SWITCH.CALL_HOME_ENABLED,
   CORE_SWITCH.USER_IP_ADDRESS,
   CORE_SWITCH.NIC_PROFILE_ID,
   CORE_SWITCH.MANAGING_SERVER_IP_ADDRESS,
   CORE_SWITCH.VF_ENABLED,
   CORE_SWITCH.VF_SUPPORTED,
   CORE_SWITCH.MANAGED_ELEMENT_ID as CORE_MANAGED_ELEMENT_ID,
   CORE_SWITCH.NAT_PRIVATE_IP_ADDRESS,
   CORE_SWITCH.ALTERNATE_IP_ADDRESS,
   CORE_SWITCH.MAC_ADDRESS,
   VIRTUAL_SWITCH.ID,
   VIRTUAL_SWITCH.NAME,
   VIRTUAL_SWITCH.OPERATIONAL_STATUS,
   VIRTUAL_SWITCH.SWITCH_MODE,
   VIRTUAL_SWITCH.AD_CAPABLE,
   VIRTUAL_SWITCH.WWN,
   VIRTUAL_SWITCH.ROLE,
   VIRTUAL_SWITCH.FCS_ROLE,
   VIRTUAL_SWITCH.DOMAIN_ID,
   VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID,
   VIRTUAL_SWITCH.BASE_SWITCH,
   VIRTUAL_SWITCH.MAX_ZONE_CONFIG_SIZE,
   VIRTUAL_SWITCH.CREATION_TIME,
   VIRTUAL_SWITCH.LAST_UPDATE_TIME,
   VIRTUAL_SWITCH.USER_NAME,
   VIRTUAL_SWITCH.PASSWORD,
   VIRTUAL_SWITCH.MANAGEMENT_STATE,
   VIRTUAL_SWITCH.STATE,
   VIRTUAL_SWITCH.STATUS,
   VIRTUAL_SWITCH.STATUS_REASON,
   VIRTUAL_SWITCH.FABRIC_IDID_MODE,
   VIRTUAL_SWITCH.LOGICAL_ID,
   VIRTUAL_SWITCH.USER_DEFINED_VALUE_1,
   VIRTUAL_SWITCH.USER_DEFINED_VALUE_2,
   VIRTUAL_SWITCH.USER_DEFINED_VALUE_3,
   VIRTUAL_SWITCH.INTEROP_MODE,
   VIRTUAL_SWITCH.CRYPTO_CAPABLE,
   VIRTUAL_SWITCH.FCR_CAPABLE,
   VIRTUAL_SWITCH.FCIP_CAPABLE,
   VIRTUAL_SWITCH.LF_ENABLED,
```

```
   VIRTUAL_SWITCH.FCOE_CAPABLE,
   VIRTUAL_SWITCH.L2_CAPABLE,
   VIRTUAL_SWITCH.L3_CAPABLE,
   VIRTUAL_SWITCH.DEFAULT_LOGICAL_SWITCH,
   VIRTUAL_SWITCH.FEATURES_SUPPORTED,
   VIRTUAL_SWITCH.FMS_MODE,
   VIRTUAL_SWITCH.DYNAMIC_LOAD_SHARING,
   VIRTUAL_SWITCH.PORT_BASED_ROUTING,
   VIRTUAL_SWITCH.IN_ORDER_DELIVERY,
   VIRTUAL_SWITCH.INSISTENT_DID_MODE,
   VIRTUAL_SWITCH.PREVIOUS_OPERATIONAL_STATUS,
   VIRTUAL_SWITCH.LAST_SCAN_TIME,
   VIRTUAL_SWITCH.DOMAIN_MODE_239,
   VIRTUAL_SWITCH.DOMAIN_ID_OFFSET,
   VIRTUAL_SWITCH.DISCOVERED_PORT_COUNT,
   VIRTUAL_SWITCH.FCOE_LOGIN_ENABLED,
   VIRTUAL_SWITCH.LAST_PORT_MEMBERSHIP_CHANGE,
   VIRTUAL_SWITCH.FCIP_CIRCUIT_CAPABLE,
   VIRTUAL_SWITCH.MAX_FCIP_TUNNELS,
   VIRTUAL_SWITCH.MAX_FCIP_CIRCUITS,
   VIRTUAL_SWITCH.FCIP_LICENSED,
   VIRTUAL_SWITCH.ADDRESSING_MODE,
   VIRTUAL_SWITCH.PREVIOUS_STATE,
   VIRTUAL_SWITCH.MANAGED_ELEMENT_ID,
   VIRTUAL_SWITCH.HIF_ENABLED,
   VIRTUAL_SWITCH.AUTO_SNMP,
   VIRTUAL_SWITCH.RNID_SEQUENCE_NUMBER,
   VIRTUAL_SWITCH.VCS_ID,
   VIRTUAL_SWITCH.CLUSTER_TYPE,
   VIRTUAL_SWITCH.CLUSTER_MODE,
   VIRTUAL_SWITCH.RNID_TAG,
   VIRTUAL_SWITCH.SWITCH_ID,
   VIRTUAL_SWITCH.MONITORED,
   VIRTUAL_SWITCH.FEATURES_ENABLED,
   VIRTUAL_SWITCH.MAPS_ENABLED_ACTIONS,
   VIRTUAL_SWITCH.FABRIC_STATUS,
   FABRIC_MEMBER.FABRIC_ID,
   FABRIC_MEMBER.TRUSTED,
   FABRIC_MEMBER.MISSING,
   FABRIC_MEMBER.MISSING_TIME,
   FABRIC.MANAGED as FABRIC_MANAGED,
   FABRIC.PRINCIPAL_SWITCH_WWN,
   FABRIC.SEED_SWITCH_WWN,
   FABRIC.TYPE as FABRIC_TYPE
from
   CORE_SWITCH,
   VIRTUAL_SWITCH,
   FABRIC_MEMBER,
   FABRIC
where
   VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID
   and FABRIC_MEMBER.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
   and FABRIC_MEMBER.FABRIC_ID = FABRIC.ID;
```

DEVICE_INFO

```
create or replace view DEVICE_INFO as
    select distinct
  DEVICE_NODE.ID as DEVICE_NODE_ID,
```

```
DEVICE_NODE.WWN as DEVICE_NODE_WWN,
DEVICE_NODE.TYPE as DEVICE_NODE_TYPE,
DEVICE_NODE.SYMBOLIC_NAME as DEVICE_NODE_SYMBOLIC_NAME,
DEVICE_NODE.DEVICE_TYPE,
DEVICE_NODE.FDMI_HOST_NAME,
DEVICE_NODE.VENDOR,
DEVICE_NODE.CAPABILITY_,
DEVICE_NODE.AG,
DEVICE_NODE.SIMULATED,
DEVICE_PORT.ID as DEVICE_PORT_ID,
DEVICE_PORT.DOMAIN_ID as DEVICE_PORT_DOMAIN_ID,
DEVICE_PORT.WWN as DEVICE_PORT_WWN,
DEVICE_PORT.NUMBER,
DEVICE_PORT.PORT_ID,
DEVICE_PORT.TYPE as DEVICE_PORT_TYPE,
DEVICE_PORT.SYMBOLIC_NAME as DEVICE_PORT_SYMBOLIC_NAME,
DEVICE_PORT.FC4_TYPE,
DEVICE_PORT.IP_PORT,
DEVICE_PORT.HARDWARE_ADDRESS,
DEVICE_PORT.TRUSTED as DEVICE_PORT_TRUSTED,
DEVICE_PORT.MISSING as DEVICE_PORT_MISSING,
DEVICE_PORT.COS,
DEVICE_PORT.NPV_PHYSICAL,
SWITCH_PORT.ID as SWITCH_PORT_ID,
SWITCH_PORT.WWN as SWITCH_PORT_WWN,
SWITCH_PORT.NAME as SWITCH_PORT_NAME,
SWITCH_PORT.SLOT_NUMBER,
SWITCH_PORT.PORT_NUMBER,
SWITCH_PORT.PORT_INDEX,
SWITCH_PORT.TYPE as SWITCH_PORT_TYPE,
SWITCH_PORT.FULL_TYPE as SWITCH_PORT_FULL_TYPE,
SWITCH_PORT.STATUS as SWITCH_PORT_STATUS,
SWITCH_PORT.HEALTH as SWITCH_PORT_HEALTH,
SWITCH_PORT.SPEED,
SWITCH_PORT.MAX_PORT_SPEED,
SWITCH_PORT.NPIV,
SWITCH_PORT.NPIV_CAPABLE,
SWITCH_PORT.CALCULATED_STATUS,
SWITCH_PORT.AREA_ID,
SWITCH_PORT.PHYSICAL_PORT,
SWITCH_PORT.CATEGORY,
SWITCH_PORT.PERSISTENT_DISABLE,
SWITCH_PORT.BLOCKED,
SWITCH_PORT.FCR_INTEROP_MODE,
SWITCH_PORT.SPEED_TYPE,
SWITCH_INFO.IP_ADDRESS,
SWITCH_INFO.PHYSICAL_SWITCH_WWN,
SWITCH_INFO.FIRMWARE_VERSION,
SWITCH_INFO.REACHABLE,
SWITCH_INFO.SYSLOG_REGISTERED,
SWITCH_INFO.SNMP_REGISTERED,
SWITCH_INFO.ID as VIRTUAL_SWITCH_ID,
SWITCH_INFO.NAME as VIRTUAL_SWITCH_NAME,
SWITCH_INFO.OPERATIONAL_STATUS,
SWITCH_INFO.SWITCH_MODE,
SWITCH_INFO.WWN as VIRTUAL_SWITCH_WWN,
SWITCH_INFO.DOMAIN_ID as VIRTUAL_SWITCH_DOMAIN_ID,
SWITCH_INFO.VIRTUAL_FABRIC_ID,
SWITCH_INFO.BASE_SWITCH,
SWITCH_INFO.STATE as VIRTUAL_SWITCH_STATE,
```

```
  SWITCH_INFO.STATUS as VIRTUAL_SWITCH_STATUS,
  SWITCH_INFO.FABRIC_ID,
  SWITCH_INFO.MONITORED,
  SWITCH_INFO.CRYPTO_CAPABLE
from
  DEVICE_NODE, DEVICE_PORT, SWITCH_PORT, SWITCH_INFO
where
  DEVICE_PORT.NODE_ID = DEVICE_NODE.ID and
  DEVICE_PORT.SWITCH_PORT_WWN = SWITCH_PORT.WWN and
  SWITCH_PORT.VIRTUAL_SWITCH_ID = SWITCH_INFO.ID and
  DEVICE_NODE.FABRIC_ID = SWITCH_INFO.FABRIC_ID;
```

N2F_PORT_MAP_INFO

```
create or replace view N2F_PORT_MAP_INFO as
select
    N2F_PORT_MAP.VIRTUAL_SWITCH_ID,
    N2F_PORT_MAP.N_PORT,
    N2F_PORT_MAP.F_PORT,
    AG_N_PORT.REMOTE_PORT_WWN as EDGE_SWITCH_PORT_WWN,
    AG_N_PORT.WWN as AG_N_PORT_WWN,
    AG_F_PORT.WWN as AG_F_PORT_WWN,
    AG_F_PORT.REMOTE_NODE_WWN,
    AG_F_PORT.REMOTE_PORT_WWN as DEVICE_PORT_WWN
from
    N2F_PORT_MAP,
    SWITCH_PORT AG_N_PORT,
    SWITCH_PORT AG_F_PORT,
    VIRTUAL_SWITCH AG_SWITCH
where
    N2F_PORT_MAP.VIRTUAL_SWITCH_ID = AG_N_PORT.VIRTUAL_SWITCH_ID
    and N2F_PORT_MAP.N_PORT = AG_N_PORT.USER_PORT_NUMBER
    and N2F_PORT_MAP.VIRTUAL_SWITCH_ID = AG_F_PORT.VIRTUAL_SWITCH_ID
    and N2F_PORT_MAP.F_PORT = AG_F_PORT.USER_PORT_NUMBER
    and AG_N_PORT.VIRTUAL_SWITCH_ID = AG_SWITCH.ID
    and AG_SWITCH.MONITORED = 1;
```

DEVICE_NODE_INFO

```
create or replace view DEVICE_NODE_INFO as
select
    DEVICE_NODE.ID,
    DEVICE_NODE.FABRIC_ID,
    DEVICE_NODE.WWN,
    DEVICE_NODE.TYPE,
    DEVICE_NODE.DEVICE_TYPE,
    DEVICE_NODE.SYMBOLIC_NAME,
    DEVICE_NODE.FDMI_HOST_NAME,
    DEVICE_NODE.VENDOR,
    DEVICE_NODE.CAPABILITY_,
    DEVICE_NODE.TRUSTED,
    DEVICE_NODE.CREATION_TIME,
    DEVICE_NODE.MISSING,
    DEVICE_NODE.MISSING_TIME,
    DEVICE_NODE.PROXY_DEVICE,
    DEVICE_NODE.AG,
    DEVICE_NODE.PREVIOUS_MISSING_STATE,
    USER_DEFINED_DEVICE_DETAIL.NAME,
```

```
    USER_DEFINED_DEVICE_DETAIL.TYPE as USER_DEFINED_TYPE,
    USER_DEFINED_DEVICE_DETAIL.IP_ADDRESS,
    USER_DEFINED_DEVICE_DETAIL.CONTACT,
    USER_DEFINED_DEVICE_DETAIL.LOCATION,
    USER_DEFINED_DEVICE_DETAIL.DESCRIPTION,
    USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE1,
    USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE2,
    USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE3,
    FABRIC.PRINCIPAL_SWITCH_WWN as PRINCIPAL_WWN,
    DEVICE_FDMI_DETAILS.SERIAL_NUMBER AS FDMI_SERIAL_NUMBER,
    DEVICE_FDMI_DETAILS.FIRMWARE_VERSION AS FDMI_FIRMWARE_VERSION,
    DEVICE_FDMI_DETAILS.DRIVER_VERSION AS FDMI_DRIVER_VERSION,
    DEVICE_FDMI_DETAILS.MANUFACTURER AS FDMI_MANUFACTURER,
    DEVICE_FDMI_DETAILS.MODEL AS FDMI_MODEL,
    DEVICE_FDMI_DETAILS.HARDWARE_VERSION AS FDMI_HARDWARE_VERSION,
    DEVICE_FDMI_DETAILS.MODEL_DESCRIPTION AS FDMI_MODEL_DESCRIPTION,
    DEVICE_FDMI_DETAILS.NODE_NAME AS FDMI_NODE_NAME
from
    DEVICE_NODE
        left outer join USER_DEFINED_DEVICE_DETAIL
            on DEVICE_NODE.WWN = USER_DEFINED_DEVICE_DETAIL.WWN
        left outer join FABRIC
            on DEVICE_NODE.FABRIC_ID = FABRIC.ID
        left outer join DEVICE_FDMI_DETAILS
            on DEVICE_NODE.ID = DEVICE_FDMI_DETAILS.DEVICE_NODE_ID;
```

DEVICE_PORT_INFO

```
CREATE VIEW device_port_info AS
    select
    DEVICE_PORT.ID,
    DEVICE_PORT.NODE_ID,
    DEVICE_PORT.DOMAIN_ID,
    DEVICE_PORT.WWN,
     DEVICE_PORT.SWITCH_PORT_WWN,
    DEVICE_PORT.NUMBER,
    DEVICE_PORT.PORT_ID,
     DEVICE_PORT.TYPE,
    DEVICE_PORT.SYMBOLIC_NAME,
    DEVICE_PORT.FC4_TYPE,
    DEVICE_PORT.COS,
    DEVICE_PORT.IP_PORT,
    DEVICE_PORT.HARDWARE_ADDRESS,
    DEVICE_PORT.TRUSTED,
    DEVICE_PORT.CREATION_TIME,
    DEVICE_PORT.MISSING,
    DEVICE_PORT.MISSING_TIME,
     DEVICE_PORT.NPV_PHYSICAL,
     DEVICE_PORT.EDGE_SWITCH_PORT_WWN,
    DEVICE_PORT.LOGGED_TO_AG,
     DEVICE_PORT.AG_NODE_WWN,
     DEVICE_PORT.AG_N_PORT_WWN,
     DEVICE_PORT.MISSING_REASON,
     FICON_DEVICE_PORT.TYPE_NUMBER,
    FICON_DEVICE_PORT.MODEL_NUMBER,
    FICON_DEVICE_PORT.MANUFACTURER,
    FICON_DEVICE_PORT.MANUFACTURER_PLANT,
    FICON_DEVICE_PORT.SEQUENCE_NUMBER,
    FICON_DEVICE_PORT.TAG,
```

```
    FICON_DEVICE_PORT.FLAG,
    FICON_DEVICE_PORT.PARAMS,
    USER_DEFINED_DEVICE_DETAIL.NAME,
    USER_DEFINED_DEVICE_DETAIL.TYPE as USER_DEFINED_TYPE,
    USER_DEFINED_DEVICE_DETAIL.IP_ADDRESS,
    USER_DEFINED_DEVICE_DETAIL.CONTACT,
    USER_DEFINED_DEVICE_DETAIL.LOCATION,
    USER_DEFINED_DEVICE_DETAIL.DESCRIPTION,
    USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE1,
    USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE2,
    USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE3,
     DEVICE_NODE.WWN as DEVICE_NODE_WWN,
     DEVICE_NODE.FDMI_HOST_NAME,
     DEVICE_NODE.SYMBOLIC_NAME as DEVICE_SYMBOLIC_NAME,
     DEVICE_NODE.AG as AG_PORT,
     coalesce(SWITCH_PORT.NAME, VIRTUAL_FCOE_PORT.NAME) as SWITCH_PORT_NAME,
     coalesce (SWITCH_PORT.TYPE, VIRTUAL_FCOE_PORT.PORT_TYPE) as SWITCH_PORT_TYPE,
     SWITCH_PORT.LOGICAL_PORT_WWN,
     coalesce(VS1.WWN, VS2.WWN) as SWITCH_WWN,
     coalesce(VS1.MANAGEMENT_STATE, VS2.MANAGEMENT_STATE) as MANAGEMENT_STATE,
     coalesce(VS1.MONITORED, VS2.MONITORED) as MONITORED,
     FABRIC.PRINCIPAL_SWITCH_WWN as PRINCIPAL_WWN,
     FABRIC.ID as FABRIC_ID
from
    DEVICE_PORT
        left outer join USER_DEFINED_DEVICE_DETAIL
            on DEVICE_PORT.WWN = USER_DEFINED_DEVICE_DETAIL.WWN
        left outer join FICON_DEVICE_PORT
            on DEVICE_PORT.ID = FICON_DEVICE_PORT.DEVICE_PORT_ID
         left outer join DEVICE_NODE
             on DEVICE_PORT.NODE_ID = DEVICE_NODE.ID
         left outer join SWITCH_PORT
             on DEVICE_PORT.SWITCH_PORT_WWN = SWITCH_PORT.WWN
         left outer join VIRTUAL_FCOE_PORT
             on DEVICE_PORT.SWITCH_PORT_WWN = VIRTUAL_FCOE_PORT.PORT_WWN
         left outer join VIRTUAL_SWITCH VS1
             on SWITCH_PORT.VIRTUAL_SWITCH_ID = VS1.ID
         left outer join VIRTUAL_SWITCH VS2
             on VIRTUAL_FCOE_PORT.VIRTUAL_SWITCH_ID = VS2.ID
         left outer join FABRIC
             on DEVICE_NODE.FABRIC_ID = FABRIC.ID;
```

DEV_PORT_GIGE_PORT_LINK_INFO

```
create or replace view DEV_PORT_GIGE_PORT_LINK_INFO as
select
    DEVICE_PORT_GIGE_PORT_LINK.DEVICE_PORT_ID,
    DEVICE_PORT_GIGE_PORT_LINK.GIGE_PORT_ID,
    DEVICE_PORT_GIGE_PORT_LINK.DIRECT_ATTACH,
    DEVICE_PORT_GIGE_PORT_LINK.VIRTUAL_FCOE_PORT_ID,
    DEVICE_PORT.TRUSTED,
    DEVICE_PORT.CREATION_TIME,
    DEVICE_PORT.MISSING,
    DEVICE_PORT.MISSING_TIME,
    DEVICE_PORT_GIGE_PORT_LINK.LAG_ID
from
    DEVICE_PORT_GIGE_PORT_LINK,
    DEVICE_PORT
where
```

```
    DEVICE_PORT_GIGE_PORT_LINK.DEVICE_PORT_ID = DEVICE_PORT.ID;
```

DEV_PORT_MAC_ADDR_MAP_INFO

```
create or replace view DEV_PORT_MAC_ADDR_MAP_INFO as
select
    DEVICE_PORT_MAC_ADDRESS_MAP.DEVICE_PORT_ID,
    DEVICE_PORT_MAC_ADDRESS_MAP.MAC_ADDRESS,
    DEVICE_NODE.ID as DEVICE_NODE_ID,
    DEVICE_NODE.FABRIC_ID,
    DEVICE_PORT.TRUSTED,
    DEVICE_PORT.CREATION_TIME,
    DEVICE_PORT.MISSING,
    DEVICE_PORT.MISSING_TIME
from
    DEVICE_PORT_MAC_ADDRESS_MAP,
    DEVICE_PORT,
    DEVICE_NODE
where
    DEVICE_PORT_MAC_ADDRESS_MAP.DEVICE_PORT_ID = DEVICE_PORT.ID
    and DEVICE_PORT.NODE_ID = DEVICE_NODE.ID;
```

ISL_CONNECTION_INFO

```
create or replace view ISL_CONNECTION_INFO as
select
 distinct ISL_CONNECTION.ID,
 ISL_CONNECTION.FABRIC_ID,
 ISL_CONNECTION.SOURCE_SWITCH_PORT_ID,
 ISL_CONNECTION.TARGET_SWITCH_PORT_ID,
 ISL_CONNECTION.COST,
 ISL_CONNECTION.TYPE,
 ISL_CONNECTION.TRUSTED,
 ISL_CONNECTION.MISSING,
 ISL_CONNECTION.MISSING_TIME,
 ISL_CONNECTION.CREATION_TIME,
 ISL_CONNECTION.TRUNKED,
 SOURCE_SWITCH_PORT.VIRTUAL_SWITCH_ID as SOURCE_SWITCH_ID,
 SOURCE_SWITCH_PORT.USER_PORT_NUMBER as SOURCE_SWITCH_PORT_NUMBER,
 DEST_SWITCH_PORT.VIRTUAL_SWITCH_ID as DEST_SWITCH_ID,
 DEST_SWITCH_PORT.USER_PORT_NUMBER as DEST_SWITCH_PORT_NUMBER

from
 ISL_CONNECTION,
 SWITCH_PORT SOURCE_SWITCH_PORT,
 SWITCH_PORT DEST_SWITCH_PORT

where
 ISL_CONNECTION.SOURCE_SWITCH_PORT_ID = SOURCE_SWITCH_PORT.ID
 and ISL_CONNECTION.TARGET_SWITCH_PORT_ID = DEST_SWITCH_PORT.ID;
```

ISL_INFO

```
create or replace view ISL_INFO as
select distinct
```

```
    ISL.ID,
    ISL.FABRIC_ID,
    ISL.COST,
    ISL.TYPE,
    ISL.SOURCE_DOMAIN_ID,
    ISL.SOURCE_PORT_NUMBER,
    ISL.MISSING,
     ISL.MISSING_TIME,
     ISL.TRUSTED,
     ISL.CREATION_TIME,
     ISL.TRUNKED,
    SOURCE_VIRTUAL_SWITCH.ID as SOURCE_SWITCH_ID,
    SOURCE_VIRTUAL_SWITCH.NAME as SOURCE_SWITCH_NAME,
    SOURCE_VIRTUAL_SWITCH.WWN as SOURCE_SWITCH_WWN,
     SOURCE_VIRTUAL_SWITCH.CORE_SWITCH_ID as SOURCE_CORE_SWITCH_ID,
     SOURCE_VIRTUAL_SWITCH.BASE_SWITCH as SOURCE_BASE_SWITCH,
     SOURCE_VIRTUAL_SWITCH.MANAGEMENT_STATE as
SOURCE_VIRTUAL_SWITCH_MANAGEMENT_STATE,
     SOURCE_VIRTUAL_SWITCH.MONITORED as SOURCE_VIRTUAL_SWITCH_MONITORED,
     SOURCE_SWITCH_PORT.ID as SOURCE_SWITCH_PORT_ID,
    SOURCE_SWITCH_PORT.WWN as SOURCE_SWITCH_PORT_WWN,
    SOURCE_SWITCH_PORT.NAME as SOURCE_SWITCH_PORT_NAME,
     SOURCE_SWITCH_PORT.TYPE as PORT_TYPE,
     SOURCE_SWITCH_PORT.KIND as SOURCE_SWITCH_PORT_KIND,
     SOURCE_SWITCH_PORT.PHYSICAL_PORT as SOURCE_PHYSICAL_PORT,
     SOURCE_SWITCH_PORT.TRUNKED as SOURCE_SWITCH_PORT_TRUNKED,
     ISL.DEST_DOMAIN_ID,
    ISL.DEST_PORT_NUMBER,
    DEST_VIRTUAL_SWITCH.ID as DEST_SWITCH_ID,
    DEST_VIRTUAL_SWITCH.NAME as DEST_SWITCH_NAME,
     DEST_VIRTUAL_SWITCH.WWN as DEST_SWITCH_WWN,
     DEST_VIRTUAL_SWITCH.CORE_SWITCH_ID as DEST_CORE_SWITCH_ID,
     DEST_VIRTUAL_SWITCH.BASE_SWITCH as DEST_BASE_SWITCH,
     DEST_VIRTUAL_SWITCH.MANAGEMENT_STATE as DEST_VIRTUAL_SWITCH_MANAGEMENT_STATE,
     DEST_VIRTUAL_SWITCH.MONITORED as DEST_VIRTUAL_SWITCH_MONITORED,
    DEST_SWITCH_PORT.ID as DEST_SWITCH_PORT_ID,
    DEST_SWITCH_PORT.WWN as DEST_SWITCH_PORT_WWN,
     DEST_SWITCH_PORT.NAME as DEST_SWITCH_PORT_NAME,
     DEST_SWITCH_PORT.KIND as DEST_SWITCH_PORT_KIND,
     DEST_SWITCH_PORT.PHYSICAL_PORT as DEST_PHYSICAL_PORT,
     DEST_SWITCH_PORT.TRUNKED as DEST_SWITCH_PORT_TRUNKED,
     FABRIC.PRINCIPAL_SWITCH_WWN as PRINCIPAL_SWITCH_WWN
from
    ISL,
     FABRIC_MEMBER SOURCE_FABRIC_MEMBER,
     VIRTUAL_SWITCH         SOURCE_VIRTUAL_SWITCH,
     SWITCH_PORT   SOURCE_SWITCH_PORT,
     FABRIC_MEMBER DEST_FABRIC_MEMBER,
     VIRTUAL_SWITCH         DEST_VIRTUAL_SWITCH,
     SWITCH_PORT   DEST_SWITCH_PORT,
     FABRIC
where
    SOURCE_FABRIC_MEMBER.FABRIC_ID = ISL.FABRIC_ID and
    SOURCE_VIRTUAL_SWITCH.ID = SOURCE_FABRIC_MEMBER.VIRTUAL_SWITCH_ID and
    SOURCE_VIRTUAL_SWITCH.DOMAIN_ID = ISL.SOURCE_DOMAIN_ID and
    SOURCE_SWITCH_PORT.VIRTUAL_SWITCH_ID = SOURCE_VIRTUAL_SWITCH.ID and
     SOURCE_SWITCH_PORT.CATEGORY = 1 and
    SOURCE_SWITCH_PORT.USER_PORT_NUMBER = ISL.SOURCE_PORT_NUMBER and
    DEST_FABRIC_MEMBER.FABRIC_ID = ISL.FABRIC_ID and
    DEST_VIRTUAL_SWITCH.ID = DEST_FABRIC_MEMBER.VIRTUAL_SWITCH_ID and
```

```
    DEST_VIRTUAL_SWITCH.DOMAIN_ID = ISL.DEST_DOMAIN_ID and
    DEST_SWITCH_PORT.VIRTUAL_SWITCH_ID = DEST_VIRTUAL_SWITCH.ID and
     DEST_SWITCH_PORT.CATEGORY = 1 and
    DEST_SWITCH_PORT.USER_PORT_NUMBER = ISL.DEST_PORT_NUMBER and
     FABRIC.ID = ISL.FABRIC_ID;
```

ETHERNET_ISL_INFO

```
create or replace view ETHERNET_ISL_INFO as
select
    ETHERNET_ISL.ID as ETHERNET_ISL_ID,
    ETHERNET_ISL.SOURCE_PORT_ID,
    ETHERNET_ISL.DEST_PORT_ID,
    ETHERNET_ISL.TRUSTED,
    ETHERNET_ISL.CREATION_TIME,
    ETHERNET_ISL.MISSING,
    ETHERNET_ISL.MISSING_TIME,
    SOURCE_SWITCH_PORT.VIRTUAL_SWITCH_ID as SOURCE_SWITCH_ID,
    SOURCE_SWITCH_PORT.USER_PORT_NUMBER as SOURCE_PORT_NUMBER,
    SOURCE_SWITCH_PORT.TYPE as SOURCE_PORT_TYPE,
    SOURCE_VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID as SOURCE_VIRTUAL_FABRIC_ID,
    DEST_SWITCH_PORT.VIRTUAL_SWITCH_ID as DEST_SWITCH_ID,
    DEST_SWITCH_PORT.USER_PORT_NUMBER as DEST_PORT_NUMBER,
    DEST_SWITCH_PORT.TYPE as DEST_PORT_TYPE,
    DEST_VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID as DEST_VIRTUAL_FABRIC_ID
from
    ETHERNET_ISL,
    GIGE_PORT       SOURCE_GIGE_PORT,
    VIRTUAL_SWITCH  SOURCE_VIRTUAL_SWITCH,
    SWITCH_PORT     SOURCE_SWITCH_PORT,
    GIGE_PORT       DEST_GIGE_PORT,
    VIRTUAL_SWITCH  DEST_VIRTUAL_SWITCH,
    SWITCH_PORT     DEST_SWITCH_PORT
where
    SOURCE_GIGE_PORT.ID  = ETHERNET_ISL.SOURCE_PORT_ID and
    SOURCE_GIGE_PORT.SWITCH_PORT_ID = SOURCE_SWITCH_PORT.ID and
    SOURCE_SWITCH_PORT.VIRTUAL_SWITCH_ID = SOURCE_VIRTUAL_SWITCH.ID and
    DEST_GIGE_PORT.ID  = ETHERNET_ISL.DEST_PORT_ID and
    DEST_GIGE_PORT.SWITCH_PORT_ID = DEST_SWITCH_PORT.ID and
    DEST_SWITCH_PORT.VIRTUAL_SWITCH_ID = DEST_VIRTUAL_SWITCH.ID;
```

EVENT_DETAILS_INFO

```
create or replace view EVENT_DETAILS_INFO (ID, ME_ID, SEVERITY, AREA,
ACKNOWLEDGED, SOURCE_NAME, SOURCE_ADDR, LAST_OCCURRENCE_HOST_TIME,
FIRST_OCCURRENCE_HOST_TIME, EVENT_COUNT, EVENT_KEY, AUDIT, RESOLVED, ACKED_TIME,
EVENT_ACTION_ID, DEVICE_GROUP_ID, PORT_GROUP_ID, SPECIAL_EVENT, ORIGIN,
EVENT_CATEGORY, DESCRIPTION, MODULE, RAS_LOG_ID, PRODUCT_ADDRESS, CONTRIBUTORS,
NODE_WWN, PORT_WWN, OPERATIONAL_STATUS, FIRST_OCCURRENCE_SWITCH_TIME,
LAST_OCCURRENCE_SWITCH_TIME, VIRTUAL_FABRIC_ID, UNIT, SLOT, PORT, OID, USER_NAME,
EVENT_NUMBER, FRU_CODE, REASON_CODE, FRU_POSITION, INTERFACE_TYPE, PORT_NAME,
MAC_ADDRESS) as
select
    EVENT.ID as ID,
    EVENT.ME_ID as ME_ID,
    EVENT.SEVERITY as SEVERITY,
    EVENT.AREA as AREA,
    EVENT.ACKNOWLEDGED as ACKNOWLEDGED,
```

```
    EVENT.SOURCE_NAME as SOURCE_NAME,
    EVENT.SOURCE_ADDR as SOURCE_ADDR,
    EVENT.LAST_OCCURRENCE_HOST_TIME as LAST_OCCURRENCE_HOST_TIME,
    EVENT.FIRST_OCCURRENCE_HOST_TIME as FIRST_OCCURRENCE_HOST_TIME,
    EVENT.EVENT_COUNT as EVENT_COUNT,
    EVENT.EVENT_KEY as EVENT_KEY,
    EVENT.EVENT_AUDIT as AUDIT,
    EVENT.RESOLVED as RESOLVED,
    EVENT.ACKED_TIME as ACKED_TIME,
    EVENT.EVENT_ACTION_ID as EVENT_ACTION_ID,
    EVENT.DEVICE_GROUP_ID as DEVICE_GROUP_ID,
    EVENT.PORT_GROUP_ID as PORT_GROUP_ID,
    EVENT.SPECIAL_EVENT,
    EVENT_ORIGIN.ID as ORIGIN,
    EVENT_CATEGORY.ID as EVENT_CATEGORY,
    EVENT_DESCRIPTION.DESCRIPTION as DESCRIPTION,
    EVENT_MODULE.ID as MODULE,
    EVENT_DETAILS.RAS_LOG_ID as RAS_LOG_ID,
    EVENT_DETAILS.PRODUCT_ADDRESS as PRODUCT_ADDRESS,
    EVENT_DETAILS.CONTRIBUTORS as CONTRIBUTORS,
    EVENT_DETAILS.NODE_WWN as NODE_WWN,
    EVENT_DETAILS.PORT_WWN as PORT_WWN,
    EVENT_DETAILS.OPERATIONAL_STATUS as OPERATIONAL_STATUS,
    EVENT_DETAILS.FIRST_OCCURRENCE_SWITCH_TIME as FIRST_OCCURRENCE_SWITCH_TIME,
    EVENT_DETAILS.LAST_OCCURRENCE_SWITCH_TIME as LAST_OCCURRENCE_SWITCH_TIME,
    EVENT_DETAILS.VIRTUAL_FABRIC_ID as VIRTUAL_FABRIC_ID,
    EVENT_DETAILS.UNIT as UNIT,
    EVENT_DETAILS.SLOT as SLOT,
    EVENT_DETAILS.PORT as PORT,
    EVENT_DETAILS.OID,
    EVENT_DETAILS.USER_NAME as USER_NAME,
    EVENT_CALL_HOME.EVENT_NUMBER as EVENT_NUMBER,
    EVENT_CALL_HOME.FRU_CODE as FRU_CODE,
    EVENT_CALL_HOME.REASON_CODE as REASON_CODE,
    EVENT_CALL_HOME.FRU_POSITION as FRU_POSITION,
    EVENT_DETAILS.INTERFACE_TYPE as INTERFACE_TYPE,
    EVENT_DETAILS.PORT_NAME as PORT_NAME,
    EVENT_DETAILS.MAC_ADDRESS
from
    EVENT
        left outer join EVENT_ORIGIN on EVENT.EVENT_ORIGIN_ID = EVENT_ORIGIN.ID
        left outer join EVENT_CATEGORY on EVENT.EVENT_CATEGORY_ID =
EVENT_CATEGORY.ID
        left outer join EVENT_MODULE on EVENT.EVENT_MODULE_ID = EVENT_MODULE.ID
        left outer join EVENT_DESCRIPTION on EVENT.EVENT_DESCRIPTION_ID =
EVENT_DESCRIPTION.ID
        left outer join EVENT_DETAILS on EVENT.ID = EVENT_DETAILS.EVENT_ID
       left outer join EVENT_CALL_HOME on EVENT.ID = EVENT_CALL_HOME.EVENT_ID;
```

EVENT_INFO

```
create or replace view EVENT_INFO as
select
    EVENT.ID as ID,
    EVENT.ME_ID as ME_ID,
    EVENT.SEVERITY as SEVERITY,
    EVENT.AREA as AREA,
    EVENT.ACKNOWLEDGED as ACKNOWLEDGED,
    EVENT.SOURCE_NAME as SOURCE_NAME,
```

```
    EVENT.SOURCE_ADDR as SOURCE_ADDR,
    EVENT.LAST_OCCURRENCE_HOST_TIME as LAST_OCCURRENCE_HOST_TIME,
    EVENT.FIRST_OCCURRENCE_HOST_TIME as FIRST_OCCURRENCE_HOST_TIME,
    EVENT.EVENT_COUNT as EVENT_COUNT,
    EVENT.EVENT_AUDIT as AUDIT,
    EVENT.EVENT_ACTION_ID,
    EVENT.SPECIAL_EVENT,
    EVENT_ORIGIN.ID as ORIGIN,
    EVENT_CATEGORY.ID as EVENT_CATEGORY,
    EVENT_DESCRIPTION.DESCRIPTION as DESCRIPTION,
    EVENT_MODULE.ID as MODULE,
    EVENT_DETAILS.RAS_LOG_ID as RAS_LOG_ID,
    EVENT_DETAILS.PRODUCT_ADDRESS as PRODUCT_ADDRESS,
    EVENT_DETAILS.CONTRIBUTORS as CONTRIBUTORS,
    EVENT_DETAILS.NODE_WWN as NODE_WWN,
    EVENT_DETAILS.OPERATIONAL_STATUS as OPERATIONAL_STATUS,
    EVENT_DETAILS.FIRST_OCCURRENCE_SWITCH_TIME as FIRST_OCCURRENCE_SWITCH_TIME,
    EVENT_DETAILS.LAST_OCCURRENCE_SWITCH_TIME as LAST_OCCURRENCE_SWITCH_TIME,
    EVENT_DETAILS.VIRTUAL_FABRIC_ID as VIRTUAL_FABRIC_ID,
    EVENT_DETAILS.USER_NAME as USER_NAME,
    EVENT_DETAILS.PORT_NAME as PORT_NAME,
    EVENT_DETAILS.MAC_ADDRESS
from
    EVENT
        left join EVENT_DETAILS on EVENT.ID = EVENT_DETAILS.EVENT_ID,
EVENT_ORIGIN, EVENT_CATEGORY, EVENT_MODULE, EVENT_DESCRIPTION
       where EVENT.EVENT_ORIGIN_ID = EVENT_ORIGIN.ID and EVENT.EVENT_CATEGORY_ID
= EVENT_CATEGORY.ID and EVENT.EVENT_MODULE_ID = EVENT_MODULE.ID
        and   EVENT.EVENT_DESCRIPTION_ID = EVENT_DESCRIPTION.ID;
```

FABRIC_INFO

```
CREATE VIEW fabric_info AS
    select
    FABRIC.ID,
    FABRIC.SAN_ID,
    FABRIC.SEED_SWITCH_WWN,
    FABRIC.NAME,
    FABRIC.ACTIVE_ZONESET_NAME,
    FABRIC.MANAGEMENT_STATE,
    FABRIC.LAST_FABRIC_CHANGED,
    FABRIC.SECURE,
    FABRIC.AD_ENVIRONMENT,
    FABRIC.MANAGED,
    FABRIC.CONTACT,
    FABRIC.LOCATION,
    FABRIC.DESCRIPTION,
    FABRIC.CREATION_TIME,
    FABRIC.LAST_SCAN_TIME,
    FABRIC.LAST_UPDATE_TIME,
    FABRIC.TRACK_CHANGES,
    FABRIC.TYPE,
     FABRIC.HAS_NOS_AG,
     FABRIC.USER_DEFINED_VALUE_1,
     FABRIC.USER_DEFINED_VALUE_2,
     FABRIC.USER_DEFINED_VALUE_3,
    FABRIC.PRINCIPAL_SWITCH_WWN,
    FABRIC.ZONE_TRANSACTION_TIMEOUT,
     FABRIC.FABRIC_MODEL,
```

```
    FABRIC.ENHANCED_TI_ZONE_SUPPORT,
    FABRIC.FABRIC_NAME,
    VIRTUAL_SWITCH.ID as SEED_SWITCH_ID,
   VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID,
    VIRTUAL_SWITCH.INTEROP_MODE,
   CORE_SWITCH.IP_ADDRESS as SEED_SWITCH_IP_ADDRESS,
   (select count(*) from FABRIC_MEMBER
        where FABRIC_MEMBER.FABRIC_ID = FABRIC.ID) as SWITCH_COUNT
from
   FABRIC, CORE_SWITCH, VIRTUAL_SWITCH, FABRIC_MEMBER
where
   FABRIC.SEED_SWITCH_WWN = VIRTUAL_SWITCH.WWN and
   VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID and
   FABRIC_MEMBER.FABRIC_ID = FABRIC.ID;
```

FCIP_TUNNEL_CIRCUIT_INFO

```
CREATE VIEW fcip_tunnel_circuit_info AS
   select
    FCIP_TUNNEL_CIRCUIT.ID,
    FCIP_TUNNEL_CIRCUIT.TUNNEL_ID,
    FCIP_TUNNEL_CIRCUIT.CIRCUIT_NUMBER,
    FCIP_TUNNEL_CIRCUIT.COMPRESSION_ENABLED,
    FCIP_TUNNEL_CIRCUIT.TURBO_WRITE_ENABLED,
    FCIP_TUNNEL_CIRCUIT.TAPE_ACCELERATION_ENABLED,
    FCIP_TUNNEL_CIRCUIT.IKE_POLICY_NUM,
    FCIP_TUNNEL_CIRCUIT.IPSEC_POLICY_NUM,
    FCIP_TUNNEL_CIRCUIT.PRESHARED_KEY,
    FCIP_TUNNEL_CIRCUIT.SOURCE_IP,
    FCIP_TUNNEL_CIRCUIT.DEST_IP,
    FCIP_TUNNEL_CIRCUIT.VLAN_TAG,
    FCIP_TUNNEL_CIRCUIT.SELECTIVE_ACK,
    FCIP_TUNNEL_CIRCUIT.QOS_MAPPING,
    FCIP_TUNNEL_CIRCUIT.PATH_MTU_DISCOVERY,
    FCIP_TUNNEL_CIRCUIT.MIN_COMM_RATE,
    FCIP_TUNNEL_CIRCUIT.MAX_COMM_RATE,
    FCIP_TUNNEL_CIRCUIT.MIN_RETRANSMIT_TIME,
    FCIP_TUNNEL_CIRCUIT.MAX_RETRANSMIT_TIME,
    FCIP_TUNNEL_CIRCUIT.KEEP_ALIVE_TIMEOUT,
    FCIP_TUNNEL_CIRCUIT.ADMIN_STATUS,
    FCIP_TUNNEL_CIRCUIT.METRIC,
    FCIP_TUNNEL_CIRCUIT.DATA_L2_COS,
    FCIP_TUNNEL_CIRCUIT.DSCP_DATA,
    FCIP_TUNNEL_CIRCUIT.MAX_RETRANSMISSIONS,
    FCIP_TUNNEL_CIRCUIT.SLOT_NUMBER,
    FCIP_TUNNEL_CIRCUIT.VE_PORT_NUMBER,
    FCIP_TUNNEL_CIRCUIT.SECURITY_FLAG,
    FCIP_TUNNEL_CIRCUIT.DSCP_CONTROL,
    FCIP_TUNNEL_CIRCUIT.CIRCUIT_STATUS,
    FCIP_TUNNEL_CIRCUIT.ENABLED,
    FCIP_TUNNEL_CIRCUIT.MISMATCHED_CONFIGURATIONS,
    FCIP_TUNNEL_CIRCUIT.CIRCUIT_STATUS_STRING,
    FCIP_TUNNEL_CIRCUIT.L2COS_F_CLASS,
    FCIP_TUNNEL_CIRCUIT.L2_COS_HIGH,
    FCIP_TUNNEL_CIRCUIT.L2_COS_MEDIUM,
    FCIP_TUNNEL_CIRCUIT.L2_COS_LOW,
    FCIP_TUNNEL_CIRCUIT.DSCP_F_CLASS,
    FCIP_TUNNEL_CIRCUIT.DSCP_HIGH,
    FCIP_TUNNEL_CIRCUIT.DSCP_MEDIUM,
```

```
    FCIP_TUNNEL_CIRCUIT.DSCP_LOW,
    FCIP_TUNNEL_CIRCUIT.FAILOVER_CIRCUIT,
    FCIP_TUNNEL_CIRCUIT.FAILOVER_GROUP_ID,
    GIGE_PORT.PORT_NUMBER GIGE_PORT_NUMBER,
    GIGE_PORT.SLOT_NUMBER GIGE_PORT_SLOT_NUMBER,
    FCIP_CIRCUIT_PORT_MAP.SWITCH_PORT_ID GIGE_PORT_ID,
    SWITCH_PORT.VIRTUAL_SWITCH_ID,
    SWITCH_PORT.USER_PORT_NUMBER
from
    FCIP_TUNNEL_CIRCUIT
        left outer join FCIP_CIRCUIT_PORT_MAP on
            FCIP_CIRCUIT_PORT_MAP.CIRCUIT_ID = FCIP_TUNNEL_CIRCUIT.ID
        left outer join GIGE_PORT
            on FCIP_CIRCUIT_PORT_MAP.SWITCH_PORT_ID = GIGE_PORT.ID
        left outer join SWITCH_PORT
            on GIGE_PORT.SWITCH_PORT_ID = SWITCH_PORT.ID;
```

FCIP_TUNNEL_INFO

```
create or replace view FCIP_TUNNEL_INFO as
select
   FCIP_TUNNEL.ID,
   FCIP_TUNNEL.TUNNEL_ID,
   FCIP_TUNNEL.VLAN_TAG,
   FCIP_TUNNEL.SOURCE_IP,
   FCIP_TUNNEL.DEST_IP,
   FCIP_TUNNEL.LOCAL_WWN,
   FCIP_TUNNEL.REMOTE_WWN_RESTRICT,
   FCIP_TUNNEL.COMMUNICATION_RATE,
   FCIP_TUNNEL.MIN_RETRANSMIT_TIME,
   FCIP_TUNNEL.SELECTIVE_ACK_ENABLED,
   FCIP_TUNNEL.KEEP_ALIVE_TIMEOUT,
   FCIP_TUNNEL.MAX_RETRANSMISSION,
   FCIP_TUNNEL.WAN_TOV_ENABLED,
   FCIP_TUNNEL.TUNNEL_STATUS,
   FCIP_TUNNEL.DESCRIPTION,
   FCIP_TUNNEL.FICON_TRB_ID_ENABLED,
   FCIP_TUNNEL.FICON_TT_EMUL_ENABLED,
   FCIP_TUNNEL.FICON_DLA_EMUL_ENABLED,
   FCIP_TUNNEL.FICON_TAPE_WRITE_MAX_PIPE,
   FCIP_TUNNEL.FICON_TAPE_READ_MAX_PIPE,
   FCIP_TUNNEL.FICON_TAPE_WRITE_MAX_OPS,
   FCIP_TUNNEL.FICON_TAPE_READ_MAX_OPS,
   FCIP_TUNNEL.FICON_TAPE_WRITE_TIMER,
   FCIP_TUNNEL.FICON_TAPE_MAX_WRITE_CHAIN,
   FCIP_TUNNEL.FICON_OXID_BASE,
   FCIP_TUNNEL.FICON_XRC_EMULATION_ENABLED,
   FCIP_TUNNEL.FICON_TW_EMUL_ENABLED,
   FCIP_TUNNEL.FICON_TR_EMUL_ENABLED,
   FCIP_TUNNEL.FICON_DEBUG_FLAGS,
   FCIP_TUNNEL.REMOTE_WWN,
   FCIP_TUNNEL.CDC,
   FCIP_TUNNEL.ADMIN_STATUS,
   FCIP_TUNNEL.CONTROL_L2_COS,
   FCIP_TUNNEL.DSCP_CONTROL,
   FCIP_TUNNEL.TRUNKING_ALGORITHM,
   FCIP_TUNNEL.EXTENDED_TUNNEL,
   FCIP_TUNNEL.VIRTUAL_SWITCH_ID,
   FCIP_TUNNEL.CIRCUIT_COUNT,
```

```
   FCIP_TUNNEL.MISMATCHED_CONFIG_DETAILS,
   FCIP_TUNNEL.SLOT_NUMBER,
   FCIP_TUNNEL.FICON_ENABLED,
   FCIP_TUNNEL.TPERF_ENABLED,
   FCIP_TUNNEL.AUTH_KEY,
   FCIP_TUNNEL.CONNECTED_COUNT,
   FCIP_TUNNEL.TUNNEL_STATUS_STRING,
   FCIP_TUNNEL.COMPRESSION_MODE,
   FCIP_TUNNEL.TURBO_WRITE_ENABLED,
   FCIP_TUNNEL.TAPE_ACCELERATION_ENABLED,
   FCIP_TUNNEL.IPSEC_ENABLED,
   FCIP_TUNNEL.PRESHARED_KEY,
   FCIP_TUNNEL.QOS_HIGH,
   FCIP_TUNNEL.QOS_MEDIUM,
   FCIP_TUNNEL.QOS_LOW,
   FCIP_TUNNEL.BACKWARD_COMPATIBLE,
   FCIP_TUNNEL.FICON_TERADATA_READ_ENABLED,
   FCIP_TUNNEL.FICON_TERADATA_WRITE_ENABLED,
   PORT.WWN as VIRTUAL_PORT_WWN,
   PORT.REMOTE_PORT_WWN as REMOTE_PORT_WWN,
   PORT.REMOTE_NODE_WWN as REMOTE_NODE_WWN,
   PORT.ID as SWITCH_PORT_ID,
   PORT.PORT_NUMBER as SWITCH_PORT_NUMBER,
   PORT.USER_PORT_NUMBER as USER_PORT_NUMBER,
   PORT.PORT_INDEX,
   PORT.STATUS_MESSAGE
from
   FCIP_TUNNEL
     left outer join
     FCIP_PORT_TUNNEL_MAP on
     FCIP_PORT_TUNNEL_MAP.TUNNEL_ID = FCIP_TUNNEL.ID
     left outer join SWITCH_PORT PORT
            on FCIP_PORT_TUNNEL_MAP.SWITCHPORT_ID = PORT.ID;
```

FCOE_DEVICE_INFO

```
create or replace view FCOE_DEVICE_INFO as
select
    FCOE_DEVICE.DEVICE_NODE_ID,
    FCOE_DEVICE.DIRECT_ATTACH,
    FCOE_DEVICE.ATTACH_ID,
    FCOE_DEVICE.MAC_ADDRESS,
    DEVICE_NODE.TRUSTED,
    DEVICE_NODE.CREATION_TIME,
    DEVICE_NODE.MISSING,
    DEVICE_NODE.MISSING_TIME
from
    FCOE_DEVICE,
    DEVICE_NODE
where
    FCOE_DEVICE.DEVICE_NODE_ID = DEVICE_NODE.ID;
```

FRU_INFO

```
create or replace view FRU_INFO as
select
    FRU.ID,
    FRU.CORE_SWITCH_ID,
```

```
    FRU.TAG,
    FRU.PART_NUMBER,
    FRU.SERIAL_NUMBER,
    FRU.VENDOR_PART_NUMBER,
    FRU.VENDOR_SERIAL_NUMBER,
    FRU.CAN_BE_FRUED,
    FRU.SLOT_NUMBER,
    FRU.MANUFACTURER_DATE,
    FRU.UPDATE_DATE,
    FRU.VERSION,
    FRU.MANUFACTURER,
    FRU.VENDOR_EQUIPMENT_TYPE,
    FRU.OPERATIONAL_STATUS,
    FRU.TOTAL_OUTPUT_POWER,
    FRU.SPEED,
    FRU.CREATION_TIME,
    FRU.LAST_UPDATE_TIME,
    FRU.PREVIOUS_OP_STATUS,
    FRU.VENDOR,
    CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN,
    VIRTUAL_SWITCH.SWITCH_MODE as VIRTUAL_SWITCH_MODE,
    VIRTUAL_SWITCH.MANAGEMENT_STATE,
    VIRTUAL_SWITCH.MONITORED
from
    FRU,
    CORE_SWITCH,
    VIRTUAL_SWITCH
where
    FRU.CORE_SWITCH_ID = CORE_SWITCH.ID and
    FRU.CORE_SWITCH_ID = VIRTUAL_SWITCH.CORE_SWITCH_ID;
```

GIGE_PORT_ECLOUD_LINK_INFO

```
create or replace view GIGE_PORT_ECLOUD_LINK_INFO as
select
    GIGE_PORT_ETHERNET_CLOUD_LINK.ID,
    GIGE_PORT_ETHERNET_CLOUD_LINK.SWITCH_PORT_ID as GIGE_PORT_ID,
    GIGE_PORT_ETHERNET_CLOUD_LINK.CLOUD_ID,
    GIGE_PORT_ETHERNET_CLOUD_LINK.TRUSTED,
    GIGE_PORT_ETHERNET_CLOUD_LINK.CREATION_TIME,
    GIGE_PORT_ETHERNET_CLOUD_LINK.MISSING,
    GIGE_PORT_ETHERNET_CLOUD_LINK.MISSING_TIME,
    GIGE_PORT.SWITCH_PORT_ID,
    GIGE_PORT.PORT_TYPE,
    SWITCH_PORT.VIRTUAL_SWITCH_ID,
    SWITCH_PORT.USER_PORT_NUMBER,
    VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID
from
    GIGE_PORT_ETHERNET_CLOUD_LINK,
    GIGE_PORT,
    SWITCH_PORT,
    VIRTUAL_SWITCH
where
    GIGE_PORT_ETHERNET_CLOUD_LINK.SWITCH_PORT_ID = GIGE_PORT.ID and
    GIGE_PORT.SWITCH_PORT_ID = SWITCH_PORT.ID and
    SWITCH_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID;
```

GIGE_PORT_INFO

```
create or replace view GIGE_PORT_INFO as
select
    GIGE_PORT.ID,
    GIGE_PORT.SWITCH_PORT_ID,
    GIGE_PORT.PORT_NUMBER,
    GIGE_PORT.SLOT_NUMBER,
    GIGE_PORT.ENABLED,
    GIGE_PORT.SPEED,
    GIGE_PORT.MAX_SPEED,
    GIGE_PORT.MAC_ADDRESS,
    GIGE_PORT.PORT_NAME,
    GIGE_PORT.OPERATIONAL_STATUS,
    GIGE_PORT.LED_STATE,
    GIGE_PORT.SPEED_LED_STATE,
    GIGE_PORT.PORT_TYPE,
    GIGE_PORT.PERSISTENTLY_DISABLED,
    GIGE_PORT.INTERFACE_TYPE,
    GIGE_PORT.CHECKSUM,
    GIGE_PORT.FCIP_CAPABLE,
    coalesce(CARD.FCIP_CIRCUIT_CAPABLE, VIRTUAL_SWITCH.FCIP_CIRCUIT_CAPABLE) as
FCIP_CIRCUIT_CAPABLE,
    GIGE_PORT.ISCSI_CAPABLE,
    GIGE_PORT.REMOTE_MAC_ADDRESS,
    GIGE_PORT.INBAND_MANAGEMENT_STATUS,
    GIGE_PORT.LAST_UPDATE,
    SWITCH_PORT.VIRTUAL_SWITCH_ID,
    SWITCH_PORT.USER_PORT_NUMBER,
    SWITCH_PORT.PORT_INDEX,
    SWITCH_PORT.SPEED_TYPE,
    VIRTUAL_SWITCH.WWN as VIRTUAL_SWITCH_WWN,
    VIRTUAL_SWITCH.MANAGEMENT_STATE,
    VIRTUAL_SWITCH.MONITORED,
    CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN
from
    GIGE_PORT,
    SWITCH_PORT,
    CORE_SWITCH
        left outer join CARD on CORE_SWITCH.ID = CARD.CORE_SWITCH_ID,
    VIRTUAL_SWITCH
where
    GIGE_PORT.SWITCH_PORT_ID = SWITCH_PORT.ID and
    SWITCH_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID and
    VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID and
    GIGE_PORT.SLOT_NUMBER in (0, CARD.SLOT_NUMBER);
```

HBA_PORT_DETAILS_INFO

```
create or replace view HBA_PORT_DETAILS_INFO as
select
    HBA_PORT.DEVICE_PORT_ID,
    HBA_PORT.CONFIGURED_STATE,
    HBA_PORT.CONFIGURED_SPEED,
    HBA_PORT.CONFIGURED_TOPOLOGY,
    HBA_PORT.MAX_SPEED_SUPPORTED,
    HBA_PORT.OPERATING_STATE,
    HBA_PORT.OPERATING_TOPOLOGY,
```

```
HBA_PORT.SUPPORTED_FC4_TYPES,
HBA_PORT.SUPPORTED_COS,
HBA_PORT.TRUSTED as HBA_PORT_TRUSTED,
HBA_PORT.CREATION_TIME as HBA_PORT_CREATION_TIME,
HBA_PORT.MISSING as HBA_PORT_MISSING,
HBA_PORT.MISSING_TIME as HBA_PORT_MISSING_TIME,
HBA_PORT.OPERATING_SPEED,
HBA_PORT.CNA_PORT_ID,
HBA_PORT.PORT_NWWN,
HBA_PORT.PHYSICAL_PORT_WWN,
HBA_PORT.SWITCH_IP,
HBA_PORT.PRINCIPAL_SWITCH_WWN,
HBA_PORT.HBA_ID,
HBA_PORT.PORT_NUMBER,
HBA_PORT.NAME,
HBA_PORT.FACTORY_PORT_WWN,
HBA_PORT.FACTORY_NODE_WWN,
HBA_PORT.PREBOOT_CREATED,
HBA_PORT.MAX_BANDWIDTH,
HBA_PORT.PCIF_INDEX,
HBA_PORT.MAX_PCIF,
HBA_PORT_DETAIL.PERSISTENT_BINDING,
HBA_PORT_DETAIL.FABRIC_NAME,
HBA_PORT_DETAIL.BOOT_OVER_SAN,
HBA_PORT_DETAIL.BOOT_OPTION,
HBA_PORT_DETAIL.BOOT_SPEED,
HBA_PORT_DETAIL.BOOT_TOPOLOGY,
HBA_PORT_DETAIL.BB_CREDIT,
HBA_PORT_DETAIL.FRAME_DATA_FIELD_SIZE,
HBA_PORT_DETAIL.HARDWARE_PATH,
HBA_PORT_DETAIL.V_PORT_COUNT,
HBA_PORT_DETAIL.QUEUE_DEPTH,
HBA_PORT_DETAIL.INTERRUPT_CONTROL_COALESCE,
HBA_PORT_DETAIL.INTERRUPT_CONTROL_LATENCY,
HBA_PORT_DETAIL.INTERRUPT_CONTROL_DELAY,
HBA_PORT_DETAIL.BEACON_STATE,
HBA_PORT_DETAIL.LINK_BEACON_STATE,
HBA_PORT_DETAIL.MPIO_MODE_STATE,
HBA_PORT_DETAIL.PATH_TIME_OUT,
HBA_PORT_DETAIL.LOGGING_LEVEL,
HBA_PORT_DETAIL.TARGET_RATE_LIMIT,
HBA_PORT_DETAIL.DEFAULT_RATE_LIMIT,
HBA_PORT_DETAIL.VF_MODE,
HBA_PORT_DETAIL.RECIEVE_BUFFER_CREDIT,
HBA_PORT_DETAIL.TRANSMIT_BUFFER_CREDIT,
HBA_PORT_DETAIL.FCSP_AUTH_STATE,
HBA_PORT_DETAIL.FCSP_STATUS,
HBA_PORT_DETAIL.FCSP_ALGORITHM,
HBA_PORT_DETAIL.FCSP_GROUP,
HBA_PORT_DETAIL.FCSP_ERROR_STATUS,
HBA_PORT_DETAIL.QOS_CONFIGURED_STATE,
HBA_PORT_DETAIL.QOS_OPERATING_STATE,
HBA_PORT_DETAIL.QOS_TOTAL_BB_CREDIT,
HBA_PORT_DETAIL.QOS_PRIORITY_LEVEL,
HBA_PORT_DETAIL.QOS_HIGH_BW_ALLOCATION,
HBA_PORT_DETAIL.QOS_MEDIUM_BW_ALLOCATION,
HBA_PORT_DETAIL.QOS_LOW_BW_ALLOCATION,
HBA_PORT_DETAIL.MEDIA as MEDIA,
HBA_PORT_DETAIL.IOC_ID as IOC_ID,
HBA_PORT_DETAIL.PREBOOT_DISABLED,
```

```
    HBA_PORT_FCOE_DETAILS.BANDWIDTH as FCOE_BANDWIDTH,
    HBA_PORT_FCOE_DETAILS.FIP_STATE,
    HBA_PORT_FCOE_DETAILS.DISCOVERY_PRIORITY,
    HBA_PORT_FCOE_DETAILS.FCF_FCMAP,
    HBA_PORT_FCOE_DETAILS.FCF_FPMA_MAC,
    HBA_PORT_FCOE_DETAILS.FCF_MAC,
    HBA_PORT_FCOE_DETAILS.FCF_MODE,
    HBA_PORT_FCOE_DETAILS.FCF_NAMEID,
    HBA_PORT_FCOE_DETAILS.FCPIM_MPIO_MODE,
    HBA_PORT_FCOE_DETAILS.PORT_LOG_ENABLED,
    HBA_PORT_FCOE_DETAILS.MAX_FRAME_SIZE as FCOE_MAX_FRAME_SIZE,
    HBA_PORT_FCOE_DETAILS.MTU as FCOE_MTU,
    HBA_PORT_FCOE_DETAILS.PATH_TOV as FCOE_PATH_TOV,
    HBA_PORT_FCOE_DETAILS.SCSI_QUEUE_DEPTH as FCOE_SCSI_QUEUE_DEPTH,
    HBA_PORT_FCOE_DETAILS.STATE as FCOE_STATE,
    HBA_PORT_FCOE_DETAILS.SUPPORTED_CLASS as FCOE_SUPPORTED_CLASS,
    HBA_PORT_FCOE_DETAILS.TRL_SPEED as FCOE_TRL_SPEED,
    HBA_PORT_FCOE_DETAILS.TRL_STATE as FCOE_TRL_STATE,
    HBA_PORT_FCOE_DETAILS.PG_ID as FCOE_PG_ID,
    HBA_PORT_FCOE_DETAILS.PRIORITIES as FCOE_PRIORITIES,
    HBA_PORT_FCOE_DETAILS.FCOE_MAC,
    HBA_PORT.SYNTHETIC_FC,
    HBA_PORT_DETAIL.ALARM_WARNING,
    HBA_PORT_DETAIL.IO_EXEC_THROTTLE_MAX,
    HBA_PORT_DETAIL.IO_EXEC_THROTTLE_OPERATIONAL,
    HBA_PORT_DETAIL.IO_EXEC_THROTTLE_CONFIGURED,
    HBA_PORT_DETAIL.BOOTUP_DELAY,
    HBA_PORT_DETAIL.FEC_STATE,
    HBA_PORT_DETAIL.BB_CREDIT_RECOVERY_STATUS,
    HBA_PORT_DETAIL.CONFIGURED_BB_SCN_COUNT,
    HBA_PORT_DETAIL.NEGOTIATED_BB_SCN_COUNT
from
    HBA_PORT
        left outer join HBA_PORT_DETAIL
            on HBA_PORT.DEVICE_PORT_ID = HBA_PORT_DETAIL.DEVICE_PORT_ID
        left outer join HBA_PORT_FCOE_DETAILS
            on HBA_PORT.DEVICE_PORT_ID = HBA_PORT_FCOE_DETAILS.DEVICE_PORT_ID;
```

HBA_TARGET_INFO

```
create or replace view HBA_TARGET_INFO as
select
    HBA_TARGET.DEVICE_PORT_ID,
    HBA_TARGET.HBA_REMOTE_PORT_LUN_ID,
    HBA_TARGET.BOOT_LUN,
    HBA_TARGET.TRUSTED,
    HBA_TARGET.CREATION_TIME,
    HBA_TARGET.MISSING,
    HBA_TARGET.MISSING_TIME,
    HBA_TARGET.TARGET_ID as HBA_PORT_TARGET_ID,
    HBA_REMOTE_PORT.ID as HBA_REMOTE_PORT_ID,
    HBA_REMOTE_PORT.SYMBOLIC_NAME,
    HBA_REMOTE_PORT.PORT_WWN,
    HBA_REMOTE_PORT.NODE_WWN,
    HBA_REMOTE_PORT.NAME,
    HBA_REMOTE_PORT.FC_ADDRESS,
    HBA_REMOTE_PORT.FRAME_DATA_SIZE,
    HBA_REMOTE_PORT.SPEED,
    HBA_REMOTE_PORT.STATE,
```

```
    HBA_REMOTE_PORT.SUPPORTED_COS,
    HBA_REMOTE_PORT.DEVICE_TYPE,
    HBA_REMOTE_PORT.BIND_TYPE,
    HBA_REMOTE_PORT.TARGET_ID,
    HBA_REMOTE_PORT.ROLE,
    HBA_REMOTE_PORT.VENDOR,
    HBA_REMOTE_PORT.PRODUCT_ID,
    HBA_REMOTE_PORT.PRODUCT_VERSION,
    HBA_REMOTE_PORT.QOS_PRIORITY,
    HBA_REMOTE_PORT.QOS_FLOW_ID,
    HBA_REMOTE_PORT.CURRENT_SPEED,
    HBA_REMOTE_PORT.TRL_ENFORCED,
    HBA_REMOTE_PORT.BUS_NO,
    HBA_REMOTE_PORT_LUN.FCP_LUN,
    HBA_REMOTE_PORT_LUN.CAPACITY,
    HBA_REMOTE_PORT_LUN.BLOCK_SIZE,
    HBA_REMOTE_PORT_LUN.VENDOR as LUN_VENDOR,
    HBA_REMOTE_PORT_LUN.PRODUCT_ID as LUN_PRODUCT_ID,
    HBA_REMOTE_PORT_LUN.PRODUCT_VERSION as LUN_PRODUCT_VERSION,
    HBA_REMOTE_PORT_LUN.PRODUCT_SERIAL_NO,
    HBA_REMOTE_PORT_LUN.TARGET_WWN,
    HBA_REMOTE_PORT_LUN.PHYSICAL_LUN,
    HBA_REMOTE_PORT_LUN.LUN_ID,
    HBA_REMOTE_PORT.FCP_IM_STATE,
    HBA_REMOTE_PORT.IO_LATENCY_MIN,
    HBA_REMOTE_PORT.IO_LATENCY_MAX,
    HBA_REMOTE_PORT.IO_LATENCY_AVERAGE,
    HBA_REMOTE_PORT.DATA_RETRANSMISSION_SUPPORT,
    HBA_REMOTE_PORT.REC_SUPPORT,
    HBA_REMOTE_PORT.TASK_RENTRY_IDENT_SUPPORT,
    HBA_REMOTE_PORT.CONFIRMED_COMPLETIONS_SUPPORT
from
    HBA_TARGET, HBA_REMOTE_PORT, HBA_REMOTE_PORT_LUN
where
    HBA_TARGET.HBA_REMOTE_PORT_LUN_ID = HBA_REMOTE_PORT_LUN.ID and
    HBA_REMOTE_PORT.ID = HBA_REMOTE_PORT_LUN.HBA_REMOTE_PORT_ID;
```

HEALTH_STATUS_INFO

```
create or replace view HEALTH_STATUS_INFO as
select
    DEPLOYMENT_CONFIGURATION.ID as CONFIGURATION_ID,
    DEPLOYMENT_CONFIGURATION.NAME,
    DEPLOYMENT_STATUS.ID as STATUS_ID,
    DEPLOYMENT_STATUS.DEPLOYMENT_TIME,
    DEPLOYMENT_STATUS.DEPLOYED_BY,
    HEALTH_STATUS.RULE_ID,
    HEALTH_STATUS.RULE_DESCRIPTION,
    HEALTH_TARGET_STATUS.TARGET_ID,
    HEALTH_TARGET_STATUS.TARGET_TYPE,
    HEALTH_TARGET_STATUS.STATUS,
    HEALTH_TARGET_STATUS.MESSAGE,
    HEALTH_TARGET_STATUS.LEGACY_NAME
from
    DEPLOYMENT_CONFIGURATION,
    DEPLOYMENT_STATUS,
    HEALTH_STATUS,
    HEALTH_TARGET_STATUS
where
```

```
    DEPLOYMENT_STATUS.DEPLOYMENT_CONFIGURATION_ID = DEPLOYMENT_CONFIGURATION.ID
    and HEALTH_STATUS.DEPLOYMENT_STATUS_ID = DEPLOYMENT_STATUS.ID
    and HEALTH_TARGET_STATUS.HEALTH_STATUS_ID = HEALTH_STATUS.ID;
```

HOST_DISCOVERY_REQUEST_INFO

```
create or replace view HOST_DISCOVERY_REQUEST_INFO as
select
    HOST_DISCOVERY_REQUEST.ID,
    HOST_DISCOVERY_REQUEST.HOST_NAME AS REQUEST_HOST_NAME,
    HOST_DISCOVERY_REQUEST.DEVICE_ENCLOSURE_ID,
    HOST_DISCOVERY_REQUEST.REQUEST_GROUP_ID,
    HOST_DISCOVERY_REQUEST.HOST_DISCOVERY_OPTION_ID,
    HOST_DISCOVERY_REQUEST.VM_MANAGEMENT_STATE,
    HOST_DISCOVERY_REQUEST.JSON_MANAGEMENT_STATE,
    HOST_DISCOVERY_REQUEST.CIM_MANAGEMENT_STATE,
    HOST_DISCOVERY_REQUEST.MANAGEMENT_STATE,
    HOST_DISCOVERY_OPTION.DISCOVER_JSON,
    HOST_DISCOVERY_OPTION.JSON_USERNAME,
    HOST_DISCOVERY_OPTION.JSON_PASSWD,
    HOST_DISCOVERY_OPTION.DISCOVER_CIM,
    HOST_DISCOVERY_OPTION.CIM_IMPL,
    HOST_DISCOVERY_OPTION.CIM_USERNAME,
    HOST_DISCOVERY_OPTION.CIM_PASSWORD,
    HOST_DISCOVERY_OPTION.CIM_NAMESPACE,
    HOST_DISCOVERY_OPTION.CIM_PORT,
    HOST_DISCOVERY_OPTION.DISCOVER_VM,
    HOST_DISCOVERY_OPTION.VM_USERNAME,
    HOST_DISCOVERY_OPTION.VM_PASSWORD,
    HOST_DISCOVERY_OPTION.JSON_PORT,
    HOST_DISCOVERY_OPTION.VM_PORT,
    HOST_DISCOVERY_OPTION.Application_Name_USER_NAME,
    HOST_DISCOVERY_OPTION.Application_Name_SERVER_ADDRESS,
    DEVICE_ENCLOSURE.NAME,
    DEVICE_ENCLOSURE.TYPE,
    DEVICE_ENCLOSURE.ICON,
    DEVICE_ENCLOSURE.OS,
    DEVICE_ENCLOSURE.APPLICATIONS,
    DEVICE_ENCLOSURE.DEPARTMENT,
    DEVICE_ENCLOSURE.CONTACT,
    DEVICE_ENCLOSURE.LOCATION,
    DEVICE_ENCLOSURE.DESCRIPTION,
    DEVICE_ENCLOSURE.COMMENT_,
    DEVICE_ENCLOSURE.IP_ADDRESS,
    DEVICE_ENCLOSURE.VENDOR,
    DEVICE_ENCLOSURE.MODEL,
    DEVICE_ENCLOSURE.SERIAL_NUMBER,
    DEVICE_ENCLOSURE.FIRMWARE,
    DEVICE_ENCLOSURE.USER_DEFINED_VALUE1,
    DEVICE_ENCLOSURE.USER_DEFINED_VALUE2,
    DEVICE_ENCLOSURE.USER_DEFINED_VALUE3,
    DEVICE_ENCLOSURE.HCM_AGENT_VERSION,
    DEVICE_ENCLOSURE.OS_VERSION,
    DEVICE_ENCLOSURE.CREATED_BY,
    DEVICE_ENCLOSURE.TRACK_CHANGES,
    DEVICE_ENCLOSURE.LAST_UPDATE_TIME,
    DEVICE_ENCLOSURE.LAST_UPDATE_MODULE,
    DEVICE_ENCLOSURE.TRUSTED,
    DEVICE_ENCLOSURE.CREATION_TIME,
```

```
    DEVICE_ENCLOSURE.MISSING,
    DEVICE_ENCLOSURE.MISSING_TIME,
    DEVICE_ENCLOSURE.HOST_NAME,
    DEVICE_ENCLOSURE.SYSLOG_REGISTERED,
    DEVICE_ENCLOSURE.VIRTUALIZATION,
    DEVICE_ENCLOSURE.MANAGED_ELEMENT_ID,
    HOST_DISCOVERY_REQUEST.MANAGEMENT_STATE_DETAILS
from
    HOST_DISCOVERY_REQUEST
        join HOST_DISCOVERY_OPTION on
HOST_DISCOVERY_REQUEST.HOST_DISCOVERY_OPTION_ID = HOST_DISCOVERY_OPTION.ID
        left outer join DEVICE_ENCLOSURE on
HOST_DISCOVERY_REQUEST.DEVICE_ENCLOSURE_ID = DEVICE_ENCLOSURE.ID;
```

IFL_INFO

```
create or replace view IFL_INFO as
select
    IFL.ID as IFL_ID,
    IFL.EDGE_FABRIC_ID,
    (select distinct FCR_PORT.VIRTUAL_SWITCH_ID
        from SWITCH_PORT FCR_PORT
        where FCR_PORT.WWN = IFL.BB_PORT_WWN)
        as FCR_SWITCH_ID,
    IFL.EDGE_PORT_WWN,
    IFL.BB_FABRIC_ID,
    IFL.BB_PORT_WWN ,
    IFL.BB_RA_TOV,
    IFL.BB_ED_TOV,
    IFL.BB_PID_FORMAT,
    SWITCH_PORT.VIRTUAL_SWITCH_ID as EDGE_SWITCH_ID,
    SWITCH_PORT.ID as EDGE_PORT_ID,
    SWITCH_PORT.USER_PORT_NUMBER as EDGE_PORT_NUMBER,
    SWITCH_PORT.TYPE as EDGE_PORT_TYPE
from IFL
    left outer join SWITCH_PORT
        on IFL.EDGE_PORT_WWN = SWITCH_PORT.WWN;
```

ISL_INFO

```
create or replace view ISL_INFO as
select distinct
    ISL.ID,
    ISL.FABRIC_ID,
    ISL.COST,
    ISL.TYPE,
    ISL.SOURCE_DOMAIN_ID,
    ISL.SOURCE_PORT_NUMBER,
    ISL.MISSING,
    SOURCE_VIRTUAL_SWITCH.ID as SOURCE_SWITCH_ID,
    SOURCE_VIRTUAL_SWITCH.NAME as SOURCE_SWITCH_NAME,
    SOURCE_VIRTUAL_SWITCH.WWN as SOURCE_SWITCH_WWN,
    SOURCE_VIRTUAL_SWITCH.CORE_SWITCH_ID as SOURCE_CORE_SWITCH_ID,
    SOURCE_VIRTUAL_SWITCH.BASE_SWITCH as SOURCE_BASE_SWITCH,
    SOURCE_VIRTUAL_SWITCH.MANAGEMENT_STATE as
SOURCE_VIRTUAL_SWITCH_MANAGEMENT_STATE,
    SOURCE_VIRTUAL_SWITCH.MONITORED as SOURCE_VIRTUAL_SWITCH_MONITORED,
    SOURCE_SWITCH_PORT.ID as SOURCE_SWITCH_PORT_ID,
```

```
    SOURCE_SWITCH_PORT.WWN as SOURCE_SWITCH_PORT_WWN,
    SOURCE_SWITCH_PORT.NAME as SOURCE_SWITCH_PORT_NAME,
     SOURCE_SWITCH_PORT.TYPE as PORT_TYPE,
     SOURCE_SWITCH_PORT.KIND as SOURCE_SWITCH_PORT_KIND,
     SOURCE_SWITCH_PORT.PHYSICAL_PORT as SOURCE_PHYSICAL_PORT,
     SOURCE_SWITCH_PORT.TRUNKED as SOURCE_SWITCH_PORT_TRUNKED,
     ISL.DEST_DOMAIN_ID,
    ISL.DEST_PORT_NUMBER,
    DEST_VIRTUAL_SWITCH.ID as DEST_SWITCH_ID,
    DEST_VIRTUAL_SWITCH.NAME as DEST_SWITCH_NAME,
     DEST_VIRTUAL_SWITCH.WWN as DEST_SWITCH_WWN,
     DEST_VIRTUAL_SWITCH.CORE_SWITCH_ID as DEST_CORE_SWITCH_ID,
     DEST_VIRTUAL_SWITCH.BASE_SWITCH as DEST_BASE_SWITCH,
     DEST_VIRTUAL_SWITCH.MANAGEMENT_STATE as DEST_VIRTUAL_SWITCH_MANAGEMENT_STATE,
     DEST_VIRTUAL_SWITCH.MONITORED as DEST_VIRTUAL_SWITCH_MONITORED,
    DEST_SWITCH_PORT.ID as DEST_SWITCH_PORT_ID,
    DEST_SWITCH_PORT.WWN as DEST_SWITCH_PORT_WWN,
     DEST_SWITCH_PORT.NAME as DEST_SWITCH_PORT_NAME,
     DEST_SWITCH_PORT.KIND as DEST_SWITCH_PORT_KIND,
     DEST_SWITCH_PORT.PHYSICAL_PORT as DEST_PHYSICAL_PORT,
     DEST_SWITCH_PORT.TRUNKED as DEST_SWITCH_PORT_TRUNKED,
     FABRIC.PRINCIPAL_SWITCH_WWN as PRINCIPAL_SWITCH_WWN
from
    ISL,
     FABRIC_MEMBER SOURCE_FABRIC_MEMBER,
     VIRTUAL_SWITCH          SOURCE_VIRTUAL_SWITCH,
     SWITCH_PORT   SOURCE_SWITCH_PORT,
     FABRIC_MEMBER DEST_FABRIC_MEMBER,
     VIRTUAL_SWITCH          DEST_VIRTUAL_SWITCH,
     SWITCH_PORT   DEST_SWITCH_PORT,
     FABRIC
where
    SOURCE_FABRIC_MEMBER.FABRIC_ID = ISL.FABRIC_ID and
    SOURCE_VIRTUAL_SWITCH.ID = SOURCE_FABRIC_MEMBER.VIRTUAL_SWITCH_ID and
    SOURCE_VIRTUAL_SWITCH.DOMAIN_ID = ISL.SOURCE_DOMAIN_ID and
    SOURCE_SWITCH_PORT.VIRTUAL_SWITCH_ID = SOURCE_VIRTUAL_SWITCH.ID and
     SOURCE_SWITCH_PORT.CATEGORY = 1 and
    SOURCE_SWITCH_PORT.USER_PORT_NUMBER = ISL.SOURCE_PORT_NUMBER and
    DEST_FABRIC_MEMBER.FABRIC_ID = ISL.FABRIC_ID and
    DEST_VIRTUAL_SWITCH.ID = DEST_FABRIC_MEMBER.VIRTUAL_SWITCH_ID and
    DEST_VIRTUAL_SWITCH.DOMAIN_ID = ISL.DEST_DOMAIN_ID and
    DEST_SWITCH_PORT.VIRTUAL_SWITCH_ID = DEST_VIRTUAL_SWITCH.ID and
     DEST_SWITCH_PORT.CATEGORY = 1 and
    DEST_SWITCH_PORT.USER_PORT_NUMBER = ISL.DEST_PORT_NUMBER and
     FABRIC.ID = ISL.FABRIC_ID;
```

ISL_TRILL_INFO

```
create or replace view ISL_TRILL_INFO as
select distinct
    VCS_DEVICE.DEVICE_ID as VCS_DEVICE_ID,
    SOURCE_CLUSTER_MEMBER.CLUSTER_ME_ID,
    ISL.ID,
    ISL.FABRIC_ID,
    ISL.COST,
    ISL.MISSING,
    ISL.SOURCE_DOMAIN_ID,
    ISL.SOURCE_PORT_NUMBER,
    SOURCE_DEVICE.MANAGED_ELEMENT_ID as SOURCE_ME_ID,
```

```
    SOURCE_DEVICE.DEVICE_ID as SOURCE_DEVICE_ID,
    SOURCE_DEVICE.SYS_NAME as SOURCE_DEVICE_NAME,
    SOURCE_SWITCH_PORT.ID as SOURCE_SWITCH_PORT_ID,
    SOURCE_SWITCH_PORT.NAME as SOURCE_SWITCH_PORT_NAME,
    SOURCE_SWITCH_PORT.IDENTIFIER as SOURCE_SWITCH_PORT_IDENTIFIER,
    SOURCE_SWITCH_PORT.TYPE as PORT_TYPE,
    SOURCE_SWITCH_PORT.KIND as SOURCE_SWITCH_PORT_KIND,
    SOURCE_SWITCH_PORT.PHYSICAL_PORT as SOURCE_PHYSICAL_PORT,
    SOURCE_SWITCH_PORT.TRUNKED as SOURCE_SWITCH_PORT_TRUNKED,
    ISL.DEST_DOMAIN_ID,
    ISL.DEST_PORT_NUMBER,
    DEST_DEVICE.DEVICE_ID as DEST_DEVICE_ID,
    DEST_DEVICE.MANAGED_ELEMENT_ID AS DEST_ME_ID,
    DEST_DEVICE.SYS_NAME as DEST_DEVICE_NAME,
    DEST_SWITCH_PORT.ID as DEST_SWITCH_PORT_ID,
    DEST_SWITCH_PORT.NAME as DEST_SWITCH_PORT_NAME,
    DEST_SWITCH_PORT.IDENTIFIER as DEST_SWITCH_PORT_IDENTIFIER,
    DEST_SWITCH_PORT.KIND as DEST_SWITCH_PORT_KIND,
    DEST_SWITCH_PORT.PHYSICAL_PORT as DEST_PHYSICAL_PORT,
    DEST_SWITCH_PORT.TRUNKED as DEST_SWITCH_PORT_TRUNKED

from
    ISL,
    DEVICE VCS_DEVICE,
    VCS_CLUSTER_MEMBER SOURCE_CLUSTER_MEMBER,
    VCS_CLUSTER_MEMBER DEST_CLUSTER_MEMBER,
    DEVICE SOURCE_DEVICE,
    SWITCH_PORT SOURCE_SWITCH_PORT,
    FABRIC_MEMBER SOURCE_FABRIC_MEMBER,
    VIRTUAL_SWITCH SOURCE_VIRTUAL_SWITCH,
    DEVICE DEST_DEVICE,
    SWITCH_PORT DEST_SWITCH_PORT,
    FABRIC_MEMBER DEST_FABRIC_MEMBER,
    VIRTUAL_SWITCH DEST_VIRTUAL_SWITCH,
    FABRIC

where
    SOURCE_FABRIC_MEMBER.FABRIC_ID = ISL.FABRIC_ID and
    SOURCE_VIRTUAL_SWITCH.ID = SOURCE_FABRIC_MEMBER.VIRTUAL_SWITCH_ID and
    SOURCE_VIRTUAL_SWITCH.DOMAIN_ID = ISL.SOURCE_DOMAIN_ID and
    SOURCE_SWITCH_PORT.VIRTUAL_SWITCH_ID = SOURCE_VIRTUAL_SWITCH.ID and
    SOURCE_SWITCH_PORT.USER_PORT_NUMBER = ISL.SOURCE_PORT_NUMBER and
    DEST_FABRIC_MEMBER.FABRIC_ID = ISL.FABRIC_ID and
    DEST_VIRTUAL_SWITCH.ID = DEST_FABRIC_MEMBER.VIRTUAL_SWITCH_ID and
    DEST_VIRTUAL_SWITCH.DOMAIN_ID = ISL.DEST_DOMAIN_ID and
    DEST_SWITCH_PORT.VIRTUAL_SWITCH_ID = DEST_VIRTUAL_SWITCH.ID and
    DEST_SWITCH_PORT.USER_PORT_NUMBER = ISL.DEST_PORT_NUMBER and
    FABRIC.ID = ISL.FABRIC_ID and
    SOURCE_VIRTUAL_SWITCH.MANAGED_ELEMENT_ID = SOURCE_DEVICE.MANAGED_ELEMENT_ID
and
    DEST_VIRTUAL_SWITCH.MANAGED_ELEMENT_ID = DEST_DEVICE.MANAGED_ELEMENT_ID and
    SOURCE_CLUSTER_MEMBER.MEMBER_ME_ID = SOURCE_DEVICE.MANAGED_ELEMENT_ID and
    DEST_CLUSTER_MEMBER.MEMBER_ME_ID = DEST_DEVICE.MANAGED_ELEMENT_ID and
    VCS_DEVICE.MANAGED_ELEMENT_ID = SOURCE_CLUSTER_MEMBER.CLUSTER_ME_ID;
```

ISL_TRUNK_GROUP_MEMBER_INFO

```
CREATE VIEW isl_trunk_group_member_info AS
   select
```

```
    ISL_TRUNK_GROUP.ID,
    ISL_TRUNK_GROUP.VIRTUAL_SWITCH_ID,
    ISL_TRUNK_GROUP.MASTER_USER_PORT,
    ISL_TRUNK_MEMBER.MISSING,
    ISL_TRUNK_MEMBER.TRUSTED,
    ISL_TRUNK_MEMBER.MISSING_TIME,
    ISL_TRUNK_MEMBER.PORT_NUMBER,
    SWITCH_PORT.WWN,
    SWITCH_PORT.TYPE,
    SWITCH_PORT.STATUS,
    SWITCH_PORT.SPEED,
    SWITCH_PORT.ID as SWITCH_PORT_ID,
    SWITCH_PORT.SPEED_TYPE
from
    ISL_TRUNK_GROUP,
    ISL_TRUNK_MEMBER,
    SWITCH_PORT
where
    ISL_TRUNK_GROUP.id = ISL_TRUNK_MEMBER.GROUP_ID
    and ISL_TRUNK_GROUP.VIRTUAL_SWITCH_ID = SWITCH_PORT.VIRTUAL_SWITCH_ID
    and ISL_TRUNK_MEMBER.PORT_NUMBER= SWITCH_PORT.USER_PORT_NUMBER;
```

ISL_TRUNK_INFO

```
CREATE VIEW isl_trunk_info AS
    select
   ISL_TRUNK_GROUP.ID,
   ISL_TRUNK_GROUP.TRUSTED,
   ISL_TRUNK_GROUP.MISSING,
   ISL_TRUNK_GROUP.MISSING_TIME,
   ISL_TRUNK_GROUP.MEMBER_TRACKING_STATUS,
   ISL_INFO.COST,
   ISL_INFO.TYPE,
   ISL_INFO.SOURCE_PORT_NUMBER,
   ISL_INFO.SOURCE_SWITCH_ID,
   ISL_INFO.MISSING_REASON,
   SOURCE_CORE_SWITCH.IP_ADDRESS as SOURCE_SWITCH_IP_ADDRESS,
   SOURCE_VIRTUAL_SWITCH.WWN as SOURCE_SWITCH_WWN,
   SOURCE_VIRTUAL_SWITCH.MANAGEMENT_STATE as SOURCE_SWITCH_MANAGEMENT_STATE,
   SOURCE_VIRTUAL_SWITCH.MONITORED as SOURCE_SWITCH_MONITORED,
   ISL_INFO.SOURCE_DOMAIN_ID as MASTER_PORT,
   ISL_INFO.SOURCE_SWITCH_NAME,
   ISL_INFO.SOURCE_SWITCH_PORT_ID,
   ISL_INFO.DEST_PORT_NUMBER,
   ISL_INFO.DEST_SWITCH_ID,
   DEST_CORE_SWITCH.IP_ADDRESS as DEST_SWITCH_IP_ADDRESS,
   DEST_VIRTUAL_SWITCH.WWN as DEST_SWITCH_WWN,
   DEST_VIRTUAL_SWITCH.MANAGEMENT_STATE as DEST_SWITCH_MANAGEMENT_STATE,
   DEST_VIRTUAL_SWITCH.MONITORED as DEST_SWITCH_MONITORED,
   ISL_INFO.SOURCE_SWITCH_PORT_WWN,
   ISL_INFO.DEST_DOMAIN_ID as REMOTE_MASTER_PORT,
   ISL_INFO.DEST_SWITCH_NAME,
   ISL_INFO.DEST_SWITCH_PORT_ID

from
   ISL_TRUNK_GROUP,
   ISL_INFO,
   CORE_SWITCH SOURCE_CORE_SWITCH,
   CORE_SWITCH DEST_CORE_SWITCH,
```

```
   VIRTUAL_SWITCH SOURCE_VIRTUAL_SWITCH,
   VIRTUAL_SWITCH DEST_VIRTUAL_SWITCH
where
   ISL_INFO.SOURCE_SWITCH_ID = ISL_TRUNK_GROUP.VIRTUAL_SWITCH_ID
   and ISL_INFO.SOURCE_PORT_NUMBER = ISL_TRUNK_GROUP.MASTER_USER_PORT
   and ISL_INFO.SOURCE_SWITCH_ID = SOURCE_VIRTUAL_SWITCH.ID
   and SOURCE_VIRTUAL_SWITCH.CORE_SWITCH_ID = SOURCE_CORE_SWITCH.ID
   and ISL_INFO.DEST_SWITCH_ID = DEST_VIRTUAL_SWITCH.ID
   and DEST_VIRTUAL_SWITCH.CORE_SWITCH_ID = DEST_CORE_SWITCH.ID;
```

L2_NEIGHBOR_INFO

```
create or replace view L2_NEIGHBOR_INFO as
select
   L2_NEIGHBOR.INTERFACE_ID,
   L2_NEIGHBOR.RMT_IP_ADDRESS,
   L2_NEIGHBOR.RMT_IF_NAME,
   LLDP_DATA.DEVICE_ID as RMT_DEVICE_ID,
   LLDP_DATA.INTERFACE_ID as RMT_INTERFACE_ID,
   PHY_INTF.PHYSICAL_ADDRESS as RMT_INTERFACE_MAC,
   RMT_DEVICE.IS_ROUTER
from
   device RMT_DEVICE,
   LLDP_DATA,
   L2_NEIGHBOR,
   physical_interface PHY_INTF
where
   LLDP_DATA.CHASSIS_ID = L2_NEIGHBOR.LLDP_REM_CHASSIS_ID
   and LLDP_DATA.CHASSIS_ID_SUBTYPE = L2_NEIGHBOR.LLDP_REM_CHASSIS_ID_SUBTYPE
   and LLDP_DATA.PORT_ID = L2_NEIGHBOR.LLDP_REM_PORT_ID
   and LLDP_DATA.PORT_ID_SUBTYPE = L2_NEIGHBOR.LLDP_REM_PORT_ID_SUBTYPE
   and LLDP_DATA.DEVICE_ID = RMT_DEVICE.device_id
   and PHY_INTF.interface_id = LLDP_DATA.INTERFACE_ID;
```

MAPS_EVENT_DETAILS_INFO

```
CREATE OR REPLACE VIEW MAPS_EVENT_DETAILS_INFO AS
 SELECT MAPS_EVENT.ID,
    MAPS_EVENT.HOST_TIME,
    MAPS_EVENT.CATEGORY,
    MAPS_EVENT.VIOLATION_TYPE,
    MAPS_EVENT.MANAGED_ELEMENT_ID,
    MAPS_EVENT.ORIGIN_FABRIC_ID,
    MAPS_EVENT.SWITCH_PORT_ID,
    MAPS_EVENT.INTERFACE_ID,
    MAPS_EVENT.FCIP_CIRCUIT_ID,
    MAPS_EVENT.FRU_NAME,
    MAPS_EVENT.VM_ID,
    MAPS_EVENT.FLOW_DEFINITION_ID,
    MAPS_EVENT_DETAILS.SWITCH_TIME,
    MAPS_EVENT_DETAILS.RULE_NAME,
    MAPS_EVENT_DETAILS.RULE_CONDITION,
    MAPS_EVENT_DETAILS.TIME_BASE,
    MAPS_EVENT_DETAILS.ACTIONS,
    MAPS_EVENT_DETAILS.CURRENT_VALUE,
    MAPS_EVENT_DETAILS.SWITCH_ENABLED_ACTIONS,
    VIRTUAL_SWITCH.NAME AS SWITCH_NAME,
    SWITCH_PORT.NAME AS SWITCH_PORT_NAME,
```

```
    INTERFACE.NAME AS INTERFACE_NAME,
    SWITCH_PORT.WWN AS SWITCH_PORT_WWN,
    SWITCH_PORT.SLOT_NUMBER AS SWITCH_PORT_SLOT,
    SWITCH_PORT.PORT_NUMBER AS SWITCH_PORT_NUMBER,
    SWITCH_PORT.PORT_ID AS SWITCH_PORT_PORT_ID,
    FCIP_TUNNEL_CIRCUIT.CIRCUIT_NUMBER,
    FCIP_TUNNEL_CIRCUIT.SLOT_NUMBER AS FCIP_SLOT_NUMBER,
    FCIP_TUNNEL_CIRCUIT.VE_PORT_NUMBER AS FCIP_PORT_NUMBER,
    NP_FLOW_DEFINITION.NAME AS FLOW_NAME,
    MAPS_EVENT_CAUSE_ACTION.ACTION

   FROM MAPS_EVENT_DETAILS

   JOIN MAPS_EVENT ON MAPS_EVENT.ID = MAPS_EVENT_DETAILS.MAPS_EVENT_ID
   LEFT JOIN MAPS_EVENT_CAUSE_ACTION ON MAPS_EVENT.VIOLATION_TYPE =
MAPS_EVENT_CAUSE_ACTION.VIOLATION_TYPE
   LEFT JOIN VIRTUAL_SWITCH ON MAPS_EVENT.MANAGED_ELEMENT_ID =
VIRTUAL_SWITCH.MANAGED_ELEMENT_ID
   LEFT JOIN SWITCH_PORT ON MAPS_EVENT.SWITCH_PORT_ID = SWITCH_PORT.ID
   LEFT JOIN INTERFACE ON MAPS_EVENT.INTERFACE_ID = INTERFACE.INTERFACE_ID
   LEFT JOIN FCIP_TUNNEL_CIRCUIT ON MAPS_EVENT.FCIP_CIRCUIT_ID =
FCIP_TUNNEL_CIRCUIT.ID
   LEFT JOIN NP_FLOW_DEFINITION ON MAPS_EVENT.FLOW_DEFINITION_ID =
NP_FLOW_DEFINITION.ID;
```

MODULE_INFO

```
CREATE VIEW module_info AS
    select distinct
TEMP_MODULE.MODULE_ID,
TEMP_MODULE.NUM_PORTS,
TEMP_MODULE.IS_PRESENT,
case
    when TEMP_MODULE.IS_PRESENT = 1 then 'YES'
    else 'NO'
end as IS_PRESENT_TXT,
TEMP_MODULE.IS_MANAGEMENT_MODULE,
case
    when TEMP_MODULE.IS_MANAGEMENT_MODULE = 1 then 'YES'
    else 'NO'
end as IS_MANAGEMENT_MODULE_TXT,
TEMP_MODULE.NUM_CPUS,
TEMP_MODULE.HW_REVISION,
TEMP_MODULE.SW_REVISION,
TEMP_MODULE.SLOT_NUM,
TEMP_MODULE.DEVICE_ID,
TEMP_MODULE.PHYSICAL_DEVICE_ID,
TEMP_MODULE.UNIT_NUMBER,
TEMP_MODULE.UNIT_PRESENT,
case
    when TEMP_MODULE.UNIT_PRESENT = 1 then 'YES'
    else 'NO'
end as UNIT_PRESENT_TXT,
TEMP_MODULE.MANAGED_ELEMENT_ID,
TEMP_MODULE.IP_ADDRESS,
TEMP_FOUNDRY_MODULE.SERIAL_NUM,
TEMP_FOUNDRY_MODULE.DRAM_SIZE,
TEMP_FOUNDRY_MODULE.BOOT_FLASH_SIZE,
```

```
TEMP_FOUNDRY_MODULE.CODE_FLASH_SIZE,
TEMP_FOUNDRY_MODULE.MODULE_TYPE,
TEMP_MODULE.DESCRIPTION as MODULE_TYPE_TXT,
TEMP_MODULE.MODULE_STATUS,
TEMP_MODULE.REDUNDANT_STATUS
from
    (
    select distinct
    MODULE.MODULE_ID,
    MODULE.NUM_PORTS,
    MODULE.IS_PRESENT,
    MODULE.IS_MANAGEMENT_MODULE,
    MODULE.NUM_CPUS,
    MODULE.HW_REVISION,
    MODULE.SW_REVISION,
    SLOT.SLOT_NUM,
    PHYSICAL_DEVICE.DEVICE_ID,
    PHYSICAL_DEVICE.PHYSICAL_DEVICE_ID,
    PHYSICAL_DEVICE.UNIT_NUMBER,
    PHYSICAL_DEVICE.UNIT_PRESENT,
    DEVICE.MANAGED_ELEMENT_ID,
    DEVICE.IP_ADDRESS,
    MODULE.DESCRIPTION,
     MODULE.MODULE_STATUS,
     MODULE.REDUNDANT_STATUS
    from MODULE, SLOT, MODULE_SLOT_PRESENT, DEVICE, PHYSICAL_DEVICE
    where
    MODULE.MODULE_ID = MODULE_SLOT_PRESENT.MODULE_ID
    and MODULE_SLOT_PRESENT.SLOT_ID = SLOT.SLOT_ID
    and SLOT.PHYSICAL_DEVICE_ID = PHYSICAL_DEVICE.PHYSICAL_DEVICE_ID
    and DEVICE.DEVICE_ID = PHYSICAL_DEVICE.DEVICE_ID
    ) TEMP_MODULE
left join
    (
    select
    FOUNDRY_MODULE.MODULE_ID,
    FOUNDRY_MODULE.SERIAL_NUM,
    FOUNDRY_MODULE.DRAM_SIZE,
    FOUNDRY_MODULE.BOOT_FLASH_SIZE,
    FOUNDRY_MODULE.CODE_FLASH_SIZE,
    FOUNDRY_MODULE.MODULE_TYPE
    from FOUNDRY_MODULE
    ) TEMP_FOUNDRY_MODULE ON TEMP_MODULE.MODULE_ID =
TEMP_FOUNDRY_MODULE.MODULE_ID;
```

NPORT_WWN_MAP_INFO

This view provides a consolidation between Nport WWN map and AG"s N and F ports. It considers only those N-Ports that are currently occupied that is having non-empty remote port wwn. This is required because NPort-WWN mapping might exist for NPorts that are not yet online and if a device is connected to AG through some F-Port that is mapped to some other N-Port that is online then AG will use that mapping.

```
create or replace view NPORT_WWN_MAP_INFO as
select
    NPORT_WWN_MAP.VIRTUAL_SWITCH_ID,
    NPORT_WWN_MAP.N_PORT,
    NPORT_WWN_MAP.DEVICE_PORT_WWN,
```

```
    AG_N_PORT.REMOTE_PORT_WWN as EDGE_SWITCH_PORT_WWN,
    AG_N_PORT.WWN as AG_N_PORT_WWN,
    AG_F_PORT.USER_PORT_NUMBER as F_PORT,
    AG_F_PORT.WWN as AG_F_PORT_WWN,
    AG_F_PORT.REMOTE_NODE_WWN
from
    NPORT_WWN_MAP,
    SWITCH_PORT AG_N_PORT,
    SWITCH_PORT AG_F_PORT,
    VIRTUAL_SWITCH AG_SWITCH
where
    NPORT_WWN_MAP.VIRTUAL_SWITCH_ID = AG_N_PORT.VIRTUAL_SWITCH_ID
    and NPORT_WWN_MAP.N_PORT = AG_N_PORT.USER_PORT_NUMBER
    and NPORT_WWN_MAP.VIRTUAL_SWITCH_ID =  AG_F_PORT.VIRTUAL_SWITCH_ID
    and NPORT_WWN_MAP.DEVICE_PORT_WWN = AG_F_PORT.REMOTE_PORT_WWN
    AND AG_N_PORT.VIRTUAL_SWITCH_ID = AG_SWITCH.ID
    and AG_SWITCH.MONITORED = 1;
```

PHANTOM_PORT_INFO

```
create or replace view PHANTOM_PORT_INFO as
select
    PHANTOM_PORT.ID,
    PHANTOM_PORT.WWN,
    PHANTOM_PORT.VIRTUAL_SWITCH_ID,
    PHANTOM_PORT.PORT_NUMBER,
    PHANTOM_PORT.PORT_ID,
    PHANTOM_PORT.SPEED,
    PHANTOM_PORT.MAX_SPEED,
    PHANTOM_PORT.TYPE,
    PHANTOM_PORT.REMOTE_NODE_WWN,
    PHANTOM_PORT.REMOTE_PORT_WWN,
    PHANTOM_PORT.PHANTOM_TYPE,
    PHANTOM_PORT.BB_FABRIC_ID,
    VIRTUAL_SWITCH.WWN as VIRTUAL_SWITCH_WWN,
    VIRTUAL_SWITCH.MANAGEMENT_STATE,
    VIRTUAL_SWITCH.MONITORED
from
    PHANTOM_PORT,
    VIRTUAL_SWITCH
where
    PHANTOM_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID;
```

PRODUCT_INFO

```
CREATE VIEW product_info AS
    select distinct
TEMP_DEVICE.DEVICE_ID,
TEMP_DEVICE.MANAGED_ELEMENT_ID,
TEMP_DEVICE.ALIAS_NAME,
TEMP_DEVICE.HOST_NAME,
TEMP_DEVICE.OPER_STATUS,
case
    when TEMP_DEVICE.OPER_STATUS = 1 then
    (case
        when TEMP_DEVICE.FABRIC_WATCH_STATUS = 2 then 'DEGRADED'
        when TEMP_DEVICE.FABRIC_WATCH_STATUS = 3 then 'DOWN'
        else 'REACHABLE'
```

```
     end)
    when TEMP_DEVICE.OPER_STATUS = 2 then 'NOT REACHABLE'
    when TEMP_DEVICE.OPER_STATUS = 3 then 'DEGRADED'
    when TEMP_DEVICE.OPER_STATUS = 4 then 'MARGINAL'
    when TEMP_DEVICE.OPER_STATUS = 5 then 'DOWN'
    else 'UNKNOWN'
end as OPER_STATUS_TXT,
TEMP_DEVICE.FABRIC_WATCH_STATUS,
TEMP_DEVICE.FABRIC_WATCH_STATUS_REASON,
TEMP_DEVICE.ADMIN_STATUS,
case
    when TEMP_DEVICE.ADMIN_STATUS = 1 then 'TROUBLESHOOTING'
    else 'NORMAL'
end as ADMIN_STATUS_TXT,
TEMP_DEVICE.ADMIN_STATUS_LAST_UPDATED,
TEMP_DEVICE.MEMO,
TEMP_DEVICE.MEMO_LAST_UPDATED,
TEMP_DEVICE.SYS_OID,
TEMP_DEVICE.RBRIDGE_ID,
TEMP_DEVICE.IP_ADDRESS,
TEMP_FOUNDRY_DEVICE.PRODUCT_TYPE,
case
    when TEMP_DEVICE.IS_ROUTER = 1 then 'ROUTER'
    else 'L2 SWITCH'
end as PRODUCT_TYPE_TXT,
case
    when TEMP_DEVICE.IS_FOUNDRY = 1 then 'IOS'
    when TEMP_DEVICE.IS_DCB_SWITCH = 1 then 'FOS'
    when TEMP_DEVICE.IS_VCS_CAPABLE = 1 then 'NOS'
    else 'UNKNOWN'
end as SWITCH_OS,
TEMP_DEVICE.IS_ROUTER,
TEMP_DEVICE.IS_SLB,
TEMP_DEVICE.SERIAL_NUMBER,
TEMP_DEVICE.SYS_NAME,
case
    when TEMP_DEVICE.SUB_CATEGORY > 0 then (select distinct VCSD.SYS_NAME from
DEVICE as VCSD where VCSD.MANAGED_ELEMENT_ID
    in (select distinct VM.CLUSTER_ME_ID from VCS_CLUSTER_MEMBER as VM where
TEMP_DEVICE.MANAGED_ELEMENT_ID = VM.MEMBER_ME_ID))
    else null
end as VCS_NAME,

case
    when TEMP_DEVICE.SUB_CATEGORY > 0 then (select distinct VCSD.IP_ADDRESS from
DEVICE as VCSD where VCSD.MANAGED_ELEMENT_ID
    in (select distinct VM.CLUSTER_ME_ID from VCS_CLUSTER_MEMBER as VM where
TEMP_DEVICE.MANAGED_ELEMENT_ID = VM.MEMBER_ME_ID))
    else null
end as VCS_IP_ADDRESS,
TEMP_DEVICE.SYS_CONTACT,
TEMP_DEVICE.SYS_LOCATION,
TEMP_DEVICE.DESCRIPTION,
TEMP_DEVICE.LAST_SEEN_TIME,
TO_TIMESTAMP(TEMP_DEVICE.LAST_SEEN_TIME,'YYYYMMDDHH24MISS') as
LAST_SEEN_TIMESTAMP,
TEMP_DEVICE.VendOR,
TEMP_DEVICE.CATEGORY,
case
    when TEMP_DEVICE.CATEGORY = 1 then 'FIXED CONFIGURATION'
```

```
    when TEMP_DEVICE.CATEGORY = 2 then 'CHASSIS'
    when TEMP_DEVICE.CATEGORY = 3 then 'STACK'
    when TEMP_DEVICE.CATEGORY = 4 then 'ACCESS POINT'
    when TEMP_DEVICE.CATEGORY = 5 then 'WIRELESS CONTROLLER'
    else 'UNKNOWN'
end as CATEGORY_TXT,
TEMP_DEVICE.SUB_CATEGORY,
case
    when TEMP_DEVICE.SUB_CATEGORY = 1 then 'DCB 8000'
    when TEMP_DEVICE.SUB_CATEGORY = 2 then 'DCB 8470'
    when TEMP_DEVICE.SUB_CATEGORY = 3 then 'DCB M8428'
    when TEMP_DEVICE.SUB_CATEGORY = 4 then 'DCX'
    when TEMP_DEVICE.SUB_CATEGORY = 5 then 'DCX-4S'
    when TEMP_DEVICE.SUB_CATEGORY = 6 then 'VCS/VDX'
    when TEMP_DEVICE.SUB_CATEGORY = 7 then 'VDX 6720-24'
    when TEMP_DEVICE.SUB_CATEGORY = 8 then 'VDX 6720-60'
    when TEMP_DEVICE.SUB_CATEGORY = 9 then 'VDX 6710'
    when TEMP_DEVICE.SUB_CATEGORY = 10 then 'VDX 6730-24'
    when TEMP_DEVICE.SUB_CATEGORY = 11 then 'VDX 6730-60'
    when TEMP_DEVICE.SUB_CATEGORY = 12 then 'VDX 8770-4'
    when TEMP_DEVICE.SUB_CATEGORY = 13 then 'VDX 8770-8'
    when TEMP_DEVICE.SUB_CATEGORY = 14 then 'VDX 8770-16'
    when TEMP_DEVICE.SUB_CATEGORY = 15 then 'VDX 2730'
    else 'IP DEVICE'
end as SUB_CATEGORY_TXT,
TEMP_DEVICE.FIRST_SEEN_TIME,
TO_TIMESTAMP(TEMP_DEVICE.FIRST_SEEN_TIME,'YYYYMMDDHH24MISS') as
FIRST_SEEN_TIMESTAMP,
TEMP_DEVICE.PORT_COUNT,
TEMP_DEVICE.LICENSE_PORT_COUNT,
case
    when TEMP_DEVICE.SUB_CATEGORY = 0 then (select distinct SWITCH_MODEL.MODEL
from SWITCH_MODEL where TEMP_DEVICE.SYS_OID = SWITCH_MODEL.SYS_OID)
    else TEMP_DEVICE.BRIEF_PRODUCT_FAMILY
end as MODEL,
TEMP_FOUNDRY_DEVICE.IMAGE_VERSION as FIRMWARE,
TEMP_PHYSICAL_DEVICE.PHYSICAL_DEVICE_ID,
TEMP_PHYSICAL_DEVICE.NUM_SLOTS,
TEMP_PHYSICAL_DEVICE.UNIT_NUMBER,
TEMP_DEVICE.USER_DEFINED_VALUE_1,
TEMP_DEVICE.USER_DEFINED_VALUE_2,
TEMP_DEVICE.USER_DEFINED_VALUE_3
from DEVICE as TEMP_DEVICE
left join
(
    select
    FOUNDRY_DEVICE.DEVICE_ID,
    FOUNDRY_DEVICE.PRODUCT_TYPE,
    FOUNDRY_DEVICE.IMAGE_VERSION
    from FOUNDRY_DEVICE
) TEMP_FOUNDRY_DEVICE on TEMP_DEVICE.DEVICE_ID = TEMP_FOUNDRY_DEVICE.DEVICE_ID
left join
(
    select
    PHYSICAL_DEVICE.DEVICE_ID,
    PHYSICAL_DEVICE.PHYSICAL_DEVICE_ID,
    PHYSICAL_DEVICE.NUM_SLOTS,
    PHYSICAL_DEVICE.UNIT_NUMBER
    from PHYSICAL_DEVICE
) TEMP_PHYSICAL_DEVICE on TEMP_DEVICE.DEVICE_ID = TEMP_PHYSICAL_DEVICE.DEVICE_ID;
```

PORT_BOTTLENECK_CONF_INFO

This view provides combine port bottleneck configuration and enough information from switch port for the client to identify the port.

```
create or replace view PORT_BOTTLENECK_CONF_INFO as
select
    PORT_BOTTLENECK_CONFIG.SWITCH_PORT_ID,
    PORT_BOTTLENECK_CONFIG.BOTTLENECK_DETECT_ENABLED,
    PORT_BOTTLENECK_CONFIG.ALERTS_ENABLED,
    PORT_BOTTLENECK_CONFIG.CONGESTION_THRESHOLD,
    PORT_BOTTLENECK_CONFIG.LATENCY_THRESHOLD,
    PORT_BOTTLENECK_CONFIG.WINDOW_,
    PORT_BOTTLENECK_CONFIG.QUIET_TIME,
    PORT_BOTTLENECK_CONFIG.CREATION_TIME,
    PORT_BOTTLENECK_CONFIG.LAST_UPDATE_TIME,
    PORT_BOTTLENECK_CONFIG.LATENCY_SEVERITY,
    PORT_BOTTLENECK_CONFIG.LATENCY_TIME,
    SWITCH_PORT.VIRTUAL_SWITCH_ID,
    SWITCH_PORT.USER_PORT_NUMBER,
    SWITCH_PORT.TYPE,
    SWITCH_PORT.WWN
  from
    PORT_BOTTLENECK_CONFIG
        left outer join SWITCH_PORT
            on PORT_BOTTLENECK_CONFIG.SWITCH_PORT_ID = SWITCH_PORT.ID;

comment on view PORT_BOTTLENECK_CONF_INFO is
Combine port bottleneck configuration and enough info from switch port for the
client to identify the port.;
```

PORT_BOTTLENECK_STAT_INFO

This view provides combine port bottleneck status and enough information from the switch port for the client to identify the port.

```
create or replace view PORT_BOTTLENECK_STAT_INFO as
select
    PORT_BOTTLENECK_STATUS.SWITCH_PORT_ID,
    PORT_BOTTLENECK_STATUS.STATUS,
    SWITCH_PORT.VIRTUAL_SWITCH_ID,
    SWITCH_PORT.USER_PORT_NUMBER,
    SWITCH_PORT.TYPE
  from
    PORT_BOTTLENECK_STATUS
        left outer join SWITCH_PORT
            on PORT_BOTTLENECK_STATUS.SWITCH_PORT_ID = SWITCH_PORT.ID;
```

PORT_GROUP_INFO

```
create or replace view PORT_GROUP_INFO as
select
    SWITCH_PORT.ID as PORT_ID,
    SWITCH_PORT.NAME as SWITCH_PORT_NAME,
    SWITCH_PORT.WWN,
    SWITCH_PORT.HEALTH,
    SWITCH_PORT.STATUS,
```

```
    SWITCH_PORT.PORT_NUMBER,
    SWITCH_PORT.SLOT_NUMBER,
    SWITCH_PORT.FICON_SUPPORTED,
    SWITCH_PORT.STATE,
    SWITCH_PORT.USER_PORT_NUMBER,
    VIRTUAL_SWITCH.NAME as VIRTUAL_SWITCH_NAME,
    VIRTUAL_SWITCH.ID as SWITCH_ID,
    FABRIC.NAME as FABRIC_NAME,
    FABRIC.MANAGED as FABRIC_MANAGED,
    PORT_GROUP.ID as PORT_GROUP_ID,
    PORT_GROUP_MEMBER.ID as PORT_GROUP_MEMBER_ID
from
    SWITCH_PORT, VIRTUAL_SWITCH, FABRIC, FABRIC_MEMBER, PORT_GROUP_MEMBER,
PORT_GROUP
where
    VIRTUAL_SWITCH .ID = SWITCH_PORT.VIRTUAL_SWITCH_ID and
    FABRIC_MEMBER.VIRTUAL_SWITCH_ID = SWITCH_PORT.VIRTUAL_SWITCH_ID and
    FABRIC_MEMBER.FABRIC_ID = FABRIC.ID and
    SWITCH_PORT.ID = PORT_GROUP_MEMBER.SWITCH_PORT_ID and
    PORT_GROUP_MEMBER.PORT_GROUP_ID = PORT_GROUP.ID;
```

ROLE_PRIVILEGE_INFO

```
create or replace view ROLE_PRIVILEGE_INFO as
select
    ROLE.ID,
    ROLE.NAME as ROLE_NAME,
    ROLE.DESCRIPTION as ROLE_DESCRIPTION,
    ROLE.HIDDEN as ROLE_HIDDEN,
    PRIVILEGE.ID as PRIVILEGE_ID,
    PRIVILEGE.NAME as PRIVILEGE_NAME,
    PRIVILEGE.AREA as PRIVILEGE_AREA,
    ROLE_PRIVILEGE_MAP.PERMISSION
from
    ROLE,
    ROLE_PRIVILEGE_MAP,
    PRIVILEGE
where
    ROLE.ID = ROLE_PRIVILEGE_MAP.ROLE_ID and
    PRIVILEGE.ID = ROLE_PRIVILEGE_MAP.PRIVILEGE_ID;
```

PORT_PROFILE_INFO

```
create or replace view PORT_PROFILE_INFO as
select
    PORT_PROFILE.ID,
    PORT_PROFILE.SWITCH_ME_ID,
    PORT_PROFILE.NAME,
    PORT_PROFILE.STATE,
    PORT_PROFILE.SWITCH_PORT_MODE,
    PORT_PROFILE.ACL_PROFILE,
    PORT_PROFILE.QOS_PROFILE,
    PORT_PROFILE.FCOE_PROFILE,
    PORT_PROFILE.VLAN_PROFILE,
    PORT_PROFILE.VLAN_DETAILS,
    PORT_PROFILE.DEFAULT_PROFILE,
    PORT_PROFILE.ACL_NAME,
    PORT_PROFILE.FCOE_MAP_NAME,
```

```
        PORT_PROFILE.ACTIVATED,
    PORT_PROFILE_QOS_MAP.DCB_MODE,
    PORT_PROFILE_QOS_MAP.ETHERNET_MODE,
    PORT_PROFILE_QOS_MAP.PAUSE_TX,
    PORT_PROFILE_QOS_MAP.PAUSE_RX,
    PORT_PROFILE_QOS_MAP.COS_COS,
    PORT_PROFILE_QOS_MAP.TRAFFIC_CLASS,
        PORT_PROFILE_QOS_MAP.COS,
        PORT_PROFILE_QOS_MAP.CEE_MAP,
    PORT_PROFILE_QOS_PFC_MAP.COS0_TX,
    PORT_PROFILE_QOS_PFC_MAP.COS0_RX,
    PORT_PROFILE_QOS_PFC_MAP.COS1_TX,
    PORT_PROFILE_QOS_PFC_MAP.COS1_RX,
    PORT_PROFILE_QOS_PFC_MAP.COS2_TX,
    PORT_PROFILE_QOS_PFC_MAP.COS2_RX,
    PORT_PROFILE_QOS_PFC_MAP.COS3_TX,
    PORT_PROFILE_QOS_PFC_MAP.COS3_RX,
    PORT_PROFILE_QOS_PFC_MAP.COS4_TX,
    PORT_PROFILE_QOS_PFC_MAP.COS4_RX,
    PORT_PROFILE_QOS_PFC_MAP.COS5_TX,
    PORT_PROFILE_QOS_PFC_MAP.COS5_RX,
    PORT_PROFILE_QOS_PFC_MAP.COS6_TX,
    PORT_PROFILE_QOS_PFC_MAP.COS6_RX,
    PORT_PROFILE_QOS_PFC_MAP.COS7_TX,
    PORT_PROFILE_QOS_PFC_MAP.COS7_RX,
        PORT_PROFILE_QOS_MAP.TRUST_COS
from PORT_PROFILE
    left join PORT_PROFILE_QOS_MAP
        on PORT_PROFILE.ID = PORT_PROFILE_QOS_MAP.PROFILE_ID
    left join PORT_PROFILE_QOS_PFC_MAP
        on PORT_PROFILE.ID = PORT_PROFILE_QOS_PFC_MAP.PROFILE_ID;
```

PORT_PROFILE_INTERFACE_INFO

```
create or replace view PORT_PROFILE_INTERFACE_INFO as
select
    PORT_PROFILE.ID,
    PORT_PROFILE.SWITCH_ME_ID,
    PORT_PROFILE.NAME,
    PORT_PROFILE.ACL_PROFILE,
    PORT_PROFILE.QOS_PROFILE,
    PORT_PROFILE.FCOE_PROFILE,
    PORT_PROFILE.VLAN_PROFILE,
    PORT_PROFILE.VLAN_DETAILS,
    PORT_PROFILE.DEFAULT_PROFILE,
    PORT_PROFILE.ACL_NAME,
    PORT_PROFILE.FCOE_MAP_NAME,
    PORT_PROFILE_INTERFACE_MAP.INTERFACE_ID,
    PORT_PROFILE_INTERFACE_MAP.SWITCH_PORT_ID
from
    PORT_PROFILE,
    PORT_PROFILE_INTERFACE_MAP
where
    PORT_PROFILE.ID= PORT_PROFILE_INTERFACE_MAP.PROFILE_ID;
```

PORT_PROFILE_MAC_INFO

```
create or replace view PORT_PROFILE_MAC_INFO as
```

```
select
PORT_PROFILE_MAC_MAP.PROFILE_ID,
PORT_PROFILE_MAC_MAP.MAC,
PORT_PROFILE_MAC_MAP.NAME as MAC_NAME,
VM_VIRTUAL_ETHERNET_ADAPTER.PORT_GROUP_NAME,
VM_VIRTUAL_ETHERNET_ADAPTER.DISPLAY_LABEL,
VM_VIRTUAL_MACHINE.NAME as VM_NAME,
VM_VCENTER_MEMBER.HOST_NAME as HOST_NAME,
VM_VCENTER.NAME as VCENTER_NAME,
INTERFACE.IDENTIFIER
from
PORT_PROFILE_MAC_MAP
left outer join VM_VIRTUAL_ETHERNET_ADAPTER on PORT_PROFILE_MAC_MAP.MAC =
VM_VIRTUAL_ETHERNET_ADAPTER.MAC_ADDRESS
left outer join VM_VIRTUAL_MACHINE on
VM_VIRTUAL_ETHERNET_ADAPTER.VIRTUAL_MACHINE_ID = VM_VIRTUAL_MACHINE.ID
left outer join VM_VCENTER_MEMBER on VM_VIRTUAL_MACHINE.HOST_ID =
VM_VCENTER_MEMBER.VM_HOST_ID
left outer join VM_VCENTER on VM_VCENTER_MEMBER.VM_VCENTER_ID = VM_VCENTER.ID
left outer join L2_NEIGHBOR on PORT_PROFILE_MAC_MAP.MAC =
encode(L2_NEIGHBOR.LLDP_REM_PORT_ID, 'base64')
left outer join INTERFACE on L2_NEIGHBOR.INTERFACE_ID = INTERFACE.INTERFACE_ID;
```

PORT_VLAN_INFO

```
create view PORT_VLAN_INFO as
select
    PV.*,
    DEVICE_ID,
    NAME,
    TABLE_SUBTYPE
from
    VLAN V,
    PORT_VLAN PV
where
    V.VLAN_DB_ID = PV.VLAN_DB_ID;
```

PROTOCOL_VLAN_INFO

```
create or replace view PROTOCOL_VLAN_INFO as
select
        V.*,
        port_vlan_db_id,
        is_dynamic,
        protocol
    from vlan V, sub_port_vlan SPV, protocol_vlan PV
    where V.vlan_db_id = SPV.vlan_db_id AND SPV.vlan_db_id = PV.vlan_db_id;
```

SFLOW

```
create or replace view SFLOW as
```

```
  select DEVICE_ID, IN_SLOT, IN_PORT, OUT_SLOT, OUT_PORT, L4_PROTOCOL, IP_TOS,
SRC_SUBNET_BITS, DEST_SUBNET_BITS, IN_PRIORITY, OUT_PRIORITY, IN_VLAN, OUT_VLAN,
L3_PROTOCOL, L4_SRC_PORT, L4_DEST_PORT, TIME_IN_SECONDS, SRC_MAC, DEST_MAC,
L3_SRC_ADDR, L3_DEST_ADDR, TCP_FLAGS, LOCAL_AS, SRC_AS, SRC_PEER_AS,
SFLOW_IP_ROUTE_INFO_ID, IP_FLOW_LABEL, SRC_USER, DEST_USER, FRAMES, BYTES,
IN_UNIT, OUT_UNIT
  from SFLOW_HOUR_SUMMARY
  where SLNUM <= (select MAX_SLNUM from SFLOW_HOUR_SUMMARY_SLNUM fetch first 1
rows only)
  union all
  select DEVICE_ID, IN_SLOT, IN_PORT, OUT_SLOT, OUT_PORT, L4_PROTOCOL, IP_TOS,
SRC_SUBNET_BITS, DEST_SUBNET_BITS, IN_PRIORITY, OUT_PRIORITY, IN_VLAN, OUT_VLAN,
L3_PROTOCOL, L4_SRC_PORT, L4_DEST_PORT, TIME_IN_SECONDS, SRC_MAC, DEST_MAC,
L3_SRC_ADDR, L3_DEST_ADDR, TCP_FLAGS, LOCAL_AS, SRC_AS, SRC_PEER_AS,
SFLOW_IP_ROUTE_INFO_ID, IP_FLOW_LABEL, SRC_USER, DEST_USER, FRAMES, BYTES,
IN_UNIT, OUT_UNIT
  from SFLOW_STAGING
  where SLNUM >= (select MIN_SLNUM from SFLOW_STAGING_SLNUM fetch first 1 rows
only);
```

SFLOW_MINUTE_L3_VIEW

```
create or replace view SFLOW_MINUTE_L3_VIEW as
  select DEVICE_ID, TIME_IN_SECONDS, L3_SRC_ADDR, L3_DEST_ADDR, L3_PROTOCOL,
L4_PROTOCOL, TCP_FLAGS, IN_VLAN, OUT_VLAN, FRAMES, BYTES
  from SFLOW_MINUTE_L3
  where SLNUM <= (select MAX_SLNUM from SFLOW_MINUTE_L3_SLNUM fetch first 1 rows
only)
  union all
  select DEVICE_ID, TIME_IN_SECONDS, L3_SRC_ADDR, L3_DEST_ADDR, L3_PROTOCOL,
L4_PROTOCOL, TCP_FLAGS, IN_VLAN, OUT_VLAN, FRAMES, BYTES
  from SFLOW_STAGING
  where SLNUM >= (select MIN_SLNUM from SFLOW_STAGING_SLNUM fetch first 1 rows
only);
```

SFLOW_MINUTE_MAC_VIEW

```
create or replace view SFLOW_MINUTE_MAC_VIEW as
  select DEVICE_ID, TIME_IN_SECONDS, SRC_MAC, DEST_MAC, IN_VLAN, OUT_VLAN, FRAMES,
BYTES
  from SFLOW_MINUTE_MAC
  where SLNUM <= (select MAX_SLNUM from SFLOW_MINUTE_MAC_SLNUM fetch first 1 rows
only)
  union all
  select DEVICE_ID, TIME_IN_SECONDS, SRC_MAC, DEST_MAC, IN_VLAN, OUT_VLAN, FRAMES,
BYTES
  from SFLOW_STAGING
  where SLNUM >= (select MIN_SLNUM from SFLOW_STAGING_SLNUM fetch first 1 rows
only);
```

SCOM_EE_MONITOR_INFO

This view provides combined ee_monitor, ee_monitor_stats, device_port and device_node tables to get the EE Monitor information for SCOM plug-in.

```
create or replace view SCOM_EE_MONITOR_INFO as
```

```
select distinct
    EE_MONITOR.NAME,
    EE_MONITOR.SWITCH_PORT_ID,
    EE_MONITOR.SOURCE_PORT_ID,
    EE_MONITOR.DEST_PORT_ID,
    EE_MONITOR_STATS.TX,
    EE_MONITOR_STATS.RX,
    EE_MONITOR_STATS.CRCERRORS,
    EE_MONITOR_STATS.CREATION_TIME,
    SOURCE_PORT.PORT_ID as SID,
    DEST_PORT.PORT_ID as DID,
    SOURCE_NODE.WWN as SOURCE_DEVICE_WWN,
    SOURCE_PORT.WWN as SOURCE_PORT_WWN,
    DEST_NODE.WWN as DEST_DEVICE_WWN,
    DEST_PORT.WWN as DEST_PORT_WWN,
    SOURCE_NODE.FABRIC_ID as SOURCE_FABRIC_ID,
    DEST_NODE.FABRIC_ID as DEST_FABRIC_ID,
    SOURCE_PORT.DOMAIN_ID as SOURCE_SWITCH_DOMAIN_ID,
    DEST_PORT.DOMAIN_ID as DEST_SWITCH_DOMAIN_ID
from
    DEVICE_PORT as SOURCE_PORT,
    DEVICE_PORT as DEST_PORT,
    DEVICE_NODE as DEST_NODE,
    DEVICE_NODE as SOURCE_NODE,
    EE_MONITOR,
    EE_MONITOR_STATS
where
    SOURCE_PORT.ID = EE_MONITOR.SOURCE_PORT_ID
    and EE_MONITOR.ID = EE_MONITOR_STATS.EE_MONITOR_ID
    and SOURCE_PORT.NODE_ID = SOURCE_NODE.ID
    and DEST_PORT.ID = EE_MONITOR.DEST_PORT_ID
    and DEST_PORT.NODE_ID = DEST_NODE.ID
    and EE_MONITOR_STATS.CREATION_TIME in (
        select MAX(CREATION_TIME)
        from EE_MONITOR_STATS
        group by EE_MONITOR_ID);
```

SENSOR_INFO

```
create or replace view SENSOR_INFO as
select
    SENSOR.ID,
    SENSOR.CORE_SWITCH_ID,
    SENSOR.SENSOR_ID,
    SENSOR.CURRENT_READING,
    SENSOR.TYPE,
    SENSOR.SUB_TYPE,
    SENSOR.DESCRIPTION,
    SENSOR.STATUS,
    SENSOR.OPERATIONAL_STATUS,
    SENSOR.PART_NUMBER,
    SENSOR.SERIAL_NUMBER,
    SENSOR.VERSION,
    SENSOR.CREATION_TIME,
    SENSOR.LAST_UPDATE_TIME,
    SENSOR.FRU_TYPE,
    SENSOR.UNIT_NUMBER,
    SENSOR.STATE,
    CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN,
```

```
    VIRTUAL_SWITCH.SWITCH_MODE as VIRTUAL_SWITCH_MODE,
    VIRTUAL_SWITCH.MANAGEMENT_STATE,
    VIRTUAL_SWITCH.MONITORED
from
    SENSOR,
    CORE_SWITCH,
    VIRTUAL_SWITCH
where
    SENSOR.CORE_SWITCH_ID = CORE_SWITCH.ID and
    SENSOR.CORE_SWITCH_ID = VIRTUAL_SWITCH.CORE_SWITCH_ID;
```

SMART_CARD_USAGE_INFO

```
create or replace view SMART_CARD_USAGE_INFO as
select
    SC.ID SMART_CARD_ID,
    SC.CARD_TYPE,
    SC.CARD_INFO,
    SC.CARDCN_ID,
    SC.FIRST_NAME,
    SC.LAST_NAME,
    SC.NOTES,
    SC.CREATION_TIME,
    -1 ENGINE_ID,
    EG.ID ENCRYPTION_GROUP_ID,
    EG.NAME GROUP_NAME,
    -1 CARD_POSITION,
    -1 CRYPTO_SWITCH_ID,
    -1 SLOT_NUMBER
from
    SMART_CARD SC,
    ENCRYPTION_GROUP EG,
    QUORUM_CARD_GROUP_MAPPING QCGM
where
    QCGM.SMART_CARD_ID = SC.ID
    and EG.ID = QCGM.ENCRYPTION_GROUP_ID
    and SC.CARD_TYPE = 0
union
select
    SC.ID SMART_CARD_ID,
    SC.CARD_TYPE,
    SC.CARD_INFO,
    SC.CARDCN_ID,
    SC.FIRST_NAME,
    SC.LAST_NAME,
    SC.NOTES,
    SC.CREATION_TIME,
    -1 ENGINE_ID,
    EG.ID ENCRYPTION_GROUP_ID,
    EG.NAME GROUP_NAME,
    RCGM.POSITION_ CARD_POSITION,
    -1 CRYPTO_SWITCH_ID,
    -1 SLOT_NUMBER
from
    SMART_CARD SC,
    ENCRYPTION_GROUP EG,
    RECOVERY_CARD_GROUP_MAPPING RCGM
where
    SC.ID = RCGM.SMART_CARD_ID
```

```
    and EG.ID = RCGM.ENCRYPTION_GROUP_ID
    and SC.CARD_TYPE = 1
union
select
    SC.ID SMART_CARD_ID,
    SC.CARD_TYPE,
    SC.CARD_INFO,
    SC.CARDCN_ID,
    SC.FIRST_NAME,
    SC.LAST_NAME,
    SC.NOTES,
    SC.CREATION_TIME,
    EE.ID ENGINE_ID,
    -1 ENCRYPTION_GROUP_ID,
    '' GROUP_NAME,
    -1 CARD_POSITION,
    EE.SWITCH_ID CRYPTO_SWITCH_ID,
    EE.SLOT_NUMBER SLOT_NUMBER
from
    SMART_CARD SC,
    ENCRYPTION_ENGINE EE,
    SYSTEM_CARD_ENGINE_MAPPING SCEM
where
    SC.ID = SCEM.SMART_CARD_ID
    and EE.ID = SCEM.ENCRYPTION_ENGINE_ID
    and SC.CARD_TYPE = 2;
```

SWITCH_CONFIG_INFO

```
create or replace view SWITCH_CONFIG_INFO as
select
    SWITCH_CONFIG.ID,
    SWITCH_CONFIG.NAME,
    SWITCH_CONFIG.SWITCH_ID,
    SWITCH_CONFIG.CORE_SWITCH_ID,
    SWITCH_CONFIG.BACKUP_DATE_TIME,
    SWITCH_CONFIG.CONFIG_DATA,
    SWITCH_CONFIG.CEE_CONFIG_DATA,
    SWITCH_CONFIG.KEEP_COPY,
    SWITCH_CONFIG.CREATED_BY,
    SWITCH_CONFIG.COMMENTS,
    SWITCH_CONFIG.CONFIG_TYPE,
    SWITCH_CONFIG_DETAIL.IP_ADDRESS,
    SWITCH_CONFIG_DETAIL.WWN,
    SWITCH_CONFIG_DETAIL.PHYSICAL_SWITCH_WWN,
    SWITCH_CONFIG_DETAIL.MODEL_NUMBER as SWITCH_MODEL_NUMBER
from
    SWITCH_CONFIG,
    SWITCH_CONFIG_DETAIL
where
    SWITCH_CONFIG.ID= SWITCH_CONFIG_DETAIL.SWITCH_CONFIG_ID;
```

SWITCH_DETAILS_INFO

```
CREATE VIEW switch_details_info AS
    select
   CORE_SWITCH.ID as PHYSICAL_SWITCH_ID,
   CORE_SWITCH.NAME as PHYSICAL_SWITCH_NAME,
```

```
CORE_SWITCH.IP_ADDRESS,
CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN,
CORE_SWITCH.OPERATIONAL_STATUS as PHYSICAL_OPERATIONAL_STATUS,
CORE_SWITCH.TYPE,
CORE_SWITCH.MAX_VIRTUAL_SWITCHES,
CORE_SWITCH.FIRMWARE_VERSION,
CORE_SWITCH.VENDOR,
CORE_SWITCH.REACHABLE,
CORE_SWITCH.UNREACHABLE_TIME,
CORE_SWITCH.MODEL,
CORE_SWITCH.SYSLOG_REGISTERED,
CORE_SWITCH.SNMP_REGISTERED,
CORE_SWITCH.USER_IP_ADDRESS,
CORE_SWITCH.MANAGING_SERVER_IP_ADDRESS,
CORE_SWITCH.CREATION_TIME as CS_CREATION_TIME,
CORE_SWITCH.LAST_UPDATE_TIME as CS_LAST_UPDATE_TIME,
CORE_SWITCH.NUM_VIRTUAL_SWITCHES,
CORE_SWITCH.VF_ENABLED,
CORE_SWITCH.VF_SUPPORTED,
CORE_SWITCH.CALL_HOME_ENABLED,
CORE_SWITCH.MANAGED_ELEMENT_ID as CORE_MANAGED_ELEMENT_ID,
CORE_SWITCH.NAT_PRIVATE_IP_ADDRESS,
CORE_SWITCH.ALTERNATE_IP_ADDRESS,
CORE_SWITCH.MAC_ADDRESS,
VIRTUAL_SWITCH.ID,
VIRTUAL_SWITCH.NAME,
VIRTUAL_SWITCH.OPERATIONAL_STATUS,
VIRTUAL_SWITCH.SWITCH_MODE,
VIRTUAL_SWITCH.AD_CAPABLE,
VIRTUAL_SWITCH.WWN,
VIRTUAL_SWITCH.ROLE,
VIRTUAL_SWITCH.FCS_ROLE,
VIRTUAL_SWITCH.DOMAIN_ID,
VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID,
VIRTUAL_SWITCH.BASE_SWITCH,
VIRTUAL_SWITCH.MAX_ZONE_CONFIG_SIZE,
VIRTUAL_SWITCH.CREATION_TIME,
VIRTUAL_SWITCH.LAST_UPDATE_TIME,
VIRTUAL_SWITCH.USER_NAME,
VIRTUAL_SWITCH.PASSWORD,
VIRTUAL_SWITCH.MANAGEMENT_STATE,
VIRTUAL_SWITCH.STATE,
VIRTUAL_SWITCH.STATUS,
VIRTUAL_SWITCH.STATUS_REASON,
VIRTUAL_SWITCH.FABRIC_IDID_MODE,
VIRTUAL_SWITCH.LOGICAL_ID,
VIRTUAL_SWITCH.USER_DEFINED_VALUE_1,
VIRTUAL_SWITCH.USER_DEFINED_VALUE_2,
VIRTUAL_SWITCH.USER_DEFINED_VALUE_3,
VIRTUAL_SWITCH.FMS_MODE,
VIRTUAL_SWITCH.DYNAMIC_LOAD_SHARING,
VIRTUAL_SWITCH.PORT_BASED_ROUTING,
VIRTUAL_SWITCH.IN_ORDER_DELIVERY,
VIRTUAL_SWITCH.INSISTENT_DID_MODE,
VIRTUAL_SWITCH.FCR_CAPABLE,
VIRTUAL_SWITCH.LAST_PORT_MEMBERSHIP_CHANGE,
VIRTUAL_SWITCH.FCIP_CIRCUIT_CAPABLE,
VIRTUAL_SWITCH.MAX_FCIP_TUNNELS,
VIRTUAL_SWITCH.MAX_FCIP_CIRCUITS,
VIRTUAL_SWITCH.FCIP_LICENSED,
```

```
    VIRTUAL_SWITCH.MANAGED_ELEMENT_ID,
    VIRTUAL_SWITCH.RNID_SEQUENCE_NUMBER as VS_RNID_SEQUENCE_NUMBER,
    VIRTUAL_SWITCH.CLUSTER_MODE,
    VIRTUAL_SWITCH.VCS_ID,
    VIRTUAL_SWITCH.CLUSTER_TYPE,
    VIRTUAL_SWITCH.RNID_TAG,
    VIRTUAL_SWITCH.SWITCH_ID,
    VIRTUAL_SWITCH.MONITORED,
    VIRTUAL_SWITCH.MAPS_ENABLED_ACTIONS,
    VIRTUAL_SWITCH.FEATURES_ENABLED,
    VIRTUAL_SWITCH.FABRIC_STATUS,
    FABRIC_MEMBER.FABRIC_ID,
    FABRIC_MEMBER.TRUSTED,
    FABRIC_MEMBER.MISSING,
    FABRIC_MEMBER.MISSING_TIME,
    CORE_SWITCH_DETAILS.ETHERNET_MASK,
    CORE_SWITCH_DETAILS.FC_MASK,
    CORE_SWITCH_DETAILS.FC_IP,
    CORE_SWITCH_DETAILS.FC_CERTIFICATE,
    CORE_SWITCH_DETAILS.SW_LICENSE_ID,
    CORE_SWITCH_DETAILS.SUPPLIER_SERIAL_NUMBER,
    CORE_SWITCH_DETAILS.PART_NUMBER,
    CORE_SWITCH_DETAILS.CHECK_BEACON,
    CORE_SWITCH_DETAILS.TIMEZONE,
    CORE_SWITCH_DETAILS.MAX_PORT,
    CORE_SWITCH_DETAILS.CHASSIS_SERVICE_TAG,
    CORE_SWITCH_DETAILS.BAY_ID,
    CORE_SWITCH_DETAILS.TYPE_NUMBER,
    CORE_SWITCH_DETAILS.MODEL_NUMBER,
    CORE_SWITCH_DETAILS.MANUFACTURER,
    CORE_SWITCH_DETAILS.PLANT_OF_MANUFACTURER,
    CORE_SWITCH_DETAILS.SWITCH_SERIAL_NUMBER,
    CORE_SWITCH_DETAILS.ACT_CP_PRI_FW_VERSION,
    CORE_SWITCH_DETAILS.ACT_CP_SEC_FW_VERSION,
    CORE_SWITCH_DETAILS.STBY_CP_PRI_FW_VERSION,
    CORE_SWITCH_DETAILS.STBY_CP_SEC_FW_VERSION,
    CORE_SWITCH_DETAILS.TYPE as DETAILS_TYPE,
    CORE_SWITCH_DETAILS.EGM_CAPABLE,
    CORE_SWITCH_DETAILS.SUB_TYPE,
    CORE_SWITCH_DETAILS.PARTITION,
    CORE_SWITCH_DETAILS.MAX_NUM_OF_BLADES,
    CORE_SWITCH_DETAILS.SNMP_INFORMS_ENABLED,
    CORE_SWITCH_DETAILS.VENDOR_VERSION,
    CORE_SWITCH_DETAILS.VENDOR_PART_NUMBER,
    CORE_SWITCH_DETAILS.CONTACT,
    CORE_SWITCH_DETAILS.LOCATION,
    CORE_SWITCH_DETAILS.DESCRIPTION,
    CORE_SWITCH_DETAILS.RNID_SEQUENCE_NUMBER,
    CORE_SWITCH_DETAILS.FIRMWARE_VERSION as CSD_FIRMWARE_VERSION,
    CORE_SWITCH_DETAILS.CHASSIS_PACKAGE_TYPE,
    CORE_SWITCH_DETAILS.IP_ADDRESS_PREFIX,
    CORE_SWITCH_DETAILS.DOMAIN_NAME,
    CORE_SWITCH_DETAILS.FRAME_LOG_SIZE,
    CORE_SWITCH_DETAILS.FRAME_LOG_ENABLED,
    CORE_SWITCH_DETAILS.MAPS_ENABLED
from
    CORE_SWITCH,
    VIRTUAL_SWITCH,
    FABRIC_MEMBER,
    CORE_SWITCH_DETAILS
```

```
where
   VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID
   and FABRIC_MEMBER.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
   and CORE_SWITCH_DETAILS.CORE_SWITCH_ID = CORE_SWITCH.ID;
```

SWITCH_DISCOVERED_MAC_INFO

```
create or replace view SWITCH_DISCOVERED_MAC_INFO as
select
    L2_NEIGHBOR.LLDP_REM_CHASSIS_ID_VALUE,
    L2_NEIGHBOR.INTERFACE_ID,
    INTERFACE.NAME as INTERFACE_NAME,
    DEVICE.SYS_NAME as DEVICE_NAME,
    DEVICE.IP_ADDRESS, DEVICE.DEVICE_ID
from
    L2_NEIGHBOR,
    INTERFACE,
    DEVICE
where
    L2_NEIGHBOR.LLDP_REM_CHASSIS_ID_SUBTYPE = 4
    and L2_NEIGHBOR.INTERFACE_ID = INTERFACE.INTERFACE_ID
    and INTERFACE.DEVICE_ID = DEVICE.DEVICE_ID;
```

SWITCH_PORT_INFO

```
CREATE VIEW switch_port_info AS
select
    SWITCH_PORT.ID,
    SWITCH_PORT.VIRTUAL_SWITCH_ID,
    SWITCH_PORT.WWN,
    SWITCH_PORT.NAME,
    SWITCH_PORT.SLOT_NUMBER,
    SWITCH_PORT.PORT_NUMBER,
    SWITCH_PORT.USER_PORT_NUMBER,
    SWITCH_PORT.PORT_ID,
    SWITCH_PORT.PORT_INDEX,
    SWITCH_PORT.AREA_ID,
    SWITCH_PORT.MAC_ADDRESS,
    SWITCH_PORT.PORT_MOD,
    SWITCH_PORT.TYPE,
    SWITCH_PORT.FULL_TYPE,
    SWITCH_PORT.STATUS,
    SWITCH_PORT.HEALTH,
    SWITCH_PORT.STATUS_MESSAGE,
    SWITCH_PORT.PHYSICAL_PORT,
    SWITCH_PORT.LOCKED_PORT_TYPE,
    SWITCH_PORT.CATEGORY,
    SWITCH_PORT.PROTOCOL,
    SWITCH_PORT.SPEED,
    SWITCH_PORT.SPEEDS_SUPPORTED,
    SWITCH_PORT.MAX_PORT_SPEED,
    SWITCH_PORT.DESIRED_CREDITS,
    SWITCH_PORT.BUFFER_ALLOCATED,
    SWITCH_PORT.ESTIMATED_DISTANCE,
    SWITCH_PORT.ACTUAL_DISTANCE,
    SWITCH_PORT.LONG_DISTANCE_SETTING,
    SWITCH_PORT.DEGRADED_PORT,
    SWITCH_PORT.REMOTE_NODE_WWN,
```

```
SWITCH_PORT.REMOTE_PORT_WWN,
SWITCH_PORT.LICENSED,
SWITCH_PORT.SWAPPED,
SWITCH_PORT.TRUNKED,
SWITCH_PORT.TRUNK_MASTER,
SWITCH_PORT.PERSISTENT_DISABLE,
SWITCH_PORT.FICON_SUPPORTED,
SWITCH_PORT.BLOCKED,
SWITCH_PORT.PROHIBIT_PORT_NUMBERS,
SWITCH_PORT.PROHIBIT_PORT_COUNT,
SWITCH_PORT.NPIV,
SWITCH_PORT.NPIV_CAPABLE,
SWITCH_PORT.NPIV_ENABLED,
SWITCH_PORT.FC_FAST_WRITE_ENABLED,
SWITCH_PORT.ISL_RRDY_ENABLED,
SWITCH_PORT.RATE_LIMIT_CAPABLE,
SWITCH_PORT.RATE_LIMITED,
SWITCH_PORT.QOS_CAPABLE,
SWITCH_PORT.QOS_ENABLED,
SWITCH_PORT.TUNNEL_CONFIGURED,
SWITCH_PORT.FCIP_TUNNEL_UP,
SWITCH_PORT.FCR_FABRIC_ID,
SWITCH_PORT.FCR_INTEROP_MODE,
SWITCH_PORT.CALCULATED_STATUS,
SWITCH_PORT.USER_DEFINED_VALUE1,
SWITCH_PORT.USER_DEFINED_VALUE2,
SWITCH_PORT.USER_DEFINED_VALUE3,
SWITCH_PORT.KIND,
SWITCH_PORT.STATE,
SWITCH_PORT.PREVIOUS_STATUS,
SWITCH_PORT.LAST_UPDATE,
SWITCH_PORT.OCCUPIED,
SWITCH_PORT.PORT_BIT_MASK,
SWITCH_PORT.LOGICAL_PORT_NUMBER,
SWITCH_PORT.DEFAULT_AREA_ID,
SWITCH_PORT.LOGICAL_PORT_WWN,
SWITCH_PORT.LATENCY_DETECT_SUPPORTED,
SWITCH_PORT.EPORT_DISABLED,
SWITCH_PORT.SPEED_NEGOTIATED,
SWITCH_PORT.IDENTIFIER,
SWITCH_PORT.PORT_CAPABILITIES,
SWITCH_PORT.FAKE_PORT,
SWITCH_PORT.XISL_PORT_LIST,
SWITCH_PORT.PORT_COMMISSION_STATE,
SWITCH_PORT.FEATURES_ENABLED,
SWITCH_PORT.FEATURES_ACTIVE,
SWITCH_PORT.DISABLED_REASON_CODE,
SWITCH_PORT.DISABLED_REASON,
SWITCH_PORT.FENCED,
SWITCH_PORT.MASTER_PORT_NUMBER,
SWITCH_PORT.SPEED_TYPE,
VIRTUAL_SWITCH.WWN as VIRTUAL_SWITCH_WWN,
VIRTUAL_SWITCH.ROLE as SWITCH_ROLE,
VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID as VIRTUAL_FABRIC_ID,
VIRTUAL_SWITCH.DOMAIN_ID as DOMAIN_ID,
VIRTUAL_SWITCH.INTEROP_MODE as INTEROP_MODE,
VIRTUAL_SWITCH.MANAGEMENT_STATE,
VIRTUAL_SWITCH.MANAGED_ELEMENT_ID,
VIRTUAL_SWITCH.MONITORED,
CORE_SWITCH.TYPE as SWITCH_TYPE,
```

```
    CORE_SWITCH.FIRMWARE_VERSION as FIRMWARE_VERSION,
    CORE_SWITCH.IP_ADDRESS as IP_ADDRESS,
    CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN,
    CORE_SWITCH.MODEL as SWITCH_MODEL,
    CORE_SWITCH_DETAILS.MODEL_NUMBER as SWITCH_MODEL_NUMBER
FROM SWITCH_PORT, VIRTUAL_SWITCH, CORE_SWITCH
LEFT JOIN CORE_SWITCH_DETAILS
    ON CORE_SWITCH_DETAILS.CORE_SWITCH_ID = CORE_SWITCH.ID
    where SWITCH_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
    AND VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID;
```

SWITCH_SNMP_INFO

```
create or replace view SWITCH_SNMP_INFO as
select
    CORE_SWITCH.ID as PHYSICAL_SWITCH_ID,
    CORE_SWITCH.NAME as PHYSICAL_SWITCH_NAME,
    CORE_SWITCH.IP_ADDRESS,
    CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN,
    CORE_SWITCH.OPERATIONAL_STATUS as PHYSICAL_OPERATIONAL_STATUS,
    CORE_SWITCH.TYPE,
    CORE_SWITCH.MAX_VIRTUAL_SWITCHES,
    CORE_SWITCH.FIRMWARE_VERSION,
    CORE_SWITCH.VENDOR,
    CORE_SWITCH.REACHABLE,
    CORE_SWITCH.UNREACHABLE_TIME,
    CORE_SWITCH.MODEL,
    CORE_SWITCH_DETAILS.CONTACT,
    CORE_SWITCH_DETAILS.LOCATION,
    CORE_SWITCH_DETAILS.DESCRIPTION,
    VIRTUAL_SWITCH.ID,
    VIRTUAL_SWITCH.NAME,
    VIRTUAL_SWITCH.OPERATIONAL_STATUS,
    VIRTUAL_SWITCH.SWITCH_MODE,
    VIRTUAL_SWITCH.AD_CAPABLE,
    VIRTUAL_SWITCH.FCIP_CAPABLE,
    VIRTUAL_SWITCH.WWN,
    VIRTUAL_SWITCH.ROLE,
    VIRTUAL_SWITCH.FCS_ROLE,
    VIRTUAL_SWITCH.DOMAIN_ID,
    VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID,
    VIRTUAL_SWITCH.BASE_SWITCH,
    VIRTUAL_SWITCH.MAX_ZONE_CONFIG_SIZE,
    VIRTUAL_SWITCH.CREATION_TIME,
    VIRTUAL_SWITCH.LAST_UPDATE_TIME,
    VIRTUAL_SWITCH.USER_NAME,
    VIRTUAL_SWITCH.PASSWORD,
    VIRTUAL_SWITCH.MANAGEMENT_STATE,
    VIRTUAL_SWITCH.STATE,
    VIRTUAL_SWITCH.STATUS,
    VIRTUAL_SWITCH.STATUS_REASON,
    VIRTUAL_SWITCH.MONITORED,
    VIRTUAL_SWITCH.USER_DEFINED_VALUE_1,
    VIRTUAL_SWITCH.USER_DEFINED_VALUE_2,
    VIRTUAL_SWITCH.USER_DEFINED_VALUE_3,
    FABRIC_MEMBER.FABRIC_ID,
    FABRIC_MEMBER.TRUSTED,
    FABRIC_MEMBER.MISSING,
    FABRIC_MEMBER.MISSING_TIME,
```

```
    coalesce(SNMP_CREDENTIALS.PORT_NUMBER, (select SNMP_PROFILE.PORT_NUMBER from
SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_PORT_NUMBER,
    coalesce(SNMP_CREDENTIALS.RETRY_COUNT, (select SNMP_PROFILE.RETRY_COUNT from
SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_RETRY_COUNT,
    coalesce(SNMP_CREDENTIALS.TIMEOUT, (select SNMP_PROFILE.TIMEOUT from
SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_TIMEOUT,
    coalesce(SNMP_CREDENTIALS.VERSION, (select SNMP_PROFILE.VERSION from
SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_VERSION,
    coalesce(SNMP_CREDENTIALS.READ_COMMUNITY_STRING, (select
SNMP_PROFILE.READ_COMMUNITY_STRING from SNMP_PROFILE where
SNMP_PROFILE.NAME='default')) as SNMP_READ_COMMUNITY_STRING,
    coalesce(SNMP_CREDENTIALS.WRITE_COMMUNITY_STRING, (select
SNMP_PROFILE.WRITE_COMMUNITY_STRING from SNMP_PROFILE where
SNMP_PROFILE.NAME='default')) as SNMP_WRITE_COMMUNITY_STRING,
    coalesce(SNMP_CREDENTIALS.USER_NAME, (select SNMP_PROFILE.USER_NAME from
SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_USER_NAME,
    coalesce(SNMP_CREDENTIALS.CONTEXT_NAME, (select SNMP_PROFILE.CONTEXT_NAME
from SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_CONTEXT_NAME,
    coalesce(SNMP_CREDENTIALS.AUTH_PROTOCOL, (select SNMP_PROFILE.AUTH_PROTOCOL
from SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_AUTH_PROTOCOL,
    coalesce(SNMP_CREDENTIALS.AUTH_PASSWORD, (select SNMP_PROFILE.AUTH_PASSWORD
from SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_AUTH_PASSWORD,
    coalesce(SNMP_CREDENTIALS.PRIV_PROTOCOL, (select SNMP_PROFILE.PRIV_PROTOCOL
from SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_PRIV_PROTOCOL,
    coalesce(SNMP_CREDENTIALS.PRIV_PASSWORD, (select SNMP_PROFILE.PRIV_PASSWORD
from SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_PRIV_PASSWORD,
    coalesce(SNMP_CREDENTIALS.SNMP_INFORMS_ENABLED, (select
SNMP_PROFILE.SNMP_INFORMS_ENABLED from SNMP_PROFILE where
SNMP_PROFILE.NAME='default')) as SNMP_INFORMS_ENABLED
from
    VIRTUAL_SWITCH
        left outer join CORE_SWITCH
            on VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID
        left outer join CORE_SWITCH_DETAILS
            on CORE_SWITCH.ID = CORE_SWITCH_DETAILS.CORE_SWITCH_ID
        left outer join FABRIC_MEMBER
            on FABRIC_MEMBER.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
        left outer join SNMP_CREDENTIALS
            on VIRTUAL_SWITCH.ID = SNMP_CREDENTIALS.VIRTUAL_SWITCH_ID;
```

TIME_SERIES_DATA_INFO

```
CREATE VIEW time_series_data_info AS
    (  ( ( ( ( (
select * from TIME_SERIES_DATA_1
union all
select TIME_SERIES_DATA_1_30MIN.TIME_IN_SECONDS,
       TIME_SERIES_DATA_1_30MIN.TARGET_TYPE,
       TIME_SERIES_DATA_1_30MIN.MEASURE_ID,
       TIME_SERIES_DATA_1_30MIN.TARGET_ID,
       TIME_SERIES_DATA_1_30MIN.COLLECTOR_ID,
       TIME_SERIES_DATA_1_30MIN.MEASURE_INDEX,
       TIME_SERIES_DATA_1_30MIN.ME_ID,
       TIME_SERIES_DATA_1_30MIN.VALUE,
       TIME_SERIES_DATA_1_30MIN.SUM_VALUE
from TIME_SERIES_DATA_1_30MIN)
union all
select TIME_SERIES_DATA_1_2HOUR.TIME_IN_SECONDS,
       TIME_SERIES_DATA_1_2HOUR.TARGET_TYPE,
```

```
       TIME_SERIES_DATA_1_2HOUR.MEASURE_ID,
       TIME_SERIES_DATA_1_2HOUR.TARGET_ID,
       TIME_SERIES_DATA_1_2HOUR.COLLECTOR_ID,
       TIME_SERIES_DATA_1_2HOUR.MEASURE_INDEX,
       TIME_SERIES_DATA_1_2HOUR.ME_ID,
       TIME_SERIES_DATA_1_2HOUR.VALUE,
       TIME_SERIES_DATA_1_2HOUR.SUM_VALUE
from TIME_SERIES_DATA_1_2HOUR)
union all
select TIME_SERIES_DATA_1_1DAY.TIME_IN_SECONDS,
       TIME_SERIES_DATA_1_1DAY.TARGET_TYPE,
       TIME_SERIES_DATA_1_1DAY.MEASURE_ID,
       TIME_SERIES_DATA_1_1DAY.TARGET_ID,
       TIME_SERIES_DATA_1_1DAY.COLLECTOR_ID,
       TIME_SERIES_DATA_1_1DAY.MEASURE_INDEX,
       TIME_SERIES_DATA_1_1DAY.ME_ID,
       TIME_SERIES_DATA_1_1DAY.VALUE,
       TIME_SERIES_DATA_1_1DAY.SUM_VALUE
from TIME_SERIES_DATA_1_1DAY)
union all
select * from TIME_SERIES_DATA_2)
union all
select TIME_SERIES_DATA_2_30MIN.TIME_IN_SECONDS,
       TIME_SERIES_DATA_2_30MIN.TARGET_TYPE,
       TIME_SERIES_DATA_2_30MIN.MEASURE_ID,
       TIME_SERIES_DATA_2_30MIN.TARGET_ID,
       TIME_SERIES_DATA_2_30MIN.COLLECTOR_ID,
       TIME_SERIES_DATA_2_30MIN.MEASURE_INDEX,
       TIME_SERIES_DATA_2_30MIN.ME_ID,
       TIME_SERIES_DATA_2_30MIN.VALUE,
       TIME_SERIES_DATA_2_30MIN.SUM_VALUE
from TIME_SERIES_DATA_2_30MIN)
union all
select TIME_SERIES_DATA_2_2HOUR.TIME_IN_SECONDS,
       TIME_SERIES_DATA_2_2HOUR.TARGET_TYPE,
       TIME_SERIES_DATA_2_2HOUR.MEASURE_ID,
       TIME_SERIES_DATA_2_2HOUR.TARGET_ID,
       TIME_SERIES_DATA_2_2HOUR.COLLECTOR_ID,
       TIME_SERIES_DATA_2_2HOUR.MEASURE_INDEX,
       TIME_SERIES_DATA_2_2HOUR.ME_ID,
       TIME_SERIES_DATA_2_2HOUR.VALUE,
       TIME_SERIES_DATA_2_2HOUR.SUM_VALUE
from TIME_SERIES_DATA_2_2HOUR)
union all
select TIME_SERIES_DATA_2_1DAY.TIME_IN_SECONDS,
       TIME_SERIES_DATA_2_1DAY.TARGET_TYPE,
       TIME_SERIES_DATA_2_1DAY.MEASURE_ID,
       TIME_SERIES_DATA_2_1DAY.TARGET_ID,
       TIME_SERIES_DATA_2_1DAY.COLLECTOR_ID,
       TIME_SERIES_DATA_2_1DAY.MEASURE_INDEX,
       TIME_SERIES_DATA_2_1DAY.ME_ID,
       TIME_SERIES_DATA_2_1DAY.VALUE,
       TIME_SERIES_DATA_2_1DAY.SUM_VALUE
from TIME_SERIES_DATA_2_1DAY
```

TIME_SERIES_DATA_VIEW

```
create or replace view TIME_SERIES_DATA_VIEW as
```

```
(         SELECT de.device_id, cast (de.ip_address as varchar(255)) AS device_ip,
                    tsd.target_type, de.device_id AS target_id,
                    de.sys_name AS target_name,
                    measure.measure_type AS collectible_type,
                    tsd.measure_id AS collectible_id, tsd.collector_id,
                    pdc.name AS collector_name,
                    (measure.name::text || '.'::text) || tsd.measure_index::text
AS collectible_name,
                    measure.detail AS collectible_detail, tsd.value,
                    tsd.time_in_seconds, tsd.measure_index
                   FROM time_series_data_info tsd
              JOIN device de ON tsd.target_id = de.device_id
         JOIN pm_data_collector pdc ON pdc.id = tsd.collector_id
    JOIN measure ON measure.id = tsd.measure_id
   WHERE tsd.target_type = 0 OR tsd.target_type = 18
UNION ALL
                 SELECT de.device_id, cast (de.ip_address as varchar(255)) AS
device_ip,
                    tsd.target_type, ifs.interface_id AS target_id,
                    ifs.if_name AS target_name,
                    measure.measure_type AS collectible_type,
                    tsd.measure_id AS collectible_id, tsd.collector_id,
                    pm_data_collector.name AS collector_name,
                    (measure.name::text || '.'::text) || tsd.measure_index::text
AS collectible_name,
                    measure.detail AS collectible_detail, tsd.value,
                    tsd.time_in_seconds, tsd.measure_index
                   FROM time_series_data_info tsd
             JOIN interface ifs ON (tsd.target_type = 1 OR tsd.target_type = 2 OR
tsd.target_type =15) AND tsd.target_id = ifs.interface_id
         JOIN device de ON ifs.device_id = de.device_id
    JOIN pm_data_collector ON pm_data_collector.id = tsd.collector_id
   JOIN measure ON measure.id = tsd.measure_id)
UNION ALL
         SELECT de.device_id, cast (de.ip_address as varchar(255)) AS device_ip,
tsd.target_type,
            sp.id AS target_id, sp.name AS target_name,
            measure.measure_type AS collectible_type,
            tsd.measure_id AS collectible_id, tsd.collector_id,
            pm_data_collector.name AS collector_name,
            (measure.name::text || '.'::text) || tsd.measure_index::text AS
collectible_name,
            measure.detail AS collectible_detail, tsd.value,
            tsd.time_in_seconds, tsd.measure_index
           FROM time_series_data_info tsd
      JOIN switch_port sp ON tsd.target_type = 4 AND tsd.target_id = sp.id
   JOIN virtual_switch vs ON sp.virtual_switch_id = vs.id
   JOIN device de ON vs.managed_element_id = de.managed_element_id
   JOIN pm_data_collector ON pm_data_collector.id = tsd.collector_id
   JOIN measure ON measure.id = tsd.measure_id
UNION ALL
        SELECT 0 as device_id, cast (vs.ip_address as varchar(255)) AS device_ip,
tsd.target_type,
            sp.id AS target_id, sp.name AS target_name,
            measure.measure_type AS collectible_type,
            tsd.measure_id AS collectible_id, tsd.collector_id,
            pm_data_collector.name AS collector_name,
            (measure.name::text || '.'::text) || tsd.measure_index::text AS
collectible_name,
            measure.detail AS collectible_detail, tsd.value,
```

```
            tsd.time_in_seconds, tsd.measure_index
           FROM time_series_data_info tsd
      JOIN switch_port sp ON (tsd.target_type = 4 OR tsd.target_type = 5 OR
tsd.target_type = 6) AND tsd.target_id = sp.id
   JOIN switch_info vs ON sp.virtual_switch_id = vs.id
   JOIN pm_data_collector ON pm_data_collector.id = tsd.collector_id
   JOIN measure ON measure.id = tsd.measure_id
UNION ALL
SELECT 0 as device_id, cast (de.ip_address as varchar(255)) AS device_ip,
                    tsd.target_type, de.id AS target_id,
                    cast (de.physical_switch_name as text) AS target_name,
                    measure.measure_type AS collectible_type,
                    tsd.measure_id AS collectible_id, tsd.collector_id,
                    pdc.name AS collector_name,
                    (measure.name::text || '.'::text) || tsd.measure_index::text
AS collectible_name,
                    measure.detail AS collectible_detail, tsd.value,
                    tsd.time_in_seconds, tsd.measure_index
                   FROM time_series_data_info tsd
              JOIN switch_info de ON tsd.target_id = de.id
         JOIN pm_data_collector pdc ON pdc.id = tsd.collector_id
    JOIN measure ON measure.id = tsd.measure_id
   WHERE tsd.target_type = 3;
```

TRILL_INFO

```
create or replace view TRILL_INFO as
select distinct
    TRILL.ID,
    VCS_DEVICE.DEVICE_ID as VCS_DEVICE_ID,
    TRILL.CLUSTER_ME_ID,
    TRILL.COST,
    TRILL.TYPE as LINK_TYPE,
    TRILL.MISSING,
    TRILL.TRUNKED,
    TRILL.SOURCE_DOMAIN_ID,
    TRILL.SOURCE_PORT_NUMBER,
    TRILL.SOURCE_PORT_NAME as SOURCE_SWITCH_PORT_NAME,
    TRILL.SOURCE_ME_ID,
    SOURCE_DEVICE.DEVICE_ID AS SOURCE_DEVICE_ID,
    TRILL.DEST_DOMAIN_ID,
    TRILL.DEST_PORT_NUMBER,
    TRILL.DEST_PORT_NAME as DEST_SWITCH_PORT_NAME,
    TRILL.DEST_ME_ID,
    DEST_DEVICE.DEVICE_ID AS DEST_DEVICE_ID
from
    TRILL,
    device VCS_DEVICE,
    device SOURCE_DEVICE,
    VIRTUAL_SWITCH SOURCE_VIRTUAL_SWITCH,
    device DEST_DEVICE,
    VIRTUAL_SWITCH DEST_VIRTUAL_SWITCH
where
    SOURCE_DEVICE.MANAGED_ELEMENT_ID = TRILL.SOURCE_ME_ID and
    DEST_DEVICE.MANAGED_ELEMENT_ID = TRILL.DEST_ME_ID and
    VCS_DEVICE.MANAGED_ELEMENT_ID = TRILL.CLUSTER_ME_ID and
    SOURCE_VIRTUAL_SWITCH.MANAGED_ELEMENT_ID = TRILL.SOURCE_ME_ID and
    DEST_VIRTUAL_SWITCH.MANAGED_ELEMENT_ID = TRILL.DEST_ME_ID;
```

TRILL_TRUNK_INFO

```
create or replace view TRILL_TRUNK_INFO as
select
    TRILL_TRUNK_GROUP.ID,
    TRILL_TRUNK_GROUP.ME_ID,
    TRILL_TRUNK_GROUP.MASTER_PORT_NUMBER,
    TRILL_TRUNK_MEMBER.PORT_NUMBER as MEMBER_PORT_NUMBER,
    MEMBER_DEVICE.DEVICE_ID,
    INTERFACE.INTERFACE_ID,
    VCS_CLUSTER_MEMBER.CLUSTER_ME_ID,
    CLUSTER_DEVICE.DEVICE_ID as CLUSTER_DEVICE_ID
from
    TRILL_TRUNK_GROUP
    inner join
      TRILL_TRUNK_MEMBER on
      TRILL_TRUNK_MEMBER.GROUP_ID = TRILL_TRUNK_GROUP.ID
    inner join
      DEVICE as MEMBER_DEVICE on
      MEMBER_DEVICE.MANAGED_ELEMENT_ID = TRILL_TRUNK_GROUP.ME_ID
    left outer join
      INTERFACE on
      INTERFACE.DEVICE_ID = MEMBER_DEVICE.DEVICE_ID and
      INTERFACE.IDENTIFIER =  TRILL_TRUNK_MEMBER.PORT_NUMBER
    left outer join
      VCS_CLUSTER_MEMBER on
      VCS_CLUSTER_MEMBER.MEMBER_ME_ID = TRILL_TRUNK_GROUP.ME_ID
    left outer join
      DEVICE as CLUSTER_DEVICE on
      CLUSTER_DEVICE.MANAGED_ELEMENT_ID = VCS_CLUSTER_MEMBER.CLUSTER_ME_ID;
```

USER_ROLE_RESOURCE_INFO

```
create or replace view USER_ROLE_RESOURCE_INFO as
select
  RESOURCE_GROUP.ID RESOURCE_GROUP_ID,
  RESOURCE_GROUP.NAME RESOURCE_GROUP_NAME,
  ROLE.ID ROLE_ID,
  ROLE.NAME ROLE_NAME,
  USER_.NAME USER_NAME
from
  USER_,
  RESOURCE_GROUP,
  ROLE,
  USER_RESOURCE_MAP,
  USER_ROLE_MAP
where
  USER_ROLE_MAP.USER_NAME = USER_.NAME
  and USER_ROLE_MAP.ROLE_ID = ROLE.ID
  and USER_RESOURCE_MAP.RESOURCE_GROUP_ID = RESOURCE_GROUP.ID
  and USER_RESOURCE_MAP.USER_NAME = USER_.NAME;
```

VIRTUAL_FCOE_PORT_INFO

```
create or replace view VIRTUAL_FCOE_PORT_INFO as
select
    VIRTUAL_FCOE_PORT.ID,
```

```
    VIRTUAL_FCOE_PORT.VIRTUAL_SWITCH_ID,
    VIRTUAL_FCOE_PORT.PORT_WWN,
    VIRTUAL_FCOE_PORT.PORT_SPEED,
    VIRTUAL_FCOE_PORT.PORT_TYPE,
    VIRTUAL_FCOE_PORT.ENABLED,
    VIRTUAL_FCOE_PORT.STATUS,
    VIRTUAL_FCOE_PORT.TRUNK_INDEX,
    VIRTUAL_FCOE_PORT.PORT_NUMBER,
    VIRTUAL_FCOE_PORT.NAME,
    VIRTUAL_FCOE_PORT.SLOT_NUMBER,
    VIRTUAL_FCOE_PORT.VLAN_ID,
    VIRTUAL_FCOE_PORT.DEVICE_COUNT,
    VIRTUAL_FCOE_PORT.PEER_MAC,
    VIRTUAL_SWITCH.WWN as VIRTUAL_SWITCH_WWN,
    VIRTUAL_SWITCH.ROLE as SWITCH_ROLE,
    VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID as VIRTUAL_FABRIC_ID,
    VIRTUAL_SWITCH.DOMAIN_ID as DOMAIN_ID,
    VIRTUAL_SWITCH.INTEROP_MODE as INTEROP_MODE,
    VIRTUAL_SWITCH.MANAGEMENT_STATE,
    VIRTUAL_SWITCH.MONITORED,
    CORE_SWITCH.TYPE as SWITCH_TYPE,
    CORE_SWITCH.FIRMWARE_VERSION as FIRMWARE_VERSION,
    CORE_SWITCH.IP_ADDRESS as IP_ADDRESS,
    CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN,
    CORE_SWITCH.MODEL as SWITCH_MODEL,
    CORE_SWITCH_DETAILS.MODEL_NUMBER as SWITCH_MODEL_NUMBER
from
    VIRTUAL_FCOE_PORT, CORE_SWITCH, VIRTUAL_SWITCH, CORE_SWITCH_DETAILS
where
    VIRTUAL_FCOE_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID and
    VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID and
    CORE_SWITCH_DETAILS.CORE_SWITCH_ID = CORE_SWITCH.ID;
```

VIRTUAL_PORT_WWN_DETAILS_INFO

```
create or replace view VIRTUAL_PORT_WWN_DETAILS_INFO as
select distinct
    VIRTUAL_PORT_WWN_DETAILS.SWITCH_ID,
    VIRTUAL_PORT_WWN_DETAILS.SWITCH_PORT_NUMBER,
    VIRTUAL_PORT_WWN_DETAILS.SLOT_NUMBER,
    coalesce(CS1.IP_ADDRESS, CS2.IP_ADDRESS, UDDD.IP_ADDRESS) as IP_ADDRESS,
    coalesce(VS1.NAME, VS2.NAME, UDDD.NAME) as SWITCH_NAME,
    coalesce(VS1.WWN, VS2.WWN) as SWITCH_WWN,
    VIRTUAL_PORT_WWN_DETAILS.AG_NODE_WWN,
    VIRTUAL_PORT_WWN_DETAILS.AG_PORT_NUMBER,
    VIRTUAL_PORT_WWN_DETAILS.STATUS,
    VIRTUAL_PORT_WWN_DETAILS.TYPE,
    VIRTUAL_PORT_WWN_DETAILS.USER_VPWWN,
    VIRTUAL_PORT_WWN_DETAILS.AUTO_VPWWN,
    VIRTUAL_PORT_WWN_DETAILS.DEVICE_PORT_WWN,
    coalesce(SP1.ID, SP2.ID) as SWITCH_PORT_ID,
    coalesce(SP1.WWN, SP2.WWN) as PORT_WWN,
    coalesce(SP1.TYPE, SP2.TYPE) AS PORT_TYPE,
    coalesce(SP1.NAME, SP2.NAME) as PORT_NAME
from
    VIRTUAL_PORT_WWN_DETAILS
        left outer join VIRTUAL_SWITCH VS1
            on (VIRTUAL_PORT_WWN_DETAILS.AG_PORT_NUMBER = -1
                and VIRTUAL_PORT_WWN_DETAILS.SWITCH_ID = VS1.ID)
```

```
        left outer join VIRTUAL_SWITCH VS2
            on VIRTUAL_PORT_WWN_DETAILS.AG_NODE_WWN = VS2.WWN
        left outer join CORE_SWITCH CS1
            on VS1.CORE_SWITCH_ID = CS1.ID
        left outer join CORE_SWITCH CS2
            on VS2.CORE_SWITCH_ID = CS2.ID
        left outer join SWITCH_PORT SP1
            on (SP1.VIRTUAL_SWITCH_ID=VS1.ID
                and VIRTUAL_PORT_WWN_DETAILS.SLOT_NUMBER = SP1.SLOT_NUMBER
               and VIRTUAL_PORT_WWN_DETAILS.SWITCH_PORT_NUMBER = SP1.PORT_NUMBER
                and SP1.TYPE NOT IN ('GigE-Port','TE-Port'))
        left outer join SWITCH_PORT SP2
            on (SP2.VIRTUAL_SWITCH_ID=VS2.ID
                and VIRTUAL_PORT_WWN_DETAILS.AG_PORT_NUMBER = SP2.PORT_NUMBER
                and SP2.TYPE NOT IN ('GigE-Port','TE-Port'))
        left outer join USER_DEFINED_DEVICE_DETAIL UDDD
            on VIRTUAL_PORT_WWN_DETAILS.AG_NODE_WWN = UDDD.WWN;
```

VM_ADDRESS_INFO

```
create or replace view VM_ADDRESS_INFO AS
 select
    DECODE(VM_VIRTUAL_ETHERNET_ADAPTER.MAC_ADDRESS::TEXT, 'HEX'::TEXT) AS
MAC_ADDRESS,
     VM_VIRTUAL_MACHINE.NAME AS VM_NAME,
     DECODE(VM_VIRTUAL_MACHINE.IP_ADDRESS::TEXT, 'HEX'::TEXT) AS VM_ADDRESS,
     VM_VCENTER_MEMBER.HOST_NAME AS VM_HOST_NAME,
     DECODE(VM_VIRTUAL_MACHINE.IP_ADDRESS::TEXT, 'HEX'::TEXT) AS VM_HOST_ADDRESS,
     VM_VIRTUAL_ETHERNET_ADAPTER.VIRTUAL_MACHINE_ID AS VM_ID,
     VM_VIRTUAL_MACHINE.HOST_ID AS VM_HOST_ID

 FROM
    VM_VIRTUAL_MACHINE,
    VM_VIRTUAL_ETHERNET_ADAPTER,
    VM_VCENTER_MEMBER

  WHERE
    VM_VIRTUAL_MACHINE.ID = VM_VIRTUAL_ETHERNET_ADAPTER.VIRTUAL_MACHINE_ID
    AND VM_VIRTUAL_MACHINE.HOST_ID = VM_VCENTER_MEMBER.VM_HOST_ID;
```

VLAN_INT_CLASSIFIER_INFO

```
CREATE VIEW vlan_int_classifier_info AS
    select VLAN_INTERFACE_RELATION.VLAN_INTERFACE_RELATION_ID,
        VLAN_INTERFACE_RELATION.VLAN_DB_ID,
        VLAN_INTERFACE_RELATION.INTERFACE_ID,
        VLAN_INT_C_TAG_RELATION.C_TAG_ID,
        MAC_GROUP.NAME,
        MAC_GROUP.MAC_GROUP_ID,
        MAC_GROUP.TYPE,
        MAC_GROUP_MEMBER.MAC_ADDRESS,
        MAC_GROUP_MEMBER.MASK,
        MAC_GROUP.ID AS MAC_GROUP_DB_ID,
        DEVICE.DEVICE_ID
from INTERFACE ,DEVICE ,PORT_VLAN
         left outer join VLAN_INTERFACE_RELATION  on
VLAN_INTERFACE_RELATION.VLAN_DB_ID = PORT_VLAN.VLAN_DB_ID
```

```
        left outer join VLAN_INT_MAC_GROUP_RELATION TEMP_MAC_RELATION on
VLAN_INTERFACE_RELATION.VLAN_INTERFACE_RELATION_ID =
TEMP_MAC_RELATION.VLAN_INTERFACE_RELATION_ID
        left outer join VLAN_INT_C_TAG_RELATION on
VLAN_INT_C_TAG_RELATION.VLAN_INTERFACE_RELATION_ID =
VLAN_INTERFACE_RELATION.VLAN_INTERFACE_RELATION_ID
        left outer join MAC_GROUP on TEMP_MAC_RELATION.MAC_GROUP_DB_ID =
MAC_GROUP.ID
        left outer join MAC_GROUP_MEMBER on MAC_GROUP_MEMBER.MAC_GROUP_DB_ID =
MAC_GROUP.ID
        left outer join DEVICE_MAC_GROUP_MAPPING  on
DEVICE_MAC_GROUP_MAPPING.MAC_GROUP_DB_ID  =  MAC_GROUP.ID
where VLAN_INTERFACE_RELATION.INTERFACE_ID = INTERFACE.INTERFACE_ID and
INTERFACE.DEVICE_ID =  DEVICE.DEVICE_ID;
```

VM_CONNECTIVITY_INFO

This view combines fabric and VM information to derive end to end connectivity information for the VM.

```
create or replace view VM_CONNECTIVITY_INFO as
select
  VM_VCENTER.HOST AS VCENTER_HOST,
  DEVICE_PORT.SWITCH_PORT_WWN,
  DEVICE_PORT.DOMAIN_ID,
  device_port.id as device_port_id,
  DEVICE_PORT.NUMBER,
  CORE_SWITCH.IP_ADDRESS,
  CORE_SWITCH.NAME AS CORE_NAME,
  VM_VCENTER.ID AS VCENTER_ID,
  DEVICE_ENCLOSURE.ID AS HOST_DB_ID,
  DEVICE_ENCLOSURE.IP_ADDRESS AS HYPERVISOR_HOST,
  VM_VIRTUAL_MACHINE.ID as VM_ID,
  VM_VIRTUAL_MACHINE.IP_ADDRESS AS VM_IP_ADDRESS,
  VM_VIRTUAL_MACHINE.HOSTNAME AS VM_HOST_NAME,
  VM_VIRTUAL_MACHINE.UUID AS VM_UUID,
  VM_VIRTUAL_MACHINE.NAME AS VM_NAME,
  VM_PATH.NAME AS PATH_NAME,
  VM_PATH.HBA_PORT AS ADAPTER_PORT_WWN,
  VM_PATH.TARGET_PORT AS TARGET_PORT_WWN,
  VM_STORAGE.NAME AS LUN_CAN_NAME,
  VM_PATH.FS_TYPE,
  VM_VIRTUAL_MACHINE.HYPERVISOR_VM_ID,
  DEVICE_ENCLOSURE.MANAGED_ELEMENT_ID AS HOST_ME_ID,
  DEVICE_ENCLOSURE.IP_ADDRESS AS HOST_IP_ADDRESS,
  DEVICE_ENCLOSURE.HOST_NAME AS HYPERVISOR_HOST_NAME,
  FABRIC.NAME AS FABRIC_NAME,
  VIRTUAL_SWITCH.NAME AS VIRTUAL_NAME,
  SWITCH_PORT.STATUS AS SWITCH_PORT_STATUS,
  SWITCH_PORT.ID as SWITCH_PORT_ID,
  SWITCH_PORT.PORT_ID,
  SWITCH_PORT.PORT_NUMBER,
  SWITCH_PORT.SLOT_NUMBER,
  USER_DEFINED_DEVICE_DETAIL.NAME AS ADAPTER_PORT_NAME,
  VM_PATH.FABRIC_ID,
  VM_PATH.VM_PORT_WWN,
  VM_STORAGE.MODEL,
  VM_STORAGE.VENDOR
from
```

```
  DEVICE_PORT
    left join USER_DEFINED_DEVICE_DETAIL
      on DEVICE_PORT.WWN = USER_DEFINED_DEVICE_DETAIL.WWN,
  CORE_SWITCH,
  SWITCH_PORT,
  VIRTUAL_SWITCH,
  DEVICE_NODE,
  FABRIC,
  VM_STORAGE,
  VM_PATH,
  DEVICE_ENCLOSURE,
  VM_VIRTUAL_MACHINE,
  VM_VCENTER,
  VM_DATA_CENTER,
  VM_HOST
where
  VM_PATH.HBA_PORT = DEVICE_PORT.WWN
  and VM_PATH.VM_ID = VM_VIRTUAL_MACHINE.ID
  and VM_PATH.STORAGE_ID = VM_STORAGE.ID
  and VM_STORAGE.HOST_ID = DEVICE_ENCLOSURE.ID
  and DEVICE_ENCLOSURE.ID = VM_HOST.DEVICE_ENCLOSURE_ID
  and DEVICE_ENCLOSURE.ID = VM_VIRTUAL_MACHINE.HOST_ID
  and VM_HOST.VM_DATACENTER_ID = VM_DATA_CENTER.ID
  and VM_DATA_CENTER.VCENTER_ID = VM_VCENTER.ID
  and DEVICE_PORT.SWITCH_PORT_WWN = SWITCH_PORT.WWN
  and SWITCH_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
  and VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID
  and DEVICE_PORT.NODE_ID = DEVICE_NODE.ID
  and DEVICE_NODE.FABRIC_ID = FABRIC.ID

union all

select
  VM_VCENTER.HOST AS VCENTER_HOST,
  DEVICE_PORT.SWITCH_PORT_WWN,
  DEVICE_PORT.DOMAIN_ID,
  device_port.id as device_port_id,
  DEVICE_PORT.NUMBER,
  CORE_SWITCH.IP_ADDRESS,
  CORE_SWITCH.NAME as CORE_NAME,
  VM_VCENTER.ID as VCENTER_ID,
  DEVICE_ENCLOSURE.ID AS HOST_DB_ID,
  DEVICE_ENCLOSURE.IP_ADDRESS as HYPERVISOR_HOST,
  VM_VIRTUAL_MACHINE.ID as VM_ID,
  VM_VIRTUAL_MACHINE.IP_ADDRESS AS VM_IP_ADDRESS,
  VM_VIRTUAL_MACHINE.HOSTNAME AS VM_HOST_NAME,
  VM_VIRTUAL_MACHINE.UUID as VM_UUID,
  VM_VIRTUAL_MACHINE.NAME as VM_NAME,
  VM_PATH.NAME as PATH_NAME,
  VM_PATH.HBA_PORT as ADAPTER_PORT_WWN,
  VM_PATH.TARGET_PORT as TARGET_PORT_WWN,
  VM_STORAGE.NAME as LUN_CAN_NAME,
  VM_PATH.FS_TYPE,
  VM_VIRTUAL_MACHINE.HYPERVISOR_VM_ID,
  DEVICE_ENCLOSURE.MANAGED_ELEMENT_ID AS HOST_ME_ID,
  DEVICE_ENCLOSURE.IP_ADDRESS AS HOST_IP_ADDRESS,
  DEVICE_ENCLOSURE.HOST_NAME AS HYPERVISOR_HOST_NAME,
  FABRIC.NAME as FABRIC_NAME,
  VIRTUAL_SWITCH.NAME as VIRTUAL_NAME,
  SWITCH_PORT.STATUS as SWITCH_PORT_STATUS,
```

```
  SWITCH_PORT.ID as SWITCH_PORT_ID,
  SWITCH_PORT.PORT_ID,
  SWITCH_PORT.PORT_NUMBER,
  SWITCH_PORT.SLOT_NUMBER,
  USER_DEFINED_DEVICE_DETAIL.NAME as ADAPTER_PORT_NAME,
  VM_PATH.FABRIC_ID,
  VM_PATH.VM_PORT_WWN,
  VM_STORAGE.MODEL,
  VM_STORAGE.VENDOR
from
  DEVICE_PORT
    LEFT JOIN USER_DEFINED_DEVICE_DETAIL
      on DEVICE_PORT.WWN = USER_DEFINED_DEVICE_DETAIL.WWN,
  CORE_SWITCH,
  SWITCH_PORT,
  VIRTUAL_SWITCH,
  DEVICE_NODE,
  FABRIC,
  DEVICE_PORT_MAC_ADDRESS_MAP,
  GIGE_PORT,
  VM_STORAGE,
  VM_PATH,
  DEVICE_ENCLOSURE,
  VM_VIRTUAL_MACHINE,
  VM_VCENTER,
  VM_DATA_CENTER,
  VM_HOST
where
  VM_PATH.HBA_PORT = DEVICE_PORT.WWN
  and VM_PATH.VM_ID = VM_VIRTUAL_MACHINE.ID
  and VM_PATH.STORAGE_ID = VM_STORAGE.ID
  and VM_STORAGE.HOST_ID = DEVICE_ENCLOSURE.ID
  and DEVICE_ENCLOSURE.ID = VM_HOST.DEVICE_ENCLOSURE_ID
  and DEVICE_ENCLOSURE.ID = VM_VIRTUAL_MACHINE.HOST_ID
  and VM_HOST.VM_DATACENTER_ID = VM_DATA_CENTER.ID
  and VM_DATA_CENTER.VCENTER_ID = VM_VCENTER.ID
  and DEVICE_PORT.ID = DEVICE_PORT_MAC_ADDRESS_MAP.DEVICE_PORT_ID
  and DEVICE_PORT_MAC_ADDRESS_MAP.MAC_ADDRESS::TEXT =
GIGE_PORT.REMOTE_MAC_ADDRESS::TEXT
  and GIGE_PORT.SWITCH_PORT_ID = SWITCH_PORT.ID
  and SWITCH_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
  and VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID
  and DEVICE_PORT.NODE_ID = DEVICE_NODE.ID
  and DEVICE_NODE.FABRIC_ID = FABRIC.ID;

comment on view VM_CONNECTIVITY_INFO is
'Combine fabric and VM info to derive end to end connectivity information for the
VM';
```

VM_NETWORK_CONNECTIVITY_INFO

```
CREATE VIEW vm_network_connectivity_info AS
    select VM_VIRTUAL_ETHERNET_ADAPTER.ID as VNIC_ID,
VM_VIRTUAL_ETHERNET_ADAPTER.MAC_ADDRESS,VM_VIRTUAL_ETHERNET_ADAPTER.IP_ADDRESS as
VM_IP_ADDRESS, VM_VIRTUAL_ETHERNET_ADAPTER.DISPLAY_LABEL,
VM_VIRTUAL_ETHERNET_ADAPTER.PORT_GROUP_NAME, VM_VIRTUAL_MACHINE.ID as VM_ID,
VM_VIRTUAL_MACHINE.NAME as VIRTUAL_MACHINE_NAME, VM_VIRTUAL_MACHINE.HOST_ID as
HOST_ID, VM_VCENTER_MEMBER.HOST_NAME,
```

```
VM_HOST.CLUSTER_NAME, VM_DATA_CENTER.ID as DATA_CENTER_ID,
VM_VIRTUAL_ETHERNET_ADAPTER.VM_STD_VSWITCH_PORT_GROUP_ID as STD_PORT_GROUP_ID,
VM_VIRTUAL_ETHERNET_ADAPTER.VM_DV_PORT_ID as DV_PORT_ID,
VM_STD_VSWITCH_PORT_GROUP.NAME as UPLINK_PORT_GROUP_NAME,
VM_STANDARD_VIRTUAL_SWITCH.NAME as VM_SWITCH_NAME, VM_PHYSICAL_NIC.MAC_ADDRESS as
PNIC_MAC,
VM_HOST_END_DEV_CONNECTIVITY.INTERFACE_ID, INTERFACE.NAME as INTERFACE_NAME,
INTERFACE.DEVICE_ID as SWITCH_ID, DEVICE.IP_ADDRESS as SWITCH_IP, DEVICE.SYS_NAME
as SWITCH_NAME,
DEVICE.OPER_STATUS as SWITCH_STATUS, CLUSTER_DEVICE.VCS_LICENSED,
PORT_PROFILE.NAME as PORT_PROFILE_NAME, PROFILE_DOMAINS.DOMAIN_NAMES as
PORT_PROFILE_DOMAIN_NAMES, PROFILE_VLAN_MAP.VLAN as PORT_PROFILE_VLAN,
VM_NETWORK_SETTINGS.VLAN_IDS as PORT_GROUP_VLAN

from VM_VIRTUAL_MACHINE, VM_HOST, VM_DATA_CENTER, VM_VCENTER_MEMBER,
VM_VIRTUAL_ETHERNET_ADAPTER
join VM_STD_VSWITCH_PORT_GROUP on
VM_VIRTUAL_ETHERNET_ADAPTER.VM_STD_VSWITCH_PORT_GROUP_ID =
VM_STD_VSWITCH_PORT_GROUP.ID
left join VM_STANDARD_VIRTUAL_SWITCH on VM_STANDARD_VIRTUAL_SWITCH.ID =
VM_STD_VSWITCH_PORT_GROUP.VM_STANDARD_VIRTUAL__SWITCH_ID
left join VM_PHYSICAL_NIC on VM_PHYSICAL_NIC.VM_STANDARD_VIRTUAL_SWITCH_ID =
VM_STANDARD_VIRTUAL_SWITCH.ID join VM_HOST_END_DEV_CONNECTIVITY on
VM_HOST_END_DEV_CONNECTIVITY.VM_PHYSICAL_NIC_ID = VM_PHYSICAL_NIC.ID
left join INTERFACE on INTERFACE.INTERFACE_ID =
VM_HOST_END_DEV_CONNECTIVITY.INTERFACE_ID
left join DEVICE on DEVICE.DEVICE_ID = INTERFACE.DEVICE_ID
left join VCS_CLUSTER_MEMBER on VCS_CLUSTER_MEMBER.MEMBER_ME_ID =
DEVICE.MANAGED_ELEMENT_ID
left join DEVICE as CLUSTER_DEVICE on CLUSTER_DEVICE.MANAGED_ELEMENT_ID =
VCS_CLUSTER_MEMBER.CLUSTER_ME_ID
left join PORT_PROFILE_INTERFACE_MAP on PORT_PROFILE_INTERFACE_MAP.INTERFACE_ID =
INTERFACE.INTERFACE_ID
left join PORT_PROFILE on PORT_PROFILE.ID = PORT_PROFILE_INTERFACE_MAP.PROFILE_ID
left join (select PORT_PROFILE_DOMAIN_MAP.PROFILE_ID,
array_to_string(array_agg(PORT_PROFILE_DOMAIN.NAME), ',') DOMAIN_NAMES from
PORT_PROFILE_DOMAIN_MAP join PORT_PROFILE_DOMAIN on
PORT_PROFILE_DOMAIN_MAP.PROFILE_DOMAIN_ID = PORT_PROFILE_DOMAIN.ID group by
PORT_PROFILE_DOMAIN_MAP.PROFILE_ID) PROFILE_DOMAINS on PROFILE_DOMAINS.PROFILE_ID
= PORT_PROFILE.ID
left join (select PROFILE_ID, array_agg(VLANID)::varchar as VLAN from
PORT_PROFILE_VLAN_MAP group by PROFILE_ID) PROFILE_VLAN_MAP on
PROFILE_VLAN_MAP.PROFILE_ID = PORT_PROFILE.ID
left join VM_NETWORK_SETTINGS on VM_NETWORK_SETTINGS.VM_STD_VSWITCH_PORT_GROUP_ID
= VM_VIRTUAL_ETHERNET_ADAPTER.VM_STD_VSWITCH_PORT_GROUP_ID
where VM_VIRTUAL_ETHERNET_ADAPTER.VIRTUAL_MACHINE_ID = VM_VIRTUAL_MACHINE.ID and
VM_VIRTUAL_MACHINE.HOST_ID = VM_VCENTER_MEMBER.VM_HOST_ID and
VM_VIRTUAL_MACHINE.HOST_ID = VM_HOST.DEVICE_ENCLOSURE_ID and
VM_HOST.VM_DATACENTER_ID = VM_DATA_CENTER.ID

union

select VNIC_DV_PORT.VNIC_ID as VNIC_ID,
VNIC_DV_PORT.MAC_ADDRESS,VNIC_DV_PORT.VM_IP_ADDRESS,VNIC_DV_PORT.DISPLAY_LABEL,
VNIC_DV_PORT.PORT_GROUP_NAME, VNIC_DV_PORT.VM_ID,
VNIC_DV_PORT.VIRTUAL_MACHINE_NAME, VNIC_DV_PORT.HOST_ID, VNIC_DV_PORT.HOST_NAME,
VNIC_DV_PORT.HOST_NAME, VNIC_DV_PORT.DATA_CENTER_ID,
VNIC_DV_PORT.VM_STD_VSWITCH_PORT_GROUP_ID as STD_PORT_GROUP_ID,
VNIC_DV_PORT.DV_PORT_ID, PNIC_DV_PORT.PORT_GROUP_NAME as UPLINK_PORT_GROUP_NAME,
```

```
VNIC_DV_PORT.SWITCH_NAME as VM_SWITCH_NAME, PNIC_DV_PORT.PNIC_MAC,
VM_HOST_END_DEV_CONNECTIVITY.INTERFACE_ID, INTERFACE.NAME as INTERFACE_NAME,
INTERFACE.DEVICE_ID as SWITCH_ID, DEVICE.IP_ADDRESS as SWITCH_IP, DEVICE.SYS_NAME
as SWITCH_NAME, DEVICE.OPER_STATUS as SWITCH_STATUS, CLUSTER_DEVICE.VCS_LICENSED,
PORT_PROFILE.NAME as PORT_PROFILE_NAME,
PROFILE_DOMAINS.DOMAIN_NAMES as PORT_PROFILE_DOMAIN_NAMES, PROFILE_VLAN_MAP.VLAN
as PORT_PROFILE_VLAN, VM_NETWORK_SETTINGS.VLAN_IDS as PORT_GROUP_VLAN
from

(select VNIC.ID as VNIC_ID, VNIC.MAC_ADDRESS,VNIC.IP_ADDRESS as VM_IP_ADDRESS,
VNIC.DISPLAY_LABEL, VNIC.PORT_GROUP_NAME, VNIC.VM_STD_VSWITCH_PORT_GROUP_ID,
VM_VIRTUAL_MACHINE.ID as VM_ID,
VM_VIRTUAL_MACHINE.NAME as VIRTUAL_MACHINE_NAME, VM_VIRTUAL_MACHINE.HOST_ID as
HOST_ID, VM_VCENTER_MEMBER.HOST_NAME, VM_HOST.CLUSTER_NAME, VM_DATA_CENTER.ID as
DATA_CENTER_ID,
 DVPORT.ID as DV_PORT_ID, DVPORT.VM_DV_SWITCH_ID, VM_DV_SWITCH.NAME as
SWITCH_NAME
from VM_VIRTUAL_MACHINE, VM_VCENTER_MEMBER, VM_HOST, VM_DATA_CENTER,
VM_VIRTUAL_ETHERNET_ADAPTER VNIC, VM_DV_PORT DVPORT, VM_DV_SWITCH
where VNIC.VM_DV_PORT_ID = DVPORT.ID and VNIC.VIRTUAL_MACHINE_ID =
VM_VIRTUAL_MACHINE.ID and
VM_VIRTUAL_MACHINE.HOST_ID = VM_VCENTER_MEMBER.VM_HOST_ID and
DVPORT.VM_DV_SWITCH_ID = VM_DV_SWITCH.ID and VM_VIRTUAL_MACHINE.HOST_ID =
VM_HOST.DEVICE_ENCLOSURE_ID AND
VM_HOST.VM_DATACENTER_ID = VM_DATA_CENTER.ID) as VNIC_DV_PORT
left join VM_DV_PORT on VM_DV_PORT.ID = VNIC_DV_PORT.DV_PORT_ID
left join VM_NETWORK_SETTINGS on VM_NETWORK_SETTINGS.VM_DV_PORT_GROUP_ID =
VM_DV_PORT.VM_DV_PORT_GROUP_ID,

(select DVPORT.VM_DV_SWITCH_ID, DVPORTGROUP.ID as DV_PORT_GROUP_ID,
DVPORTGROUP.NAME as PORT_GROUP_NAME, PNIC.ID as PNIC_ID, PNIC.MAC_ADDRESS as
PNIC_MAC
from VM_PHYSICAL_NIC PNIC, VM_DV_PORT DVPORT, VM_DV_PORT_GROUP DVPORTGROUP
where PNIC.VM_DV_PORT_ID = DVPORT.ID and DVPORT.VM_DV_PORT_GROUP_ID =
DVPORTGROUP.ID) as PNIC_DV_PORT
join VM_HOST_END_DEV_CONNECTIVITY on
VM_HOST_END_DEV_CONNECTIVITY.VM_PHYSICAL_NIC_ID = PNIC_DV_PORT.PNIC_ID
left join INTERFACE on INTERFACE.INTERFACE_ID =
VM_HOST_END_DEV_CONNECTIVITY.INTERFACE_ID
left join DEVICE on DEVICE.DEVICE_ID = INTERFACE.DEVICE_ID
left join VCS_CLUSTER_MEMBER on VCS_CLUSTER_MEMBER.MEMBER_ME_ID =
DEVICE.MANAGED_ELEMENT_ID
left join DEVICE as CLUSTER_DEVICE on CLUSTER_DEVICE.MANAGED_ELEMENT_ID =
VCS_CLUSTER_MEMBER.CLUSTER_ME_ID
left join PORT_PROFILE_INTERFACE_MAP on PORT_PROFILE_INTERFACE_MAP.INTERFACE_ID =
INTERFACE.INTERFACE_ID
left join PORT_PROFILE on PORT_PROFILE.ID = PORT_PROFILE_INTERFACE_MAP.PROFILE_ID
left join (select PORT_PROFILE_DOMAIN_MAP.PROFILE_ID,
array_to_string(array_agg(PORT_PROFILE_DOMAIN.NAME), ',') DOMAIN_NAMES from
PORT_PROFILE_DOMAIN_MAP join PORT_PROFILE_DOMAIN on
PORT_PROFILE_DOMAIN_MAP.PROFILE_DOMAIN_ID = PORT_PROFILE_DOMAIN.ID group by
PORT_PROFILE_DOMAIN_MAP.PROFILE_ID) PROFILE_DOMAINS on PROFILE_DOMAINS.PROFILE_ID
= PORT_PROFILE.ID
left join (select PROFILE_ID, array_agg(VLANID)::varchar as VLAN from
PORT_PROFILE_VLAN_MAP group by PROFILE_ID) PROFILE_VLAN_MAP on
PROFILE_VLAN_MAP.PROFILE_ID = PORT_PROFILE.ID

where VNIC_DV_PORT.VM_DV_SWITCH_ID = PNIC_DV_PORT.VM_DV_SWITCH_ID;
```

VM_DATASTORE_DETAILS_INFO

```
create or replace view VM_DATASTORE_DETAILS_INFO as
select vm_virtual_machine_datastore_map.virtual_machine_id,
vm_virtual_machine_datastore_map.vm_datastore_details_id,
vm_datastore_details.datacenter_id,
vm_virtual_machine_datastore_map.provisioned_storage,
vm_virtual_machine_datastore_map.not_shared_storage,
vm_virtual_machine_datastore_map.used_storage,
vm_datastore_details.name, vm_datastore_details.accessible,
vm_datastore_details.status, vm_datastore_details.file_system_type,
vm_datastore_details.total_capacity, vm_datastore_details.free_space,
vm_datastore_details.last_update_time, vm_datastore_details.rdm_supported,
vm_datastore_details.perfile_thin_provisioning_supported,
vm_datastore_details.storage_iorm_supported,
vm_datastore_details.directory_hierarchy_supported, vm_datastore_details.location
from vm_virtual_machine_datastore_map, vm_datastore_details
where vm_virtual_machine_datastore_map.vm_datastore_details_id =
vm_datastore_details.id;
```

VM_EE_MONITOR_INFO

This view provides combined ee_monitor, ee_monitor_stats, device_port and device_node tables to get the EE Monitor information for vmplug-in.

```
create or replace view VM_EE_MONITOR_INFO as
select distinct
    EE_MONITOR.NAME,
    EE_MONITOR.SWITCH_PORT_ID,
    EE_MONITOR.SOURCE_PORT_ID,
    EE_MONITOR.DEST_PORT_ID,
    EE_MONITOR_STATS.TX,
    EE_MONITOR_STATS.RX,
    EE_MONITOR_STATS.CRCERRORS,
    EE_MONITOR_STATS.CREATION_TIME,
    SOURCE_PORT.PORT_ID as SID,
    DEST_PORT.PORT_ID as DID,
    SOURCE_NODE.WWN as SOURCE_DEVICE_WWN,
    SOURCE_PORT.WWN as SOURCE_PORT_WWN,
    DEST_NODE.WWN as DEST_DEVICE_WWN,
    DEST_PORT.WWN as DEST_PORT_WWN,
    SOURCE_NODE.FABRIC_ID as SOURCE_FABRIC_ID,
    DEST_NODE.FABRIC_ID as DEST_FABRIC_ID,
    SOURCE_PORT.DOMAIN_ID as SOURCE_SWITCH_DOMAIN_ID,
    DEST_PORT.DOMAIN_ID as DEST_SWITCH_DOMAIN_ID,
    VM_VIRTUAL_MACHINE.HYPERVISOR_VM_ID,
    VM_VIRTUAL_MACHINE.NAME as VM_NAME
from
    VM_PATH,
    VM_VIRTUAL_MACHINE,
    DEVICE_PORT as SOURCE_PORT,
    DEVICE_PORT as DEST_PORT,
    DEVICE_NODE as DEST_NODE,
    DEVICE_NODE as SOURCE_NODE,
    EE_MONITOR,
    EE_MONITOR_STATS
where
    VM_PATH.HBA_PORT::BPCHAR = SOURCE_PORT.WWN
```

```
    and VM_PATH.VM_ID = VM_VIRTUAL_MACHINE.ID
    and SOURCE_PORT.ID = EE_MONITOR.SOURCE_PORT_ID
    and EE_MONITOR.ID = EE_MONITOR_STATS.EE_MONITOR_ID
    and SOURCE_PORT.NODE_ID = SOURCE_NODE.ID
    and DEST_PORT.ID = EE_MONITOR.DEST_PORT_ID
    and DEST_PORT.NODE_ID = DEST_NODE.ID
    and EE_MONITOR_STATS.CREATION_TIME in (select MAX(CREATION_TIME) from
EE_MONITOR_STATS group by EE_MONITOR_ID);

comment on view VM_EE_MONITOR_INFO is
'Combined ee_monitor, ee_monitor_stats, device_port and device_node tables to get
the EE Monitor info for vmplug-in';
```

VM_HOST_INFO

```
CREATE VIEW vm_host_info AS
    select
   VM_DATA_CENTER.VCENTER_ID as VCENTER_ID,
   VM_HOST.DEVICE_ENCLOSURE_ID as HOST_ID,
   VM_HOST.VM_DATACENTER_ID as DATACENTER_ID,
   VM_HOST.NODE_WWN         as HOST_NODE_WWN,
   VM_HOST.HYPERVISOR_NAME,
   VM_HOST.HYPERVISOR_TYPE,
   VM_HOST.CPU_COUNT,
   VM_HOST.CPU_TYPE,
   VM_HOST.CPU_RESOURCES    as HOST_CPU_RESOURCES,
   VM_HOST.MEM_RESOURCES    as HOST_MEM_RESOURCES,
   VM_HOST.LICENSE_SERVER,
   VM_HOST.BOOT_TIME        as HOST_BOOT_TIME,
   VM_HOST.CLUSTER_NAME as CLUSTER_NAME,
   VM_VIRTUAL_MACHINE.ID                   as VM_ID,
   VM_VIRTUAL_MACHINE.HYPERVISOR_VM_ID,
   VM_VIRTUAL_MACHINE.NAME                 as VM_NAME,
   VM_VIRTUAL_MACHINE.DESCRIPTION          as VM_DESCRIPTION,
   VM_VIRTUAL_MACHINE.OS                   as VM_OS,
   VM_VIRTUAL_MACHINE.STATUS               as VM_STATUS,
   VM_VIRTUAL_MACHINE.VCPU_COUNT,
   VM_VIRTUAL_MACHINE.CPU_RESOURCES        as VM_CPU_RESOURCES,
   VM_VIRTUAL_MACHINE.MEM_RESOURCES        as VM_MEM_RESOURCES,
   VM_VIRTUAL_MACHINE.IP_ADDRESS           as VM_IP_ADDRESS,
   VM_VIRTUAL_MACHINE.HOSTNAME             as VM_HOSTNAME,
   VM_VIRTUAL_MACHINE.BOOT_TIME            as VM_BOOT_TIME,
   VM_VIRTUAL_MACHINE.DATASTORE_NAME,
   VM_VIRTUAL_MACHINE.DATASTORE_LOCATION,
   VM_VIRTUAL_MACHINE.NODE_WWN             as VM_NODE_WWN
from
   VM_DATA_CENTER,
   VM_HOST
      left join VM_VIRTUAL_MACHINE
         on VM_HOST.DEVICE_ENCLOSURE_ID = VM_VIRTUAL_MACHINE.HOST_ID
where
   VM_DATA_CENTER.ID = VM_HOST.VM_DATACENTER_ID;
```

VM_LUN_INFO

```
create or replace view VM_LUN_INFO as
select
   VM_STORAGE.HOST_ID,
```

```
   VM_STORAGE.ID                as LUN_ID,
   VM_STORAGE.NAME              as LUN_NAME,
   VM_STORAGE.TARGET_NODE,
   VM_STORAGE.VENDOR,
   VM_STORAGE.MODEL,
   VM_STORAGE.SERIAL_NUMBER,
   VM_STORAGE.TYPE,
   VM_STORAGE.CAPACITY,
   VM_STORAGE.STATUS            as LUN_STATUS,
   VM_STORAGE.PATH_POLICY,
   VM_STORAGE.ISCSI_TARGET_ADDRESS,
   VM_STORAGE.ISCSI_TARGET_PORT,
   VM_STORAGE.NAS_REMOTE_HOST,
   VM_STORAGE.NAS_REMOTE_PATH,
   VM_PATH.FS_TYPE,
   VM_PATH.ID               as PATH_ID,
   VM_PATH.VM_ID            as PATH_VM_ID,
   VM_PATH.NAME             as PATH_NAME,
   VM_PATH.FABRIC_ID,
   VM_PATH.HBA_PORT,
   VM_PATH.VM_PORT_WWN,
   VM_PATH.TARGET_PORT,
   VM_PATH.HBA_NODE,
   VM_PATH.VM_NODE_WWN,
   VM_PATH.TARGET_NODE      as PATH_TARGET_NODE,
   VM_PATH.HBA_NAME,
   VM_PATH.USAGE            as PATH_USAGE,
   VM_PATH.ENABLED          as PATH_ENABLED,
   VM_PATH.ACTIVE           as PATH_ACTIVE,
   VM_PATH.PREFERRED        as PATH_PREFERRED
from
   VM_STORAGE join VM_PATH on VM_STORAGE.ID = VM_PATH.STORAGE_ID;
```

VM_STATISTICS_INFO

This view gets the FC port statistics for the VM Connectivity data.

```
create or replace view VM_STATISTICS_INFO as
select distinct
    DEVICE_PORT.SWITCH_PORT_WWN,
    DEVICE_PORT.DOMAIN_ID,
    DEVICE_ENCLOSURE.IP_ADDRESS as HYPERVISOR_HOST,
    VM_PATH.HBA_PORT as ADAPTER_PORT_WWN,
    VM_VIRTUAL_MACHINE.HYPERVISOR_VM_ID,
    VM_VIRTUAL_MACHINE.NAME as VM_NAME,
    CORE_SWITCH.IP_ADDRESS,
    CORE_SWITCH.NAME as CORE_NAME,
    FC_PORT_STATS.TX,
    FC_PORT_STATS.RX,
    FC_PORT_STATS.TX_UTILIZATION,
    FC_PORT_STATS.RX_UTILIZATION,
    FC_PORT_STATS.SYNCLOSSES,
    FC_PORT_STATS.SIGNALLOSSES,
    FC_PORT_STATS.SEQUENCEERRORS,
    FC_PORT_STATS.INVALIDTRANSMISSIONS,
    FC_PORT_STATS.CRCERRORS,
    FC_PORT_STATS.CREATION_TIME,
    VIRTUAL_SWITCH.NAME as VIRTUAL_NAME,
    SWITCH_PORT.STATUS as SWITCH_PORT_STATUS,
```

```
    SWITCH_PORT.PORT_ID,
    SWITCH_PORT.PORT_NUMBER
from
    VM_STORAGE,
    VM_HOST,
    DEVICE_ENCLOSURE,
    VM_VIRTUAL_MACHINE,
    VM_PATH,
    DEVICE_PORT,
    SWITCH_PORT,
    CORE_SWITCH,
    FC_PORT_STATS,
    VIRTUAL_SWITCH
where
    VM_PATH.HBA_PORT::BPCHAR = DEVICE_PORT.WWN
    and VM_PATH.VM_ID = VM_VIRTUAL_MACHINE.ID
    and VM_PATH.STORAGE_ID = VM_STORAGE.ID
    and VM_STORAGE.HOST_ID = DEVICE_ENCLOSURE.ID
    and DEVICE_ENCLOSURE.ID = VM_HOST.DEVICE_ENCLOSURE_ID
    and DEVICE_ENCLOSURE.ID = VM_VIRTUAL_MACHINE.HOST_ID
    and DEVICE_PORT.SWITCH_PORT_WWN = SWITCH_PORT.WWN
    and SWITCH_PORT.ID = FC_PORT_STATS.PORT_ID
    and SWITCH_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
    and VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID
    and FC_PORT_STATS.CREATION_TIME in (select MAX(CREATION_TIME) from
FC_PORT_STATS group by PORT_ID)

union

select
    DEVICE_PORT.SWITCH_PORT_WWN,
    DEVICE_PORT.DOMAIN_ID,
    DEVICE_ENCLOSURE.IP_ADDRESS as HYPERVISOR_HOST,
    VM_PATH.HBA_PORT as ADAPTER_PORT_WWN,
    VM_VIRTUAL_MACHINE.HYPERVISOR_VM_ID,
    VM_VIRTUAL_MACHINE.NAME as VM_NAME,
    CORE_SWITCH.IP_ADDRESS,
    CORE_SWITCH.NAME as CORE_NAME,
    SWITCH_TE_PORT_STATS.TRANSMIT_OK,
    SWITCH_TE_PORT_STATS.RECEIVE_OK,
    SWITCH_TE_PORT_STATS.TRANSMIT_OK_PERCENT_UTIL,
    SWITCH_TE_PORT_STATS.RECEIVE_OK_PERCENT_UTIL,
    (-1) AS SYNCLOSSES,
    (-1) AS SIGNALLOSSES,
    (-1) AS SEQUENCEERRORS,
    (-1) AS INVALIDTRANSMISSIONS,
    (-1) AS CRCERRORS,
    SWITCH_TE_PORT_STATS.CREATION_TIME,
    VIRTUAL_SWITCH.NAME as VIRTUAL_NAME,
    SWITCH_PORT.STATUS as SWITCH_PORT_STATUS,
    SWITCH_PORT.PORT_ID,
    SWITCH_PORT.PORT_NUMBER
from
    VM_STORAGE,
    VM_HOST,
    DEVICE_ENCLOSURE,
    VM_VIRTUAL_MACHINE,
    VM_PATH,
    DEVICE_PORT,
    SWITCH_PORT,
```

```
    CORE_SWITCH,
    SWITCH_TE_PORT_STATS,
    VIRTUAL_SWITCH,
    DEVICE_PORT_MAC_ADDRESS_MAP,
    DEVICE_PORT_GIGE_PORT_LINK,
    GIGE_PORT
where
    VM_PATH.HBA_PORT::BPCHAR = DEVICE_PORT.WWN
    and VM_PATH.VM_ID = VM_VIRTUAL_MACHINE.ID
    and VM_PATH.STORAGE_ID = VM_STORAGE.ID
    and VM_STORAGE.HOST_ID = DEVICE_ENCLOSURE.ID
    and DEVICE_ENCLOSURE.ID = VM_HOST.DEVICE_ENCLOSURE_ID
    and DEVICE_ENCLOSURE.ID = VM_VIRTUAL_MACHINE.HOST_ID
    and DEVICE_PORT.ID = DEVICE_PORT_MAC_ADDRESS_MAP.DEVICE_PORT_ID
    and DEVICE_PORT_MAC_ADDRESS_MAP.MAC_ADDRESS = GIGE_PORT.REMOTE_MAC_ADDRESS
    and GIGE_PORT.SWITCH_PORT_ID = SWITCH_TE_PORT_STATS.PORT_ID
    and GIGE_PORT.SWITCH_PORT_ID = SWITCH_PORT.ID
    and SWITCH_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
    and VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID
    and SWITCH_TE_PORT_STATS.CREATION_TIME in (select max(CREATION_TIME) from
SWITCH_TE_PORT_STATS group by PORT_ID);
```

VR_CONN_MODULE_INFO

```
create or replace view VR_CONN_MODULE_INFO as
select distinct
    VR_CONN_MODULE.ID,
    VR_CONN_MODULE.VR_CONN_DOMAIN_ID,
    VR_CONN_MODULE.VCEM_ASSIGNED_ID,
    VR_CONN_MODULE.WWN,
    VR_CONN_MODULE.PRODUCT_NAME,
    VR_CONN_MODULE.SERIAL_NUMBER,
    VR_CONN_MODULE.STATUS,
    VR_CONN_MODULE.IO_BAY,
    VR_CONN_MODULE.VENDOR,
    VR_CONN_MODULE.CREATION_TIME,
    VR_CONN_MODULE.LAST_UPDATE_TIME,
    VR_CONN_DOMAIN.NAME as DOMAIN_NAME,
    VR_CONN_DOMAIN.GUID as DOMAIN_GUID,
    VR_CONN_DOMAIN.FIRMWARE_VERSION,
    VR_CONN_DOMAIN_GROUP.NAME as DOMAIN_GROUP_NAME,
    VCEM_PROFILE.ID as VCEM_PROFILE_ID,
    VCEM_PROFILE.DISCOVERY_STATUS,
    VCEM_PROFILE.LAST_FAILURE_TIMESTAMP as VCEM_LAST_FAILED_TIME,
    VCEM_PROFILE.LAST_SUCCESSFUL_TIMESTAMP as VCEM_LAST_SUCCESSFUL_TIME,
    VIRTUAL_SWITCH.ID as VIRTUAL_SWITCH_ID,
    VIRTUAL_SWITCH.MANAGED_ELEMENT_ID as VIRTUAL_SWITCH_ME_ID,
    VIRTUAL_SWITCH.NAME,
    CORE_SWITCH.IP_ADDRESS,
    FABRIC_MEMBER.FABRIC_ID,
    FABRIC.MANAGED as FABRIC_MANAGED
from
    VR_CONN_MODULE
    inner join
        VR_CONN_DOMAIN on
        VR_CONN_DOMAIN.ID = VR_CONN_MODULE.VR_CONN_DOMAIN_ID
    inner join
        VCEM_PROFILE on
        VCEM_PROFILE.ID = VR_CONN_DOMAIN.VCEM_PROFILE_ID
```

```
    left outer join
        VR_CONN_DOMAIN_GROUP on
        VR_CONN_DOMAIN_GROUP.ID = VR_CONN_DOMAIN.VR_CONN_DOMAIN_GROUP_ID
    left outer join
        VIRTUAL_SWITCH on
        VIRTUAL_SWITCH.WWN = VR_CONN_MODULE.WWN
    left outer join
        CORE_SWITCH on
        CORE_SWITCH.ID = VIRTUAL_SWITCH.CORE_SWITCH_ID
    inner join
        FABRIC_MEMBER on
        FABRIC_MEMBER.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
    inner join
        FABRIC on
        FABRIC_MEMBER.FABRIC_ID = FABRIC.ID
union
select distinct
    VR_CONN_MODULE.ID,
    VR_CONN_MODULE.VR_CONN_DOMAIN_ID,
    VR_CONN_MODULE.VCEM_ASSIGNED_ID,
    VR_CONN_MODULE.WWN,
    VR_CONN_MODULE.PRODUCT_NAME,
    VR_CONN_MODULE.SERIAL_NUMBER,
    VR_CONN_MODULE.STATUS,
    VR_CONN_MODULE.IO_BAY,
    VR_CONN_MODULE.VENDOR,
    VR_CONN_MODULE.CREATION_TIME,
    VR_CONN_MODULE.LAST_UPDATE_TIME,
    VR_CONN_DOMAIN.NAME as DOMAIN_NAME,
    VR_CONN_DOMAIN.GUID as DOMAIN_GUID,
    VR_CONN_DOMAIN.FIRMWARE_VERSION,
    VR_CONN_DOMAIN_GROUP.NAME as DOMAIN_GROUP_NAME,
    VCEM_PROFILE.ID as VCEM_PROFILE_ID,
    VCEM_PROFILE.DISCOVERY_STATUS,
    VCEM_PROFILE.LAST_FAILURE_TIMESTAMP as VCEM_LAST_FAILED_TIME,
    VCEM_PROFILE.LAST_SUCCESSFUL_TIMESTAMP as VCEM_LAST_SUCCESSFUL_TIME,
    VIRTUAL_SWITCH.ID as VIRTUAL_SWITCH_ID,
    VIRTUAL_SWITCH.MANAGED_ELEMENT_ID as VIRTUAL_SWITCH_ME_ID,
    VIRTUAL_SWITCH.NAME,
    CORE_SWITCH.IP_ADDRESS,
    DEVICE_NODE.FABRIC_ID,
    FABRIC.MANAGED as FABRIC_MANAGED
from
    VR_CONN_MODULE
    inner join
        VR_CONN_DOMAIN on
        VR_CONN_DOMAIN.ID = VR_CONN_MODULE.VR_CONN_DOMAIN_ID
    inner join
        VCEM_PROFILE on
        VCEM_PROFILE.ID = VR_CONN_DOMAIN.VCEM_PROFILE_ID
    left outer join
        VR_CONN_DOMAIN_GROUP on
        VR_CONN_DOMAIN_GROUP.ID = VR_CONN_DOMAIN.VR_CONN_DOMAIN_GROUP_ID
    left outer join
        VIRTUAL_SWITCH on
        VIRTUAL_SWITCH.WWN = VR_CONN_MODULE.WWN
    left outer join
        CORE_SWITCH on
        CORE_SWITCH.ID = VIRTUAL_SWITCH.CORE_SWITCH_ID
    left outer join
```

```
        DEVICE_NODE on
        DEVICE_NODE.WWN = VR_CONN_MODULE.WWN
    left outer join
        FABRIC on
        DEVICE_NODE.FABRIC_ID = FABRIC.ID;
```

VR_CONN_MODULE_PORT_INFO

```
create or replace view VR_CONN_MODULE_PORT_INFO as
select
    VR_CONN_MODULE_PORT.ID,
    VR_CONN_MODULE_PORT.VR_CONN_MODULE_ID,
    VR_CONN_MODULE_PORT.WWN,
    VR_CONN_MODULE_PORT.POSITION_,
    VR_CONN_MODULE_PORT.FABRIC_NAME,
    VR_CONN_MODULE_PORT.SPEED,
    VR_CONN_MODULE_PORT.STATUS,
    VR_CONN_MODULE_PORT.LAST_STATUS,
    VR_CONN_MODULE_PORT.REMOTE_NODE_WWN,
    VR_CONN_MODULE_PORT.CREATION_TIME,
    VR_CONN_MODULE_PORT.LAST_UPDATE_TIME,
    VR_CONN_MODULE.IO_BAY,
    VR_CONN_DOMAIN.ID as VR_CONN_DOMAIN_ID,
    VCEM_PROFILE.ID as VCEM_PROFILE_ID,
    SWITCH_PORT.ID as SWITCH_PORT_ID,
    VIRTUAL_SWITCH.ID as VIRTUAL_SWITCH_ID
from
    VR_CONN_MODULE_PORT
    inner join
        VR_CONN_MODULE on
        VR_CONN_MODULE.ID = VR_CONN_MODULE_PORT.VR_CONN_MODULE_ID
    inner join
        VR_CONN_DOMAIN on
        VR_CONN_DOMAIN.ID = VR_CONN_MODULE.VR_CONN_DOMAIN_ID
    inner join
        VCEM_PROFILE on
        VCEM_PROFILE.ID = VR_CONN_DOMAIN.VCEM_PROFILE_ID
    left outer join
        SWITCH_PORT on
        SWITCH_PORT.WWN = VR_CONN_MODULE_PORT.WWN
    left outer join
        VIRTUAL_SWITCH on
        VIRTUAL_SWITCH.WWN = VR_CONN_MODULE.WWN;
```

VR_CONN_NPIV_INFO

```
create or replace view VR_CONN_NPIV_INFO as
select
    VR_CONN_WWN.ID,
    VR_CONN_WWN.VR_CONN_FC_CONNECTION_ID,
    VR_CONN_WWN.PORT_ADDRESS as PORT_WWN,
    VR_CONN_WWN.NODE_ADDRESS as NODE_WWN,
    VR_CONN_SERVER_PROFILE.NAME as SERVER_PROFILE_NAME,
    VR_CONN_SERVER_PROFILE.BAY_NAME,
    coalesce(VR_CONN_SERVER_PROFILE.BAY_NUMBER,
VR_CONN_FC_CONNECTION.CONNECTION_BAY) as BAY_NUMBER,
    VR_CONN_SERVER_PROFILE.VIRTUAL_SERIAL_NUMBER,
    VCEM_PROFILE.ID as VCEM_PROFILE_ID,
```

```
    VR_CONN_DOMAIN.ID as VIRTUAL_CONNECT_DOMAIN_ID,
    VR_CONN_MODULE.ID as VIRTUAL_CONNECT_MODULE_ID,
    VR_CONN_MODULE_PORT.ID as VIRTUAL_CONNECT_MODULE_PORT_ID,
    VIRTUAL_SWITCH.ID as VIRTUAL_SWITCH_ID,
    coalesce(SWITCH_PORT.WWN, VR_CONN_MODULE_PORT.WWN) as UPLINK_PORT_WWN,
    coalesce(SWITCH_PORT.PORT_NUMBER, VR_CONN_MODULE_PORT.POSITION_) as
UPLINK_PORT_NUMBER,
    DEVICE_PORT.ID as DEVICE_PORT_ID,
    DEVICE_PORT.NUMBER as DEVICE_PORT_NUMBER,
    DEVICE_PORT.TYPE as DEVICE_PORT_TYPE,
    DEVICE_NODE.ID as DEVICE_NODE_ID,
    DEVICE_NODE.FABRIC_ID,
    USER_DEFINED_DEVICE_DETAIL.NAME
from
    VR_CONN_WWN
    inner join
        VR_CONN_FC_CONNECTION on
        VR_CONN_FC_CONNECTION.ID = VR_CONN_WWN.VR_CONN_FC_CONNECTION_ID
    inner join
        VR_CONN_SERVER_PROFILE on
        VR_CONN_SERVER_PROFILE.ID =
VR_CONN_FC_CONNECTION.VR_CONN_SERVER_PROFILE_ID
    inner join
        VR_CONN_DOMAIN on
        VR_CONN_DOMAIN.GUID = VR_CONN_SERVER_PROFILE.BAY_ENCLOSURE_UUID
    inner join
        VCEM_PROFILE on
        VCEM_PROFILE.ID = VR_CONN_SERVER_PROFILE.VCEM_PROFILE_ID
    inner join
        VR_CONN_MODULE on
        VR_CONN_MODULE.VR_CONN_DOMAIN_ID = VR_CONN_DOMAIN.ID and
        VR_CONN_MODULE.IO_BAY = VR_CONN_FC_CONNECTION.CONNECTION_BAY
    inner join
        VR_CONN_MODULE_PORT on
        VR_CONN_MODULE_PORT.VR_CONN_MODULE_ID = VR_CONN_MODULE.ID and
        VR_CONN_MODULE_PORT.POSITION_ = VR_CONN_FC_CONNECTION.PORT_NUMBER
    left outer join
        VIRTUAL_SWITCH on
        VIRTUAL_SWITCH.WWN = VR_CONN_MODULE.WWN
    left outer join
        SWITCH_PORT on
        SWITCH_PORT.WWN = VR_CONN_MODULE_PORT.WWN
    left outer join
        DEVICE_PORT on
        DEVICE_PORT.WWN = VR_CONN_WWN.PORT_ADDRESS
    left outer join
        DEVICE_NODE on
        DEVICE_NODE.WWN = VR_CONN_WWN.NODE_ADDRESS
    left outer join
        USER_DEFINED_DEVICE_DETAIL on
        USER_DEFINED_DEVICE_DETAIL.WWN = VR_CONN_WWN.PORT_ADDRESS;
```

VMM_DISCOVERED_MAC_INFO

```
create or replace view VMM_DISCOVERED_MAC_INFO AS
select
      VM_VIRTUAL_ETHERNET_ADAPTER.MAC_ADDRESS,
      VM_VIRTUAL_ETHERNET_ADAPTER.DISPLAY_LABEL,
      VM_VIRTUAL_ETHERNET_ADAPTER.PORT_GROUP_NAME,
```

```
      VM_VIRTUAL_MACHINE.NAME AS VIRTUAL_MACHINE_NAME,
      VM_VCENTER_MEMBER.HOST_NAME,
      VM_VCENTER.NAME AS VCENTER_NAME
from
      VM_VIRTUAL_ETHERNET_ADAPTER,
      VM_VIRTUAL_MACHINE,
      VM_VCENTER_MEMBER,
      VM_VCENTER
where
     VM_VIRTUAL_ETHERNET_ADAPTER.VIRTUAL_MACHINE_ID = VM_VIRTUAL_MACHINE.ID
     AND VM_VIRTUAL_MACHINE.HOST_ID = VM_VCENTER_MEMBER.VM_HOST_ID
     AND VM_VCENTER_MEMBER.VM_VCENTER_ID = VM_VCENTER.ID

union all
select
     VM_HOST_VIRTUAL_NIC.MAC AS MAC_ADDRESS,
     VM_HOST_VIRTUAL_NIC.DEVICE_NAME AS DISPLAY_LABEL,
     VM_HOST_VIRTUAL_NIC.PORT_GROUP_KEY AS PORT_GROUP_NAME,
     NULL::UNKNOWN AS VIRTUAL_MACHINE_NAME,
     VM_VCENTER_MEMBER.HOST_NAME,
     VM_VCENTER.NAME AS VCENTER_NAME
from
     VM_HOST_VIRTUAL_NIC,
     VM_VCENTER_MEMBER,
     VM_VCENTER
where
     VM_HOST_VIRTUAL_NIC.VM_HOST_ID = VM_VCENTER_MEMBER.VM_HOST_ID AND
VM_VCENTER_MEMBER.VM_VCENTER_ID = VM_VCENTER.ID

union all
select
      VM_PHYSICAL_NIC.MAC_ADDRESS,
      VM_PHYSICAL_NIC.DEVICE_NAME,
      NULL::UNKNOWN AS PORT_GROUP_NAME,
      NULL::UNKNOWN AS VIRTUAL_MACHINE_NAME,
      VM_VCENTER_MEMBER.HOST_NAME,
      VM_VCENTER.NAME AS VCENTER_NAME
from
      VM_PHYSICAL_NIC,
      VM_VCENTER_MEMBER,
      VM_VCENTER
where
      VM_PHYSICAL_NIC.VM_HOST_ID = VM_VCENTER_MEMBER.VM_HOST_ID AND
VM_VCENTER_MEMBER.VM_VCENTER_ID = VM_VCENTER.ID;
```

VM_VIRTUAL_ETHERNET_ADAPTER_INFO

```
create or replace view VM_VIRTUAL_ETHERNET_ADAPTER_INFO as
select
VM_VIRTUAL_ETHERNET_ADAPTER.ID,
VM_VIRTUAL_ETHERNET_ADAPTER.MAC_ADDRESS,
VM_VIRTUAL_ETHERNET_ADAPTER.DISPLAY_LABEL,
VM_VIRTUAL_ETHERNET_ADAPTER.PORT_GROUP_NAME,
VM_VIRTUAL_MACHINE.NAME as VIRTUAL_MACHINE_NAME,
VM_VCENTER_MEMBER.HOST_NAME,
VM_VCENTER.NAME as VCENTER_NAME

From
VM_VIRTUAL_ETHERNET_ADAPTER,
```

```
VM_VIRTUAL_MACHINE,
VM_VCENTER_MEMBER,
VM_VCENTER

Where
VM_VIRTUAL_ETHERNET_ADAPTER.VIRTUAL_MACHINE_ID = VM_VIRTUAL_MACHINE.ID
And  VM_VIRTUAL_MACHINE.HOST_ID = VM_VCENTER_MEMBER.VM_HOST_ID
And  VM_VCENTER_MEMBER.VM_VCENTER_ID = VM_VCENTER.ID;
```

ZONE_DB_INFO

```
create or replace view ZONE_DB_INFO as
select
    ZONE_DB.ID,
    ZONE_DB.FABRIC_ID,
    ZONE_DB.OFFLINE,
    ZONE_DB.NAME,
    ZONE_DB.CREATED,
    ZONE_DB.CREATED_BY,
    ZONE_DB.LAST_MODIFIED,
    ZONE_DB.LAST_MODIFIED_BY,
    ZONE_DB.LAST_APPLIED,
    ZONE_DB.LAST_APPLIED_BY,
    ZONE_DB.DEFAULT_ZONE_STATUS,
    ZONE_DB.MCDATA_DEFAULT_ZONE,
    ZONE_DB.MCDATA_SAFE_ZONE,
    ZONE_DB.ZONE_TXN_SUPPORTED,
    ZONE_DB.ZONE_CONFIG_SIZE,
    ZONE_DB.ZONE_AVAILABLE_SIZE,
    ZONE_DB_CONFIG.ID AS CONFIG_ID,
    ZONE_DB_CONFIG.DEFINED_CONTENT,
    ZONE_DB_CONFIG.ACTIVE_CONTENT,
    ZONE_DB_CONFIG.TI_ZONE_CONTENT
from
    ZONE_DB, ZONE_DB_CONFIG
where
    ZONE_DB.ID = ZONE_DB_CONFIG.ZONE_DB_ID;
```

AP_USAGE

```
CREATE VIEW ap_usage AS
    SELECT ap_station.device_id, ap_station.time_stamp, count(*) AS num_clients
FROM ap_station WHERE (ap_station.radio > 0) GROUP BY ap_station.device_id,
ap_station.time_stamp;
```

EVENTS

```
CREATE VIEW events AS
    SELECT emain.trap_log_id, emain.trap_sender, emain."timestamp",
emain.severity, emsgs.messages, emain.is_ack, emain.log_type, emain.slot,
emain.port, emain.device_id, emain.event_action_id, emain.device_group_id,
emain.port_group_id, emain.trap_device_ip, emain.log_sub_type, emain.unit FROM
(events_main emain LEFT JOIN events_messages emsgs ON ((emain.messages_id =
emsgs.messages_id)));
```

SFLOW_MINUTE_BGP_VIEW

```
create or replace view SFLOW_MINUTE_BGP_VIEW as
  select DEVICE_ID, TIME_IN_SECONDS, SRC_AS, SFLOW_IP_ROUTE_INFO_ID, IN_VLAN,
OUT_VLAN, FRAMES, BYTES
  from SFLOW_MINUTE_BGP
  where SLNUM <= (select MAX_SLNUM from SFLOW_MINUTE_BGP_SLNUM fetch first 1 rows
only)
  union all
  select DEVICE_ID, TIME_IN_SECONDS, SRC_AS, SFLOW_IP_ROUTE_INFO_ID, IN_VLAN,
OUT_VLAN, FRAMES, BYTES
  from SFLOW_STAGING
  where SLNUM >= (select MIN_SLNUM from SFLOW_STAGING_SLNUM fetch first 1 rows
only)
  and SRC_AS != 0 OR SFLOW_IP_ROUTE_INFO_ID != 0;
```

SFLOW_MINUTE_VLAN_VIEW

```
create or replace view SFLOW_MINUTE_VLAN_VIEW as
  select DEVICE_ID, TIME_IN_SECONDS, IN_VLAN, OUT_VLAN, FRAMES, BYTES
  from SFLOW_MINUTE_VLAN
  where SLNUM <= (select MAX_SLNUM from SFLOW_MINUTE_VLAN_SLNUM fetch first 1 rows
only)
  union all
  select DEVICE_ID, TIME_IN_SECONDS, IN_VLAN, OUT_VLAN, FRAMES, BYTES
  from SFLOW_STAGING
  where SLNUM >= (select MIN_SLNUM from SFLOW_STAGING_SLNUM fetch first 1 rows
only);
```

PHYSICAL_DEVICE_INFO

```
create or replace view PHYSICAL_DEVICE_INFO as
select
    PHYSICAL_DEVICE.PHYSICAL_DEVICE_ID as PD_PHYSICAL_DEVICE_ID,
    PHYSICAL_DEVICE.DEVICE_ID,
    PHYSICAL_DEVICE.DESCRIPTION,
    PHYSICAL_DEVICE.NUM_SLOTS,
    PHYSICAL_DEVICE.TABLE_SUBTYPE,
    PHYSICAL_DEVICE.UNIT_NUMBER,
    PHYSICAL_DEVICE.UNIT_NEIGHBOR1,
    PHYSICAL_DEVICE.UNIT_NEIGHBOR2,
    PHYSICAL_DEVICE.UNIT_PRESENT,
    FOUNDRY_PHYSICAL_DEVICE.PHYSICAL_DEVICE_ID as FPD_PHYSICAL_DEVICE_ID,
    FOUNDRY_PHYSICAL_DEVICE.SERIAL_NUMBER,
    FOUNDRY_PHYSICAL_DEVICE.PRODUCT_TYPE,
    DEVICE.IP_ADDRESS
from
    PHYSICAL_DEVICE,
    FOUNDRY_PHYSICAL_DEVICE,
    DEVICE
where
    DEVICE.DEVICE_ID = PHYSICAL_DEVICE.DEVICE_ID
    and PHYSICAL_DEVICE.PHYSICAL_DEVICE_ID =
FOUNDRY_PHYSICAL_DEVICE.PHYSICAL_DEVICE_ID;
```

SLOT_INFO

```
create or replace view SLOT_INFO as
select
    SLOT.*,
    PHYSICAL_DEVICE.UNIT_NUMBER,
    DEVICE.IP_ADDRESS
from
    PHYSICAL_DEVICE,
    SLOT,
    DEVICE
where
    DEVICE.DEVICE_ID = PHYSICAL_DEVICE.DEVICE_ID
    and SLOT.PHYSICAL_DEVICE_ID = PHYSICAL_DEVICE.PHYSICAL_DEVICE_ID;
```

MANAGED_ELEMENT_INFO

Common managed element data used by custom DTO methods to identify the managed element type, and provide a link to the details table for the managed element. Some common managed element fields are included in this view so Fault Management can use this view to identify the managed element ID for an event source.

```
create or replace view MANAGED_ELEMENT_INFO as
select
    MANAGED_ELEMENT.ID as MANAGED_ELEMENT_ID,
    DEVICE.DEVICE_ID as IP_DEVICE_ID,
    coalesce(CS_ME.ID, CS_VS.ID) as CORE_SWITCH_ID,
    VIRTUAL_SWITCH.ID as VIRTUAL_SWITCH_ID,
    DEVICE_ENCLOSURE.ID as DEVICE_ENCLOSURE_ID,
    DEVICE.IP_ADDRESS as LAN_IP_ADDRESS,
   coalesce (CS_VS.IP_ADDRESS, CS_ME.IP_ADDRESS, DEVICE_ENCLOSURE.IP_ADDRESS) as
SAN_IP_ADDRESS,
    VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID,
    coalesce (VIRTUAL_SWITCH.WWN, CS_ME.WWN, DEVICE.NODE_WWN) as NODE_WWN
from
    MANAGED_ELEMENT
        left outer join VIRTUAL_SWITCH on MANAGED_ELEMENT.ID =
VIRTUAL_SWITCH.MANAGED_ELEMENT_ID
        left outer join CORE_SWITCH CS_ME on (MANAGED_ELEMENT.ID =
CS_ME.MANAGED_ELEMENT_ID)
        left outer join CORE_SWITCH CS_VS on (CS_VS.ID =
VIRTUAL_SWITCH.CORE_SWITCH_ID)
        left outer join DEVICE on MANAGED_ELEMENT.ID = DEVICE.MANAGED_ELEMENT_ID
        left outer join DEVICE_ENCLOSURE on MANAGED_ELEMENT.ID =
DEVICE_ENCLOSURE.MANAGED_ELEMENT_ID;
```

SNMP_DATA_INFO

```
create or replace view SNMP_DATA_INFO as
select * from SNMP_DATA
union all
select * from SNMP_DATA_30MIN
union all
select * from SNMP_DATA_2HOUR
union all
select * from SNMP_DATA_1DAY;
```

SNMP_EXPR_DATA_INFO

```
create or replace view SNMP_EXPR_DATA_INFO as
select * from SNMP_EXPR_DATA
union all
select * from SNMP_EXPR_DATA_30MIN
union all
select * from SNMP_EXPR_DATA_2HOUR
union all
select * from SNMP_EXPR_DATA_1DAY;
```

SNMP_DATA_VIEW

```
create or replace view snmp_data_view as
        (        (        (        (         SELECT de.device_id, de.ip_address AS
device_ip, se.target_type, de.device_id AS target_id, de.sys_name AS target_name,
1 AS collectible_type, se.expression_id AS collectible_id, se.collector_id, (
SELECT perf_collector.name AS collector_name
                                                    FROM perf_collector
                                                   WHERE perf_collector.collector_id
= se.collector_id) AS collector_name, ( SELECT snmp_expression.name AS
collectible_name
                                                    FROM snmp_expression
                                                  WHERE snmp_expression.expression_id
= se.expression_id) AS collectible_name, ( SELECT snmp_expression.equation AS
collectible_detail
                                                    FROM snmp_expression
                                                  WHERE snmp_expression.expression_id
= se.expression_id) AS collectible_detail, se.value, se.time_in_seconds, '' AS
mib_index
                                             FROM snmp_expr_data_info se
                                        JOIN device de ON se.target_id = de.device_id
                                         WHERE se.target_type = 0
                                  UNION ALL
                                               SELECT de.device_id, de.ip_address AS
device_ip, sd.target_type, de.device_id AS target_id, de.sys_name AS target_name,
0 AS collectible_type, sd.mib_object_id AS collectible_id, sd.collector_id, (
SELECT perf_collector.name AS collector_name
                                                    FROM perf_collector
                                                   WHERE perf_collector.collector_id
= sd.collector_id) AS collector_name, ( SELECT (mib_object.name::text ||
'.'::text) || sd.mib_index::text AS collectible_name
                                                    FROM mib_object
                                                   WHERE mib_object.mib_object_id =
sd.mib_object_id) AS collectible_name, ( SELECT mib_object.oid AS
collectible_detail
                                                    FROM mib_object
                                                   WHERE mib_object.mib_object_id =
sd.mib_object_id) AS collectible_detail, sd.value, sd.time_in_seconds,
sd.mib_index
                                             FROM snmp_data_info sd
                                        JOIN device de ON sd.target_id = de.device_id
                                         WHERE sd.target_type = 0::numeric)
                           UNION ALL
                                      SELECT de.device_id, de.ip_address AS device_ip,
sd.target_type, ifs.interface_id AS target_id, ifs.if_name AS target_name, 0 AS
collectible_type, sd.mib_object_id AS collectible_id, sd.collector_id, ( SELECT
perf_collector.name AS collector_name
```

```
                                                FROM perf_collector
                                               WHERE perf_collector.collector_id =
sd.collector_id) AS collector_name, ( SELECT (mib_object.name::text || '.'::text)
|| sd.mib_index::text AS collectible_name
                                                FROM mib_object
                                               WHERE mib_object.mib_object_id =
sd.mib_object_id) AS collectible_name, ( SELECT mib_object.oid AS
collectible_detail
                                                FROM mib_object
                                               WHERE mib_object.mib_object_id =
sd.mib_object_id) AS collectible_detail, sd.value, sd.time_in_seconds,
sd.mib_index
                                     FROM snmp_data_info sd
                                JOIN interface ifs ON sd.target_type = 1::numeric AND
sd.target_id = ifs.interface_id
                            JOIN device de ON ifs.device_id = de.device_id)
                  UNION ALL
                            SELECT de.device_id, de.ip_address AS device_ip,
se.target_type, ifs.interface_id AS target_id, ifs.if_name AS target_name, 1 AS
collectible_type, se.expression_id AS collectible_id, se.collector_id, ( SELECT
perf_collector.name AS collector_name
                                     FROM perf_collector
                                    WHERE perf_collector.collector_id =
se.collector_id) AS collector_name, ( SELECT snmp_expression.name AS
collectible_name
                                     FROM snmp_expression
                                    WHERE snmp_expression.expression_id =
se.expression_id) AS collectible_name, ( SELECT snmp_expression.equation AS
collectible_detail
                                     FROM snmp_expression
                                    WHERE snmp_expression.expression_id =
se.expression_id) AS collectible_detail, se.value, se.time_in_seconds, '' AS
mib_index
                              FROM snmp_expr_data_info se
                         JOIN interface ifs ON se.target_type = 1 AND se.target_id =
ifs.interface_id
                   JOIN device de ON ifs.device_id = de.device_id)
          UNION ALL
                    SELECT de.device_id, de.ip_address AS device_ip, sd.target_type,
sp.id AS target_id, sp.name AS target_name, 0 AS collectible_type,
sd.mib_object_id AS collectible_id, sd.collector_id, ( SELECT perf_collector.name
AS collector_name
                              FROM perf_collector
                             WHERE perf_collector.collector_id = sd.collector_id) AS
collector_name, ( SELECT (mib_object.name::text || '.'::text) ||
sd.mib_index::text AS collectible_name
                              FROM mib_object
                             WHERE mib_object.mib_object_id = sd.mib_object_id) AS
collectible_name, ( SELECT mib_object.oid AS collectible_detail
                              FROM mib_object
                             WHERE mib_object.mib_object_id = sd.mib_object_id) AS
collectible_detail, sd.value, sd.time_in_seconds, sd.mib_index
                     FROM snmp_data_info sd
                JOIN switch_port sp ON sd.target_type = 4::numeric AND sd.target_id
= sp.id
           JOIN device de ON (( SELECT sw.managed_element_id
                    FROM virtual_switch sw
                   WHERE sw.id = sp.virtual_switch_id)) = de.managed_element_id)
UNION ALL
```

```
        SELECT de.device_id, de.ip_address AS device_ip, se.target_type, sp.id AS
target_id, sp.name AS target_name, 1 AS collectible_type, se.expression_id AS
collectible_id, se.collector_id, ( SELECT perf_collector.name AS collector_name
                  FROM perf_collector
                 WHERE perf_collector.collector_id = se.collector_id) AS
collector_name, ( SELECT snmp_expression.name AS collectible_name
                  FROM snmp_expression
                 WHERE snmp_expression.expression_id = se.expression_id) AS
collectible_name, ( SELECT snmp_expression.equation AS collectible_detail
                  FROM snmp_expression
                 WHERE snmp_expression.expression_id = se.expression_id) AS
collectible_detail, se.value, se.time_in_seconds, '' AS mib_index
           FROM snmp_expr_data_info se
      JOIN switch_port sp ON se.target_type = 4 AND se.target_id = sp.id
   JOIN device de ON (( SELECT sw.managed_element_id
         FROM virtual_switch sw
        WHERE sw.id = sp.virtual_switch_id)) = de.managed_element_id;
```

VM_VNETWORK_INFO

This view provideds combine VM and device information to derive VM to the ingress switch port information.

```
create or replace view VM_VNETWORK_INFO as
select
    VM_HOST.HYPERVISOR_NAME as VHOST_NAME,
    VM_VIRTUAL_MACHINE.NAME as VM_NAME,
    VM_VIRTUAL_MACHINE.HYPERVISOR_VM_ID as VM_ID,
    VM_VIRTUAL_ETHERNET_ADAPTER.MAC_ADDRESS as VNIC_MAC,
    VM_DV_PORT_GROUP.NAME as PGRP_NAME,
    VM_DV_SWITCH.NAME as VSWITCH_NAME,
    VNIC_DV_PORT.NAME as DVPORT_NAME,
    VM_PHYSICAL_NIC.DEVICE_NAME as PNIC_NAME,
    VM_PHYSICAL_NIC.MAC_ADDRESS as PNIC_MAC,
    DEVICE.SYS_NAME as SWITCH_NAME,
    DEVICE.IP_ADDRESS as SWITCH_IP,
    PHYSICAL_PORT.PORT_NUM as SWITCH_PORT,
    INTERFACE.PORT_STATUS as SWITCH_PORT_STATUS
from
    VM_HOST
        left join VM_VIRTUAL_MACHINE on VM_HOST.DEVICE_ENCLOSURE_ID =
VM_VIRTUAL_MACHINE.HOST_ID,
    VM_VIRTUAL_ETHERNET_ADAPTER,
    VM_DV_PORT VNIC_DV_PORT,
    VM_DV_PORT PNIC_DV_PORT,
    VM_DV_PORT_GROUP,
    VM_DV_SWITCH,
    VM_PHYSICAL_NIC,
    VM_HOST_END_DEV_CONNECTIVITY,
    INTERFACE,
    DEVICE,
    PHYSICAL_INTERFACE,
    PHYSICAL_PORT
where
    VM_VIRTUAL_MACHINE.ID = VM_VIRTUAL_ETHERNET_ADAPTER.VIRTUAL_MACHINE_ID and
    VM_VIRTUAL_ETHERNET_ADAPTER.VM_DV_PORT_ID is not null and
    VM_VIRTUAL_ETHERNET_ADAPTER.VM_DV_PORT_ID = VNIC_DV_PORT.ID and
    VNIC_DV_PORT.VM_DV_PORT_GROUP_ID = VM_DV_PORT_GROUP.ID and
    VNIC_DV_PORT.VM_DV_SWITCH_ID = VM_DV_SWITCH.ID and
```

```
    PNIC_DV_PORT.VM_DV_SWITCH_ID = VM_DV_SWITCH.ID and
    PNIC_DV_PORT.ID = VM_PHYSICAL_NIC.VM_DV_PORT_ID and
    VM_PHYSICAL_NIC.ID = VM_HOST_END_DEV_CONNECTIVITY.VM_PHYSICAL_NIC_ID and
    VM_HOST_END_DEV_CONNECTIVITY.INTERFACE_ID = INTERFACE.INTERFACE_ID and
    INTERFACE.DEVICE_ID = DEVICE.DEVICE_ID and
    VM_HOST_END_DEV_CONNECTIVITY.INTERFACE_ID = PHYSICAL_INTERFACE.INTERFACE_ID
and
    PHYSICAL_INTERFACE.PHYSICAL_PORT_ID = PHYSICAL_PORT.PHYSICAL_PORT_ID

union all

select
    VM_HOST.HYPERVISOR_NAME as VHOST_NAME,
    VM_VIRTUAL_MACHINE.NAME as VM_NAME,
    VM_VIRTUAL_MACHINE.HYPERVISOR_VM_ID as VM_ID,
    VM_VIRTUAL_ETHERNET_ADAPTER.MAC_ADDRESS as VNIC_MAC,
    VM_STD_VSWITCH_PORT_GROUP.NAME as PGRP_NAME,
    VM_STANDARD_VIRTUAL_SWITCH.NAME as VSWITCH_NAME,
    null as DVPORT_NAME,
    VM_PHYSICAL_NIC.DEVICE_NAME as PNIC_NAME,
    VM_PHYSICAL_NIC.MAC_ADDRESS as PNIC_MAC,
    DEVICE.SYS_NAME as SWITCH_NAME,
    DEVICE.IP_ADDRESS as SWITCH_IP,
    PHYSICAL_PORT.PORT_NUM as SWITCH_PORT,
    INTERFACE.PORT_STATUS as SWITCH_PORT_STATUS
from
    VM_HOST
        left join VM_VIRTUAL_MACHINE on VM_HOST.DEVICE_ENCLOSURE_ID =
VM_VIRTUAL_MACHINE.HOST_ID,
    VM_VIRTUAL_ETHERNET_ADAPTER,
    VM_STD_VSWITCH_PORT_GROUP,
    VM_STANDARD_VIRTUAL_SWITCH,
    VM_PHYSICAL_NIC,
    VM_HOST_END_DEV_CONNECTIVITY,
    INTERFACE,
    DEVICE,
    PHYSICAL_INTERFACE,
    PHYSICAL_PORT
where
    VM_VIRTUAL_MACHINE.ID = VM_VIRTUAL_ETHERNET_ADAPTER.VIRTUAL_MACHINE_ID and
    VM_VIRTUAL_ETHERNET_ADAPTER.VM_STD_VSWITCH_PORT_GROUP_ID is not null and
    VM_VIRTUAL_ETHERNET_ADAPTER.VM_STD_VSWITCH_PORT_GROUP_ID =
VM_STD_VSWITCH_PORT_GROUP.ID and
    VM_STD_VSWITCH_PORT_GROUP.VM_STANDARD_VIRTUAL__SWITCH_ID =
VM_STANDARD_VIRTUAL_SWITCH.ID and
   VM_STANDARD_VIRTUAL_SWITCH.ID = VM_PHYSICAL_NIC.VM_STANDARD_VIRTUAL_SWITCH_ID
and
    VM_PHYSICAL_NIC.ID = VM_HOST_END_DEV_CONNECTIVITY.VM_PHYSICAL_NIC_ID and
    VM_HOST_END_DEV_CONNECTIVITY.INTERFACE_ID = INTERFACE.INTERFACE_ID and
    INTERFACE.DEVICE_ID = DEVICE.DEVICE_ID and
    VM_HOST_END_DEV_CONNECTIVITY.INTERFACE_ID = PHYSICAL_INTERFACE.INTERFACE_ID
and
    PHYSICAL_INTERFACE.PHYSICAL_PORT_ID = PHYSICAL_PORT.PHYSICAL_PORT_ID;
```

VCS_CLUSTER_MEMBER_INFO

```
CREATE VIEW vcs_cluster_member_info AS
   select
    VCS_DEVICE.DEVICE_ID as VCS_DEVICE_ID,
```

```
    VCS_DEVICE.MANAGED_ELEMENT_ID as VCS_ME_ID,
    MEMBER_DEVICE.DEVICE_ID as MEMBER_DEVICE_ID,
    MEMBER_DEVICE.MANAGED_ELEMENT_ID as MEMBER_ME_ID,
    VCS_MEMBER.CREATION_TIME,
    VCS_MEMBER.TRUSTED,
    VCS_MEMBER.MISSING,
    VCS_MEMBER.MISSING_TIME,
    VCS_MEMBER.STATE,
    VCS_MEMBER.FABRIC_STATUS
from
    device VCS_DEVICE,
    device MEMBER_DEVICE,
    VCS_CLUSTER_MEMBER VCS_MEMBER
where
    VCS_MEMBER.CLUSTER_ME_ID = VCS_DEVICE.MANAGED_ELEMENT_ID AND
    VCS_MEMBER.MEMBER_ME_ID = MEMBER_DEVICE.MANAGED_ELEMENT_ID;
```

RESET_VCS_LICENSED

```
CREATE OR REPLACE FUNCTION reset_vcs_licensed(no_of_licenses integer)
  RETURNS void AS
$BODY$
begin
    UPDATE fabric set vcs_licensed = 0;
    UPDATE device set vcs_licensed = 0;
    UPDATE fabric set vcs_licensed = 1 WHERE fabric.id in (SELECT id FROM fabric
ORDER BY creation_time LIMIT no_of_licenses);
    UPDATE device set vcs_licensed = 1 WHERE device.managed_element_id in (SELECT
vcs_cluster_me_id FROM fabric_vcs_cluster_map WHERE fabric_id in (SELECT id FROM
fabric WHERE vcs_licensed=1));
end;
$BODY$
  LANGUAGE plpgsql VOLATILE
  COST 100;
ALTER FUNCTION reset_vcs_licensed(integer)
  OWNER TO dcmadmin;
```

TRILL_TRUNK_INFO

```
create or replace view TRILL_TRUNK_INFO as
select
    TRILL_TRUNK_GROUP.ID,
    TRILL_TRUNK_GROUP.ME_ID,
    TRILL_TRUNK_GROUP.MASTER_PORT_NUMBER,
    TRILL_TRUNK_MEMBER.PORT_NUMBER as MEMBER_PORT_NUMBER,
    MEMBER_DEVICE.DEVICE_ID,
    MASTER_INTERFACE.INTERFACE_ID as MASTER_INTERFACE_ID,
    MASTER_INTERFACE.IF_NAME as MASTER_IF_NAME,
    MEMBER_INTERFACE.INTERFACE_ID as MEMBER_INTERFACE_ID,
    MEMBER_INTERFACE.IF_NAME as MEMBER_IF_NAME,
    VCS_CLUSTER_MEMBER.CLUSTER_ME_ID,
    CLUSTER_DEVICE.DEVICE_ID as CLUSTER_DEVICE_ID
from
    TRILL_TRUNK_GROUP
        inner join TRILL_TRUNK_MEMBER on
            TRILL_TRUNK_MEMBER.GROUP_ID = TRILL_TRUNK_GROUP.ID
        inner join device MEMBER_DEVICE on
```

```
            MEMBER_DEVICE.MANAGED_ELEMENT_ID = TRILL_TRUNK_GROUP.ME_ID
        left outer join INTERFACE MASTER_INTERFACE on
            MASTER_INTERFACE.DEVICE_ID = MEMBER_DEVICE.DEVICE_ID and
MASTER_INTERFACE.IDENTIFIER = TRILL_TRUNK_GROUP.MASTER_PORT_NUMBER
        left outer join INTERFACE MEMBER_INTERFACE on
            MEMBER_INTERFACE.DEVICE_ID = MEMBER_DEVICE.DEVICE_ID and
MEMBER_INTERFACE.IDENTIFIER = TRILL_TRUNK_MEMBER.PORT_NUMBER
        left outer join VCS_CLUSTER_MEMBER on
            VCS_CLUSTER_MEMBER.MEMBER_ME_ID = TRILL_TRUNK_GROUP.ME_ID
        left outer join DEVICE CLUSTER_DEVICE on
            CLUSTER_DEVICE.MANAGED_ELEMENT_ID = VCS_CLUSTER_MEMBER.CLUSTER_ME_ID;
```

WIRELESS_INTERFACE

```
create or replace view wireless_interface as
SELECT
      l2.device_id,
      l2.device_ip_address,
      l2.physical_device_id,
      l2.unit_number,
      l2.slot_id,
      l2.slot_num,
      l2.module_id,
      l2.physical_port_id,
      l2.port_num,
      l2.interface_id,
      l2.name,
      l2.if_name,
      l2.identifier,
      l2.speed_in_mb,
      l2.physical_address,
      l2.interface_id AS radioif_id,
      wireless.radio_type,
      wireless.is_enabled,
      wireless.is_auto_channel,
      wireless.tx_power,
      wireless.channel_number,
      wireless.max_data_rate,
      wireless.beacon_rate,
      wireless.dtim,
      wireless.rts_threshold,
      wireless.is_turbo_mode,
      wireless.radio_g_mode,
      wireless.max_associated_clients
    FROM
      ((SELECT DISTINCT d.device_id, d.ip_address AS device_ip_address,
pd.physical_device_id, pd.unit_number, s.slot_id, s.slot_num, msp.module_id,
pp.physical_port_id, pp.port_num, i.interface_id, i.name, i.if_name,
i.identifier, pi.speed_in_mb, pi.physical_address
      FROM device d, physical_device pd, slot s, module_slot_present msp,
physical_port pp, physical_interface pi, interface i
      WHERE
        (((((((d.device_id = pd.device_id)
          AND (pd.physical_device_id = s.physical_device_id))
          AND (s.slot_id = msp.slot_id))
          AND (msp.module_id = pp.module_id))
          AND (pp.physical_port_id = pi.physical_port_id))
          AND (pi.interface_id = i.interface_id))
```

```
          AND ((i.table_subtype)::text = 'RADIO_INTERFACE'::text)))
        l2 LEFT JOIN
          (SELECT radio_interface.interface_id
          AS radioif_id, radio_interface.radio_type, radio_interface.is_enabled,
radio_interface.is_auto_channel, radio_interface.tx_power,
radio_interface.channel_number, radio_interface.max_data_rate,
radio_interface.beacon_rate, radio_interface.dtim, radio_interface.rts_threshold,
radio_interface.is_turbo_mode, radio_interface.radio_g_mode,
radio_interface.max_associated_clients
           FROM radio_interface)
        wireless ON ((l2.interface_id = wireless.radioif_id)));
```

WIRED_INTERFACE

```
CREATE VIEW wired_interface AS
    select
L2.DEVICE_ID,
L2.MANAGED_ELEMENT_ID,
L2.DEVICE_IP_ADDRESS,
L2.PHYSICAL_DEVICE_ID,
L2.UNIT_NUMBER,
L2.SLOT_ID,
L2.SLOT_NUM,
L2.MODULE_ID,
L2.PHYSICAL_PORT_ID,
L2.PORT_NUM,
L2.INTERFACE_ID,
L2.NAME,
L2.IF_NAME,
L2.IDENTIFIER,
L2.TABLE_SUBTYPE,
case
    when L2.TABLE_SUBTYPE like 'GBIT_ETHERNET_INTERFACE' then 'GIGABIT ETHERNET'
    when L2.TABLE_SUBTYPE like 'POS_INTERFACE' then 'POS'
    else L2.TABLE_SUBTYPE
end as TABLE_SUBTYPE_TXT,
L2.TAG_MODE,
case
    when L2.TAG_MODE = 1 then 'TAGGED'
    when L2.TAG_MODE = 2 then 'UNTAGGED'
    when L2.TAG_MODE = 3 then 'DUAL'
    else null
end as TAG_MODE_TXT,
L2.USER_DEFINED_VALUE_1,
L2.USER_DEFINED_VALUE_2,
L2.USER_DEFINED_VALUE_3,
L2.SPEED_IN_MB,
L2.PHYSICAL_ADDRESS,
L2.DUPLEX_MODE,
case
    when L2.DUPLEX_MODE = 1 then 'HALF-DUPLEX'
    when L2.DUPLEX_MODE = 2 then 'FULL-DUPLEX'
    when L2.DUPLEX_MODE = 3 then 'AUTO-SENSE'
    else null
end as DUPLEX_MODE_TXT,
L3.IP_ID,
L3.IP_INTERFACE_ID,
L3.IP_ADDRESS,
```

```
L3.SUBNET_MASK
from ( select distinct D.DEVICE_ID, D.MANAGED_ELEMENT_ID, D.IP_ADDRESS as
DEVICE_IP_ADDRESS,
            PD.PHYSICAL_DEVICE_ID, PD.UNIT_NUMBER, S.SLOT_ID, S.SLOT_NUM,
            MSP.MODULE_ID, PP.PHYSICAL_PORT_ID, PP.PORT_NUM, I.INTERFACE_ID,
            I.NAME, I.IF_NAME, I.IDENTIFIER, I.TABLE_SUBTYPE, I.TAG_MODE,
          I.USER_DEFINED_VALUE_1, I.USER_DEFINED_VALUE_2,
I.USER_DEFINED_VALUE_3,
            PI.SPEED_IN_MB, PI.PHYSICAL_ADDRESS, PI.DUPLEX_MODE
           from DEVICE D, PHYSICAL_DEVICE PD, SLOT S, MODULE_SLOT_PRESENT MSP,
            PHYSICAL_PORT PP, PHYSICAL_INTERFACE PI, INTERFACE I
          where D.DEVICE_ID = PD.DEVICE_ID and PD.PHYSICAL_DEVICE_ID =
S.PHYSICAL_DEVICE_ID and S.SLOT_ID = MSP.SLOT_ID and MSP.MODULE_ID = PP.MODULE_ID
and PP.PHYSICAL_PORT_ID = PI.PHYSICAL_PORT_ID and PI.INTERFACE_ID =
I.INTERFACE_ID and I.TABLE_SUBTYPE::TEXT <> 'RADIO_INTERFACE'::TEXT) L2
   left join ( select INM_IP_INTERFACE.INTERFACE_ID as IP_ID,
            INM_IP_INTERFACE.IP_INTERFACE_ID, INM_IP_INTERFACE.IP_ADDRESS,
            INM_IP_INTERFACE.SUBNET_MASK
           from INM_IP_INTERFACE) L3 on L2.INTERFACE_ID = L3.IP_ID;
```

CEE_PORT_INFO

```
create or replace view CEE_PORT_INFO as
CREATE VIEW cee_port_info AS
    select
     GIGE_PORT.ID,
     GIGE_PORT.SWITCH_PORT_ID,
     GIGE_PORT.PORT_NUMBER,
     CEE_PORT.ID AS CEE_PORT_ID,
     CEE_PORT.VIRTUAL_SWITCH_ID,
     CEE_PORT.IF_INDEX,
     CEE_PORT.IF_NAME,
     CEE_PORT.IF_MODE,
     CEE_PORT.L2_MODE,
     CEE_PORT.VLAN_ID,
     CEE_PORT.LAG_ID,
     CEE_PORT.IP_ADDRESS,
     CEE_PORT.MAC_ADDRESS,
     CEE_PORT.PORT_SPEED,
     CEE_PORT.ENABLED,
     CEE_PORT.OCCUPIED,
     CEE_PORT.LAST_UPDATE,
     CEE_PORT.NET_MASK,
     CEE_PORT.PROTOCOL_DOWN_REASON,
     CEE_PORT.MAC_ACL_POLICY,
     CEE_PORT.QOS_TYPE,
     CEE_PORT.QOS_NAME,
     CEE_PORT.DOT1X_ENABLED,
     CEE_PORT.PORT_ROLE,
     CEE_PORT.AMPP_PROFILE_MODE,
     CORE_SWITCH.IP_ADDRESS as PHYSICAL_SWITCH_IP,
     CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN,
     GIGE_PORT.OPERATIONAL_STATUS,
     GIGE_PORT.MAX_SPEED,
     GIGE_PORT.PORT_TYPE,
     GIGE_PORT.REMOTE_MAC_ADDRESS,
     GIGE_PORT.SLOT_NUMBER,
     VIRTUAL_SWITCH.WWN,
     VIRTUAL_SWITCH.MANAGEMENT_STATE,
```

```
    VIRTUAL_SWITCH.MANAGED_ELEMENT_ID,
    VIRTUAL_SWITCH.MONITORED,
    SWITCH_PORT.USER_PORT_NUMBER,
    SWITCH_PORT.STATE,
    SWITCH_PORT.STATUS,
    SWITCH_PORT.NAME,
    SWITCH_PORT.LICENSED,
    SWITCH_PORT.TRUNKED,
    SWITCH_PORT.TRUNK_MASTER,
    SWITCH_PORT.SPEED_TYPE
from
    CEE_PORT, GIGE_PORT, SWITCH_PORT, VIRTUAL_SWITCH, CORE_SWITCH
where
    CEE_PORT.GIGE_PORT_ID = GIGE_PORT.ID
    and GIGE_PORT.SWITCH_PORT_ID = SWITCH_PORT.ID
    and SWITCH_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
    and VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID;
```

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Z