

Enterasys®

Fixed Switching

Configuration Guide

Firmware 6.61.xx and Higher

Notice

Enterasys Networks reserves the right to make changes in specifications and other information contained in this document and its web site without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this document is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS DOCUMENT, WEB SITE, OR THE INFORMATION CONTAINED IN THEM, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNEW OF, OR SHOULD HAVE KNOWN OF, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.
50 Minuteman Road
Andover, MA 01810

© 2012 Enterasys Networks, Inc. All rights reserved.

Part Number: 9034662-02 October 2012

ENTERASYS, ENTERASYS NETWORKS, ENTERASYS SECURE NETWORKS, NETSIGHT, ENTERASYS NETSIGHT, and any logos associated therewith, are trademarks or registered trademarks of Enterasys Networks, Inc., in the United States and/or other countries. For a complete list of Enterasys trademarks, see <http://www.enterasys.com/company/trademarks.aspx>.

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

Documentation URL: <https://extranet.enterasys.com/downloads/>

Enterasys Networks, Inc. Firmware License Agreement

BEFORE OPENING OR UTILIZING THE ENCLOSED PRODUCT, CAREFULLY READ THIS LICENSE AGREEMENT.

This document is an agreement (“Agreement”) between the end user (“You”) and Enterasys Networks, Inc., on behalf of itself and its Affiliates (as hereinafter defined) (“Enterasys”) that sets forth Your rights and obligations with respect to the Enterasys software program/firmware (including any accompanying documentation, hardware or media) (“Program”) in the package and prevails over any additional, conflicting or inconsistent terms and conditions appearing on any purchase order or other document submitted by You. “Affiliate” means any person, partnership, corporation, limited liability company, other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. This Agreement constitutes the entire understanding between the parties, with respect to the subject matter of this Agreement. The Program may be contained in firmware, chips or other media.

BY INSTALLING OR OTHERWISE USING THE PROGRAM, YOU REPRESENT THAT YOU ARE AUTHORIZED TO ACCEPT THESE TERMS ON BEHALF OF THE END USER (IF THE END USER IS AN ENTITY ON WHOSE BEHALF YOU ARE AUTHORIZED TO ACT, “YOU” AND “YOUR” SHALL BE DEEMED TO REFER TO SUCH ENTITY) AND THAT YOU AGREE THAT YOU ARE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES, AMONG OTHER PROVISIONS, THE LICENSE, THE DISCLAIMER OF WARRANTY AND THE LIMITATION OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT OR ARE NOT AUTHORIZED TO ENTER INTO THIS AGREEMENT, ENTERASYS IS UNWILLING TO LICENSE THE PROGRAM TO YOU AND YOU AGREE TO RETURN THE UNOPENED PRODUCT TO ENTERASYS OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT ENTERASYS NETWORKS, LEGAL DEPARTMENT AT (978) 684-1000.

You and Enterasys agree as follows:

1. **LICENSE.** You have the non-exclusive and non-transferable right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this Agreement.
2. **RESTRICTIONS.** Except as otherwise authorized in writing by Enterasys, You may not, nor may You permit any third party to:
 - (a) Reverse engineer, decompile, disassemble or modify the Program, in whole or in part, including for reasons of error correction or interoperability, except to the extent expressly permitted by applicable law and to the extent the parties shall not be permitted by that applicable law, such rights are expressly excluded. Information necessary to achieve interoperability or correct errors is available from Enterasys upon request and upon payment of Enterasys’ applicable fee.
 - (b) Incorporate the Program in whole or in part, in any other product or create derivative works based on the Program, in whole or in part.
 - (c) Publish, disclose, copy reproduce or transmit the Program, in whole or in part.
 - (d) Assign, sell, license, sublicense, rent, lease, encumber by way of security interest, pledge or otherwise transfer the Program, in whole or in part.
 - (e) Remove any copyright, trademark, proprietary rights, disclaimer or warning notice included on or embedded in any part of the Program.
3. **APPLICABLE LAW.** This Agreement shall be interpreted and governed under the laws and in the state and federal courts of the Commonwealth of Massachusetts without regard to its conflicts of laws provisions. You accept the personal jurisdiction and venue of the Commonwealth of Massachusetts courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.
4. **EXPORT RESTRICTIONS.** You understand that Enterasys and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the product is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Program is exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Program and agree that You will use the Program for civil end uses only and not for military purposes.

If the Program is exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Section 1 or 2 of this Agreement, You agree not to (i) reexport or release the Program, the source code for the Program or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Cambodia, Cuba, Georgia, Iraq, Kazakhstan, Laos, Libya, Macau,

Moldova, Mongolia, North Korea, the People's Republic of China, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Program or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant or any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

5. **UNITED STATES GOVERNMENT RESTRICTED RIGHTS.** The enclosed Program (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Program is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

6. **DISCLAIMER OF WARRANTY.** EXCEPT FOR THOSE WARRANTIES EXPRESSLY PROVIDED TO YOU IN WRITING BY ENTERASYS, ENTERASYS DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT WITH RESPECT TO THE PROGRAM. IF IMPLIED WARRANTIES MAY NOT BE DISCLAIMED BY APPLICABLE LAW, THEN ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO THIRTY (30) DAYS AFTER DELIVERY OF THE PROGRAM TO YOU.

7. **LIMITATION OF LIABILITY.** IN NO EVENT SHALL ENTERASYS OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM, EVEN IF ENTERASYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS FOREGOING LIMITATION SHALL APPLY REGARDLESS OF THE CAUSE OF ACTION UNDER WHICH DAMAGES ARE SOUGHT.

THE CUMULATIVE LIABILITY OF ENTERASYS TO YOU FOR ALL CLAIMS RELATING TO THE PROGRAM, IN CONTRACT, TORT OR OTHERWISE, SHALL NOT EXCEED THE TOTAL AMOUNT OF FEES PAID TO ENTERASYS BY YOU FOR THE RIGHTS GRANTED HEREIN.

8. **AUDIT RIGHTS.** You hereby acknowledge that the intellectual property rights associated with the Program are of critical value to Enterasys, and, accordingly, You hereby agree to maintain complete books, records and accounts showing (i) license fees due and paid, and (ii) the use, copying and deployment of the Program. You also grant to Enterasys and its authorized representatives, upon reasonable notice, the right to audit and examine during Your normal business hours, Your books, records, accounts and hardware devices upon which the Program may be deployed to verify compliance with this Agreement, including the verification of the license fees due and paid Enterasys and the use, copying and deployment of the Program. Enterasys' right of examination shall be exercised reasonably, in good faith and in a manner calculated to not unreasonably interfere with Your business. In the event such audit discovers non-compliance with this Agreement, including copies of the Program made, used or deployed in breach of this Agreement, You shall promptly pay to Enterasys the appropriate license fees. Enterasys reserves the right, to be exercised in its sole discretion and without prior notice, to terminate this license, effective immediately, for failure to comply with this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

9. **OWNERSHIP.** This is a license agreement and not an agreement for sale. You acknowledge and agree that the Program constitutes trade secrets and/or copyrighted material of Enterasys and/or its suppliers. You agree to implement reasonable security measures to protect such trade secrets and copyrighted material. All right, title and interest in and to the Program shall remain with Enterasys and/or its suppliers. All rights not specifically granted to You shall be reserved to Enterasys.

10. **ENFORCEMENT.** You acknowledge and agree that any breach of Sections 2, 4, or 9 of this Agreement by You may cause Enterasys irreparable damage for which recovery of money damages would be inadequate, and that Enterasys may be entitled to seek timely injunctive relief to protect Enterasys' rights under this Agreement in addition to any and all remedies available at law.

11. **ASSIGNMENT.** You may not assign, transfer or sublicense this Agreement or any of Your rights or obligations under this Agreement, except that You may assign this Agreement to any person or entity which acquires substantially all of Your stock assets. Enterasys may assign this Agreement in its sole discretion. This Agreement shall be binding upon and inure to the benefit of the parties, their legal representatives, permitted transferees, successors and assigns as permitted by this Agreement. Any attempted assignment, transfer or sublicense in violation of the terms of this Agreement shall be void and a breach of this Agreement.

12. **WAIVER.** A waiver by Enterasys of a breach of any of the terms and conditions of this Agreement must be in writing and will not be construed as a waiver of any subsequent breach of such term or condition. Enterasys' failure to enforce a term upon Your breach of such term shall not be construed as a waiver of Your breach or prevent enforcement on any other occasion.

13. **SEVERABILITY.** In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired thereby, and that provision shall be reformed, construed and enforced to the maximum extent permissible. Any such invalidity, illegality, or unenforceability in any jurisdiction shall not invalidate or render illegal or unenforceable such provision in any other jurisdiction.

14. **TERMINATION.** Enterasys may terminate this Agreement immediately upon Your breach of any of the terms and conditions of this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

Contents

Chapter 1: Setting Up a Switch for the First Time

Before You Begin	1-1
Connecting to the Switch	1-2
Downloading New Firmware	1-3
Deleting a Backup Image File	1-5
Additional Configuration Tasks	1-5
Setting User Accounts and Passwords	1-5
Controlling In-band Access to the Switch	1-6
Changing SNMP Defaults	1-7
Saving the Configuration and Connecting Devices	1-7
Configuring a Stack of New Switches	1-8
Where to Go Next	1-9
Getting Help	1-10
Downloading Firmware via the Serial Port	1-10

Chapter 2: Configuring Switches in a Stack

About Switch Operation in a Stack	2-1
Stack Initialization	2-1
Configuration Management	2-2
Installing a New Stackable System of Up to Eight Units	2-2
Installing Previously-Configured Systems in a Stack	2-3
Adding a New Unit to an Existing Stack	2-3
Removing Units from an Existing Stack	2-4
Stack Disruption Times	2-4
Creating a Virtual Switch Configuration	2-4
Example	2-5
Considerations About Using “clear config” in a Stack	2-5
Configuring Standalone A4 Stack Ports	2-6
When Uplink Ports are Configured as Ethernet Ports	2-6

Chapter 3: CLI Basics

Switch Management Methods	3-1
Using the Command Line Interface	3-1
Starting a CLI Session	3-1
Connecting Using the Console Port	3-2
Connecting Using Telnet or SSH.....	3-2
Logging In	3-3
Using a Default User Account	3-3
Using an Administratively Configured User Account	3-3
Clearing and Closing the CLI	3-3
Navigating the Command Line Interface	3-3
Getting Help with CLI Syntax.....	3-3
CLI Command Defaults Descriptions	3-3
CLI Command Modes.....	3-4
Performing Keyword Lookups	3-4
Displaying Scrolling Screens	3-5
Abbreviating and Completing Commands	3-5
Basic Line Editing Commands.....	3-6
Configuring CLI Properties	3-6
Example CLI Properties Configuration	3-7

CLI Properties Display Commands	3-7
---------------------------------------	-----

Chapter 4: System Configuration

Factory Default Settings	4-1
Initial Configuration Overview	4-5
Advanced Configuration Overview	4-6
Licensing Advanced Features	4-8
License Implementation Differences	4-8
Node-Locked Licensing	4-9
Non-Node-Locked Licensing	4-9
Licensing in a Stack Environment	4-9
Applying Node-Locked Licenses in a Stack	4-10
Applying Non-Node-Locked Licenses in a Stack	4-10
Adding a New Member to a Licensed Stack	4-11
Displaying and Clearing Licenses	4-11
SNTP Configuration	4-11
Unicast Polling Mode	4-12
Broadcast Listening Mode	4-12
SNTP Authentication	4-12
Authentication Key and Trusted Key List	4-12
SNTP Defaults	4-13
Configuring SNTP	4-13
SNTP Configuration Example	4-15
DHCP Configuration	4-16
DHCP Relay Agent	4-16
DHCP Server	4-16
IP Address Pools	4-17
Automatic IP Address Pools	4-17
Manual IP Address Pools	4-17
Configuring a DHCP Server	4-17
DHCP Configuration on a Non-Routing System	4-18
DHCP Configuration on a Routing System	4-18
Managing and Displaying DHCP Server Parameters	4-20
DHCP Server Defaults	4-20
Configuring DHCP IP Address Pools	4-21
Automatic IP Address Pool Configuration	4-21
Manual IP Pool Configuration	4-21
Configuring Additional Pool Parameters	4-23
Telnet Overview	4-23
Configuring Telnet	4-24
SSH Overview	4-24
Configuring SSH	4-24
MAC Address Settings	4-24
Age Time	4-24
Limiting MAC Addresses to Specific VLANs	4-25
Setting the MAC Algorithm Mode	4-25
New MAC Address Detection	4-25
Configuring Node Aliases	4-26

Chapter 5: User Account and Password Management

User Account Overview	5-1
Emergency Access User Account	5-2
Account Lockout	5-3
Port Lockout	5-3
User Account Configuration	5-3

Password Management Overview	5-6
System Level Password Settings	5-6
Defaults	5-7
System Password Settings Configuration	5-8
Password Reset Button Functionality	5-9
Management Authentication Notification MIB Functionality	5-9

Chapter 6: Firmware Image and File Management

Managing the Firmware Image	6-1
Downloading a Firmware Image	6-1
Downloading from a TFTP or SFTP Server.....	6-2
Setting the Boot Firmware	6-3
Reverting to a Previous Image	6-3
Setting TFTP Parameters	6-4
Managing Switch Configuration and Files	6-4
Configuration Persistence Mode	6-4
Using an I-Series Memory Card	6-5
Memory Card Operation.....	6-5
Displaying and Saving the Configuration and Creating a Backup	6-5
Displaying the Configuration.....	6-6
Creating a Backup Configuration File.....	6-6
Applying a Saved Configuration	6-7
Managing Files	6-8

Chapter 7: Configuring System Power and PoE

Configuring Redundant Power Supplies	7-1
Power over Ethernet Overview	7-1
Implementing PoE	7-2
Allocation of PoE Power to Modules	7-2
When Manual Mode is Configured	7-3
Management of PoE Power to PDs	7-3
Configuring PoE	7-4
Stackable A4, B3, and C3 Devices	7-5
Stackable B5 and C5 Devices	7-6
G-Series Devices	7-7
Example PoE Configuration	7-10
PoE Display Commands	7-10

Chapter 8: Port Configuration

Port Configuration Overview	8-1
Port String Syntax Used in the CLI	8-1
Examples.....	8-2
Console Port Settings	8-2
VT100 Terminal Mode.....	8-3
Port Settings	8-3
Port Status.....	8-3
Port Name or Alias	8-3
Auto-Negotiation and Advertised Ability	8-4
Port Speed and Duplex Mode	8-4
MDI / MDIX Cable Type.....	8-4
Port Flow Control.....	8-5
Jumbo Frame Support.....	8-5
Broadcast Suppression Threshold	8-5
Protected Port Mode.....	8-6
Displaying Port Status	8-6

Displaying Cable Status	8-7
Configuring SFP Ports for 100BASE-FX	8-7
Example.....	8-8
Configuring Port Link Flap Detection	8-8
Basic Link Flap Detection Configuration	8-9
Example	8-10
Link Flap Detection Display Commands	8-11
Transmit Queue Monitoring	8-11
Port Mirroring	8-12
Mirroring Features	8-12
Configuring Port Mirroring	8-13
Remote Port Mirroring	8-13
Configuring Remote Port Mirroring.....	8-14
Configuring SMON MIB Port Mirroring	8-15
Procedures	8-15

Chapter 9: Configuring VLANs

VLAN Overview	9-1
Using VLANs to Partition Your Network	9-1
Implementing VLANs	9-2
Preparing for VLAN Configuration	9-3
Understanding How VLANs Operate	9-3
Learning Modes and Filtering Databases	9-3
VLAN Assignment and Forwarding	9-4
Receiving Frames from VLAN Ports.....	9-4
Forwarding Decisions	9-5
Example of a VLAN Switch in Operation	9-5
VLAN Support on Enterasys Switches	9-6
Maximum Active VLANs	9-6
Configurable Range	9-6
VLAN Types	9-6
Static and Dynamic VLANs	9-6
Port-Based VLANs	9-6
Policy-Based VLANs	9-7
GARP VLAN Registration Protocol (GVRP) Support	9-7
How It Works	9-7
Configuring VLANs	9-8
Default Settings	9-9
Configuring Static VLANs	9-9
Example Configuration	9-11
Creating a Secure Management VLAN	9-11
Configuring Dynamic VLANs	9-12
Configuring Protocol-Based VLAN Classification	9-13
Example Configuration	9-13
Monitoring VLANs	9-14
Terms and Definitions	9-14

Chapter 10: Configuring User Authentication

User Authentication Overview	10-1
Implementing User Authentication	10-2
Authentication Methods	10-2
IEEE 802.1x Using EAP	10-2
MAC-Based Authentication (MAC)	10-2
Port Web Authentication (PWA)	10-3
Multi-User And MultiAuth Authentication	10-3

Remote Authentication Dial-In Service (RADIUS)	10-7
How RADIUS Data Is Used	10-8
The RADIUS Filter-ID	10-8
RFC 3580 — VLAN Authorization	10-8
Policy Mappable Response	10-10
Configuring Authentication	10-12
Configuring IEEE 802.1x	10-14
Configuring MAC-based Authentication	10-15
Configuring Port Web Authentication (PWA)	10-16
Optionally Enable Guest Network Privileges	10-17
Configuring MultiAuth Authentication	10-17
Setting MultiAuth Authentication Mode	10-17
Setting MultiAuth Authentication Precedence	10-18
Setting MultiAuth Authentication Port Properties	10-18
Setting MultiAuth Authentication Timers	10-19
Displaying MultiAuth Configuration Information	10-20
Configuring VLAN Authorization	10-20
Configuring RADIUS	10-21
Configuring the Authentication Server	10-21
Configuring User + IP Phone Authentication	10-22
Example	10-23
Authentication Configuration Example	10-25
Configuring MultiAuth Authentication	10-26
Enabling RADIUS On the Switch	10-26
Creating RADIUS User Accounts on the Authentication Server	10-26
Configuring the Engineering Group 802.1x End-User Stations	10-26
Configuring the Printer Cluster for MAC-Based Authentication	10-27
Configuring the Public Area PWA Station	10-28
Terms and Definitions	10-28

Chapter 11: Configuring Link Aggregation

Link Aggregation Overview	11-1
Using Link Aggregation in a Network	11-1
Implementing Link Aggregation	11-2
LACP Operation	11-2
How a LAG Forms	11-3
Attached Ports	11-5
Single Port Attached State Rules	11-7
LAG Port Parameters	11-7
Static Port Assignment	11-8
Flexible Link Aggregation Groups	11-8
Configuring Link Aggregation	11-9
Link Aggregation Configuration Example	11-11
Configuring the S8 Distribution Switch	11-14
Configuring the Fixed Switch Stack 1	11-14
Configuring the Fixed Switch Stack 2	11-14
Configuring the Server	11-15
Terms and Definitions	11-15

Chapter 12: Configuring SNMP

SNMP Overview	12-1
Implementing SNMP	12-1
SNMP Concepts	12-2
Manager/Agent Model Components	12-2
Message Functions	12-2

Trap Versus Inform Messages	12-3
Access to MIB Objects	12-3
Community Name Strings.....	12-3
User-Based.....	12-3
SNMP Support on Enterasys Switches	12-3
Versions Supported	12-4
SNMPv1 andv2c Network Management Components	12-4
SNMPv3 User-Based Security Model (USM) Enhancements	12-4
Terms and Definitions	12-5
Security Models and Levels	12-6
Access Control	12-6
Configuring SNMP	12-7
Configuration Basics	12-7
How SNMP Processes a Notification Configuration	12-7
SNMP Defaults	12-8
Device Start Up Configuration	12-8
Configuring SNMPv1/SNMPv2c	12-9
Creating a New Configuration	12-9
Adding to or Modifying the Default Configuration	12-10
Configuring SNMPv3	12-10
Configuring an SNMPv3 Inform or Trap Engine ID	12-13
Configuring an SNMP View	12-14
Configuring Secure SNMP Community Names	12-15
Example.....	12-17
Reviewing SNMP Settings	12-18

Chapter 13: Configuring Neighbor Discovery

Neighbor Discovery Overview	13-1
Neighbor Discovery Operation	13-1
LLDP-MED	13-3
LLDPDU Frames	13-5
Configuring LLDP	13-7
LLDP Configuration Commands	13-7
Basic LLDP Configuration	13-9
Example LLDP Configuration: Time to Live.....	13-9
Example LLDP Configuration: Location Information.....	13-9
LLDP Display Commands	13-10
Configuring Enterasys Discovery Protocol	13-10
Enterasys Discovery Protocol Configuration Commands	13-10
Example Enterasys Discovery Protocol Configuration	13-11
Enterasys Discovery Protocol Show Commands	13-11
Configuring Cisco Discovery Protocol	13-11
Cisco Discovery Protocol Configuration Commands	13-12
Example Cisco Discovery Protocol Configuration	13-12
Cisco Discovery Protocol Configuration Commands	13-12

Chapter 14: Configuring Syslog

System Logging Overview	14-1
Syslog Operation	14-2
Syslog Operation on Enterasys Devices	14-2
Filtering by Severity and Facility	14-2
Syslog Components and Their Use	14-3
Basic Syslog Scenario	14-5
Interpreting Messages	14-6
Example	14-6

About Security Audit Logging	14-6
Security Events Logged	14-7
Trap Generation	14-7
Format Examples	14-8
Configuring Syslog	14-8
Syslog Command Precedence	14-8
About Server and Application Severity Levels	14-9
Configuring Syslog Server(s)	14-9
Example.....	14-9
Modifying Syslog Server Defaults	14-10
Displaying System Logging Defaults	14-10
Modifying Default Settings.....	14-10
Reviewing and Configuring Logging for Applications	14-10
Displaying Current Application Severity Levels	14-11
Enabling Console Logging and File Storage	14-11
Displaying to the Console and Saving to a File	14-11
Configuration Examples	14-12
Enabling a Server and Console Logging.....	14-12
Adjusting Settings to Allow for Logging at the Debug Level.....	14-12

Chapter 15: Configuring Spanning Tree

Spanning Tree Protocol Overview	15-1
Why Use Spanning Trees?	15-2
Spanning Tree on Enterasys Platforms	15-2
STP Operation	15-3
Rapid Spanning Tree Operation	15-4
Multiple Spanning Tree Operation	15-4
Functions and Features Supported on Enterasys Devices	15-6
Spanning Tree Versions	15-6
Maximum SID Capacities	15-6
Network Diameter	15-6
Port Forwarding	15-6
Disabling Spanning Tree	15-7
STP Features	15-7
SpanGuard	15-7
Loop Protect	15-7
Updated 802.1t.....	15-8
Multisource Detection.....	15-8
Spanning Tree Basics	15-9
Spanning Tree Bridge Protocol Data Units	15-9
Electing the Root Bridge	15-9
Assigning Path Costs	15-9
Paths to Root	15-10
Identifying Designated, Alternate, and Backup Port Roles	15-12
Assigning Port States	15-13
RSTP Operation	15-14
MSTP Operation	15-14
Common and Internal Spanning Tree (CIST).....	15-14
MST Region.....	15-15
Multiple Spanning Tree Instances (MSTI)	15-16
Configuring STP and RSTP	15-19
Reviewing and Enabling Spanning Tree	15-20
Example.....	15-20
Adjusting Spanning Tree Parameters	15-20
Setting Bridge Priority Mode and Priority.....	15-21

Setting a Port Priority.....	15-21
Assigning Port Costs	15-22
Adjusting Bridge Protocol Data Unit (BPDU) Intervals	15-22
Enabling the Backup Root Function	15-23
Adjusting RSTP Parameters	15-23
Defining Edge Port Status	15-24
Configuring MSTP	15-24
Example 1: Configuring MSTP for Traffic Segregation	15-25
Example 2: Configuring MSTP for Maximum Bandwidth Utilization	15-27
Adjusting MSTP Parameters	15-28
Monitoring MSTP	15-29
Understanding and Configuring SpanGuard	15-29
What Is SpanGuard?	15-29
How Does It Operate?	15-30
Configuring SpanGuard	15-30
Reviewing and Setting Edge Port Status.....	15-30
Enabling and Adjusting SpanGuard	15-30
Monitoring SpanGuard Status and Settings	15-31
Understanding and Configuring Loop Protect	15-31
What Is Loop Protect?	15-31
How Does It Operate?	15-31
Port Modes and Event Triggers.....	15-32
Example: Basic Loop Protect Configuration	15-32
..... Configuring Loop Protect	15-33
Enabling or Disabling Loop Protect	15-34
Specifying Loop Protect Partners	15-34
Setting the Loop Protect Event Threshold and Window	15-34
Enabling or Disabling Loop Protect Event Notifications	15-35
Setting the Disputed BPDU Threshold	15-35
Monitoring Loop Protect Status and Settings	15-35
Terms and Definitions	15-36

Chapter 16: Configuring Policy

Using Policy in Your Network	16-1
Standard and Enhanced Policy on Enterasys Platforms	16-2
Implementing Policy	16-2
Policy Configuration Overview	16-2
Using the Enterasys NetSight Policy Manager	16-2
Understanding Roles in a Secure Network	16-3
The Policy Role	16-3
Defining Policy Roles	16-3
Setting a Default VLAN for a Role.....	16-4
Adding Tagged, Untagged, and Forbidden Ports to the VLAN Egress Lists	16-4
Assigning a Class of Service to a Role.....	16-4
Defining Policy Rules	16-5
Admin Rules	16-5
Traffic Classification Rules	16-5
Applying Policy	16-7
Applying a Default Policy.....	16-8
Applying Policies Dynamically	16-8
Blocking Non-Edge Protocols at the Edge Network Layer	16-8
Configuring Policy	16-9
Policy Configuration Example	16-12
Roles	16-13
Policy Domains	16-13

Basic Edge	16-13
Standard Edge.....	16-14
Premium Edge.....	16-14
Premium Distribution	16-14
Platform Configuration	16-14
Configuring Guest Policy on Edge Platforms	16-15
Configuring Policy for the Edge Student Fixed Switch	16-15
Configuring PhoneFS Policy for the Edge Fixed Switch.....	16-16
Configuring Policy for the Edge Faculty Fixed Switch	16-17
Terms and Definitions	16-18

Chapter 17: Configuring Quality of Service

Quality of Service Overview	17-1
Implementing QoS	17-1
Quality of Service Operation	17-2
Class of Service (CoS)	17-2
CoS Settings	17-3
CoS Hardware Resource Reference	17-3
CoS Flood Control State.....	17-3
CoS Priority and ToS Rewrite.....	17-3
CoS Reference	17-4
Port Group and Type	17-4
CoS Settings Reference to Port Resource Mapping	17-5
Port Resources	17-5
Port Configuration	17-5
Preferential Queue Treatment for Packet Forwarding	17-6
Strict Priority Queuing.....	17-6
Weighted Fair Queuing.....	17-6
Hybrid Queuing.....	17-7
Rate Limiting	17-8
Flood Control	17-9
CoS Hardware Resource Configuration	17-9
IRL Configuration	17-9
CoS Port Configuration Layer.....	17-9
CoS Port Resource Layer.....	17-10
CoS Reference Layer	17-10
CoS Settings Layer.....	17-10
Enable CoS State	17-10
IRL Configuration Example Show Command Output	17-10
Flood Control Configuration	17-12
CoS Port Configuration Layer.....	17-12
CoS Port Resource Layer.....	17-12
CoS Reference Layer	17-12
CoS Settings Layer.....	17-12
Enable CoS State	17-12
Flood Control Configuration Example Show Command Output	17-12
Enabling CoS State	17-13
The QoS CLI Command Flow	17-14
Port Priority and Transmit Queue Configuration	17-15
Setting Port Priority	17-15
Example.....	17-15
Mapping Port Priority to Transmit Queues	17-15
Example.....	17-16
Setting Transmit Queue Arbitration	17-16
Port Traffic Rate Limiting	17-17

Examples	17-18
----------------	-------

Chapter 18: Configuring Network Monitoring

Basic Network Monitoring Features	18-1
Console/Telnet History Buffer	18-1
Network Diagnostics	18-2
Switch Connection Statistics	18-2
Users	18-3
RMON	18-3
RMON Design Considerations	18-4
Configuring RMON	18-5
sFlow	18-9
Using sFlow in Your Network	18-10
Definitions	18-10
sFlow Agent Functionality	18-11
Sampling Mechanisms	18-11
Packet Flow Sampling	18-11
Counter Sampling	18-11
Sampling Implementation Notes	18-12
Configuring sFlow	18-12
Overview	18-12
Procedure	18-14

Chapter 19: Configuring Multicast

Using Multicast in Your Network	19-1
Implementing Multicast	19-1
Multicast Operation	19-2
Internet Group Management Protocol (IGMP)	19-2
Overview	19-2
IGMP Support on Enterasys Devices	19-3
Example: Sending a Multicast Stream	19-4
Distance Vector Multicast Routing Protocol (DVMRP)	19-5
Overview	19-5
DVMRP Support on Enterasys Devices	19-5
Protocol Independent Multicast (PIM)	19-11
Overview	19-11
PIM Support on Enterasys Devices	19-13
PIM Terms and Definitions	19-14
Configuring IGMP	19-15
Basic IGMP Configuration	19-17
Example IGMP Configuration on Layer 3	19-17
IGMP Display Commands	19-18
Configuring DVMRP	19-18
DVMRP Configuration Commands	19-18
Basic DVMRP Configuration	19-19
Example DVMRP Configuration	19-19
Displaying DVMRP Information	19-20
Configuring PIM-SM	19-21
Design Considerations	19-21
PIM-SM Configuration Commands	19-21
Basic PIM-SM Configuration	19-22
Example Configuration	19-22
PIM-SM Display Commands	19-24

Chapter 20: IP Configuration

Enabling the Switch for Routing	20-1
Router Configuration Modes	20-1
Entering Router Configuration Modes	20-2
Example	20-3
Routing Interfaces	20-3
IPv4 Interface Addresses	20-3
IP Static Routes	20-4
Configuring Static Routes	20-5
Testing Network Connectivity	20-5
The ARP Table	20-6
Proxy ARP	20-7
ARP Configuration	20-7
IP Broadcast Settings	20-7
Directed Broadcast	20-7
UDP Broadcast Forwarding	20-8
DHCP and BOOTP Relay	20-9
IP Broadcast Configuration	20-9
Configuring ICMP Redirects	20-10
Terms and Definitions	20-10

Chapter 21: IPv4 Basic Routing Protocols

Configuring RIP	21-1
Using RIP in Your Network	21-1
RIP Configuration Overview	21-1
RIP Router Configuration	21-1
RIP Interface Configuration	21-2
RIP Configuration Example	21-3
Configuring IRDP	21-5
Using IRDP in Your Network	21-5
IRDP Configuration Overview	21-5
IRDP Configuration Example	21-5

Chapter 22: Configuring OSPFv2

OSPF Overview	22-1
OSPF Areas	22-2
OSPF Router Types	22-3
Designated Router	22-3
Authentication	22-3
Basic OSPF Topology Configuration	22-3
Configuring the Router ID	22-4
Configuring the Designated Router	22-5
Configuring Router Priority	22-6
Example.....	22-6
Configuring the Administrative Distance for OSPF Routes	22-7
Configuring SPF Timers	22-7
Configuring OSPF Areas	22-8
Configuring Area Range	22-8
Example.....	22-8
Configuring a Stub Area	22-9
Stub Area Default Route Cost	22-10
Example.....	22-10
Configuring a Not So Stubby Area (NSSA)	22-11
Example.....	22-12
Configuring Area Virtual-Links	22-12

Configuring Area Virtual-Link Authentication	22-14
Configuring Area Virtual-Link Timers	22-14
Configuring Route Redistribution	22-14
Configuring Passive Interfaces	22-14
Configuring OSPF Interfaces	22-15
Configuring Interface Cost	22-15
Configuring Interface Priority	22-15
Configuring Authentication	22-15
Configuring OSPF Interface Timers	22-16
Default Settings	22-16
Configuration Procedures	22-17
Basic OSPF Router Configuration	22-17
OSPF Interface Configuration	22-18
OSPF Area Configuration	22-18
Managing and Displaying OSPF Configuration and Statistics	22-19

Chapter 23: Configuring VRRP

VRRP Overview	23-1
VRRP Virtual Router Creation	23-2
VRRP Master Election	23-2
Enabling Master Preemption	23-3
Enabling ICMP Replies	23-3
Configuring VRRP Authentication	23-3
Enabling the VRRP Virtual Router	23-3
Configuring VRRP	23-3
Configuration Examples	23-4
Basic VRRP Configuration	23-4
Multiple Backup VRRP Configuration	23-6
Terms and Definitions	23-8

Chapter 24: Configuring Access Control Lists

Using Access Control Lists (ACLs) in Your Network	24-1
Implementing ACLs	24-1
ACL Configuration Overview	24-2
Creating IPv4 ACLs	24-2
Creating IPv6 and MAC ACLs	24-2
Creating ACL Rules	24-3
IPv4 Rules	24-3
IPv6 Rules	24-4
MAC Rules	24-4
Managing ACLs	24-4
Deleting ACLs and Rules	24-4
Moving ACL Rules	24-5
Replacing ACL Rules	24-5
Inserting ACL Rules	24-6
Applying ACLs	24-6
Configuring ACLs	24-7
Configuring IPv4 ACLs	24-7
Example	24-8
Configuring IPv6 ACLs	24-8
Example	24-9
Configuring MAC ACLs	24-10
Example	24-10
Access Control Lists on the A4	24-11
Configuring A4 ACLs	24-12

Extended IPv4 ACL Configuration	24-12
MAC ACL Configuration	24-13

Chapter 25: Configuring and Managing IPv6

Managing IPv6	25-1
Configuring IPv6 Management	25-2
Example.....	25-2
Monitoring Network Connections	25-3
IPv6 Routing Configuration	25-3
Overview	25-3
Defaults	25-4
Setting Routing General Parameters	25-5
Configuring Routing Interfaces	25-5
IPv6 Addressing	25-5
Enabling an Interface for IPv6 Routing.....	25-6
Configuration Examples	25-6
Creating Tunnel Interfaces	25-7
Configuring Static Routes	25-9
Viewing Routing Information	25-10
Testing Network Connectivity	25-11
IPv6 Neighbor Discovery	25-11
Duplicate Address Detection	25-11
Neighbor Solicitation Messages	25-12
Router Advertisements	25-12
Cache Management	25-12
Neighbor Discovery Configuration	25-13
DHCPv6 Configuration	25-14
DHCPv6 Relay Agent Configuration	25-14
DHCPv6 Server Configuration	25-15
Pool Configuration	25-15
Server Configuration.....	25-15
Default Conditions	25-16
Configuration Examples	25-16
Viewing DHCPv6 Statistics	25-18

Chapter 26: Configuring Security Features

Security Mode Configuration	26-1
About the Security Mode	26-1
Configuring the Security Mode	26-2
Security Mode and SNMP	26-2
Security Mode and User Authentication and Passwords	26-3
Security Mode and System Logging	26-3
Security Mode and File Management	26-4
IPsec Configuration	26-4
About IPsec	26-4
IPsec Defaults	26-5
IPsec Configuration	26-5
RADIUS Management Authentication	26-6
Request Transmission	26-6
Response Validation	26-7
Password Changing	26-7
Example	26-7
MAC Locking	26-7
First Arrival Configuration	26-8
MAC Locking Notifications	26-8

Disabling and Enabling Ports	26-9
MAC Locking Defaults	26-9
MAC Locking Configuration	26-10
TACACS+	26-11
TACACS+ Client Functionality	26-12
Session Authorization and Accounting	26-12
Command Authorization and Accounting	26-12
Configuring the Source Address.....	26-13
Default Settings	26-13
Basic TACACS+ Configuration	26-14
Example TACACS+ Configuration	26-15
TACACS+ Display Commands	26-15
Service ACLs	26-16
Restricting Management Access to the Console Port	26-17
Configuring a Service Access Control List	26-17
DHCP Snooping	26-18
DHCP Message Processing	26-18
Building and Maintaining the Database	26-19
Rate Limiting	26-19
Basic Configuration	26-19
Configuration Notes.....	26-20
Default Parameter Values	26-20
Managing DHCP Snooping	26-21
Dynamic ARP Inspection	26-22
Functional Description	26-22
Static Mappings.....	26-22
Optional ARP Packet Validation	26-22
Logging Invalid Packets.....	26-23
Packet Forwarding.....	26-23
Rate Limiting.....	26-23
Eligible Interfaces	26-23
Interaction with Other Functions.....	26-23
Basic Configuration	26-24
Default Parameter Values	26-24
Managing Dynamic ARP Inspection	26-24
Example Configuration	26-25
Non-Routing Example	26-25
Routing Example	26-26

Figures

3-1	CLI Startup Screen	3-2
3-2	Sample CLI Defaults Description.....	3-4
3-3	Performing a Keyword Lookup	3-4
3-4	Performing a Partial Keyword Lookup	3-4
3-5	Scrolling Screen Output.....	3-5
3-6	Abbreviating a Command	3-5
9-1	VLAN Business Scenario	9-2
9-2	Inside the Switch	9-5
9-3	Example of VLAN Propagation Using GVRP	9-8
10-1	Applying Policy to Multiple Users on a Single Port.....	10-5
10-2	Authenticating Multiple Users With Different Methods on a Single Port.....	10-6
10-3	Selecting Authentication Method When Multiple Methods are Validated	10-7
10-4	Stackable Fixed Switch Authentication Configuration Example Overview	10-25
11-1	LAG Formation	11-4
11-2	LAGs Moved to Attached State	11-6

11-3	Link Aggregation Example.....	11-12
13-1	Communication between LLDP-enabled Devices	13-3
13-2	LLDP-MED	13-5
13-3	Frame Format.....	13-6
14-1	Basic System Scenario.....	14-5
15-1	Redundant Link Causes a Loop in a Non-STP Network	15-2
15-2	Loop Avoided When STP Blocks a Duplicate Path	15-2
15-3	Multiple Spanning Tree Overview.....	15-5
15-4	Root Port Selection Based On Lowest Cost or Bridge ID.....	15-10
15-5	Root Port Selection Based On Lowest Port ID	15-11
15-6	Spanning Tree Port Role Overview	15-12
15-7	Example of an MST Region.....	15-15
15-8	MSTI 1 in a Region.....	15-18
15-9	MSTI2 in the Same Region	15-18
15-10	Example of Multiple Regions and MSTIs.....	15-19
15-11	Traffic Segregation in a Single STP Network Configuration	15-25
15-12	Traffic Segregation in an MSTP Network Configuration	15-26
15-13	Maximum Bandwidth Utilization in a Single STP Network Configuration	15-27
15-14	Maximum Bandwidth in an MSTP Network Configuration	15-28
15-15	Basic Loop Protect Scenario	15-33
15-16	Spanning Tree Without Loop Protect	15-33
15-17	Spanning Tree with Loop Protect	15-33
16-1	College-Based Policy Configuration	16-12
17-1	Assigning and Marking Traffic with a Priority.....	17-4
17-2	Strict Priority Queuing Packet Behavior	17-6
17-3	Weighted Fair Queuing Packet Behavior	17-7
17-4	Hybrid Queuing Packet Behavior	17-8
17-5	Rate Limiting Clipping Behavior	17-9
19-1	IGMP Querier Determining Group Membership	19-3
19-2	Sending a Multicast Stream with No Directly Attached Hosts	19-4
19-3	DVMRP Pruning and Grafting	19-11
19-4	PIM Traffic Flow.....	19-12
19-5	DVMRP Configuration on Two Routers.....	19-19
19-6	PIM-SM Configuration	19-23
22-1	Basic OSPF Topology	22-4
22-2	OSPF Designated Router Topology	22-6
22-3	OSPF Summarization Topology	22-9
22-4	OSPF Stub Area Topology	22-10
22-5	OSPF NSSA Topology	22-12
22-6	Virtual Link Topology	22-13
23-1	Basic VRRP Topology	23-2
23-2	Basic Configuration Example	23-5
23-3	Multi-Backup VRRP Configuration Example	23-6
25-1	Basic IPv6 Over IPv4 Tunnel.....	25-8

Tables

3-1	Basic Line Editing Commands.....	3-6
3-2	CLI Properties Configuration Commands.....	3-6
3-3	CLI Properties Show Commands	3-7
4-1	Default Settings for Basic Switch Operation.....	4-1
4-2	Default Settings for Router Operation	4-4
4-3	Advanced Configuration	4-6
4-4	Default SNTP Parameters	4-13
4-5	Managing and Displaying SNTP.....	4-14
4-6	Managing and Displaying DHCP Server	4-20

4-7	Default DHCP Server Parameters	4-20
4-8	Configuring Pool Parameters	4-23
5-1	User Account and Password Parameter Defaults by Security Mode	5-7
6-1	File Management Commands	6-8
7-1	PoE Powered Device Classes	7-2
7-2	PoE Settings Supported on Enterasys Devices	7-4
7-3	PoE Show Commands	7-10
8-1	Displaying Port Status	8-7
8-2	Linkflap Default Parameters	8-9
8-3	Link Flap Detection Show Commands	8-11
8-4	Transmit Queue Monitoring Tasks	8-11
9-1	Default VLAN Parameters	9-9
9-2	Displaying VLAN Information.....	9-14
9-3	VLAN Terms and Definitions	9-14
10-1	Default Authentication Parameters.....	10-12
10-2	PWA Guest Networking Privileges Configuration.....	10-17
10-3	Displaying MultiAuth Authentication Configuration.....	10-20
10-4	Authentication Configuration Terms and Definitions	10-28
11-1	LAG2 Port Priority Assignments	11-5
11-2	LAG Port Parameters	11-7
11-3	Default Link Aggregation Parameters.....	11-9
11-4	Managing Link Aggregation.....	11-10
11-5	Displaying Link Aggregation Information and Statistics.....	11-11
11-6	LAG and Physical Port Admin Key Assignments	11-13
11-7	Link Aggregation Configuration Terms and Definitions	11-15
12-1	SNMP Message Functions	12-2
12-2	SNMP Terms and Definitions	12-5
12-3	SNMP Security Models and Levels	12-6
12-4	Default Enterasys SNMP Configuration	12-8
12-5	Commands to Review SNMP Settings	12-18
13-1	LLDP Configuration Commands.....	13-7
13-2	LLDP Show Commands	13-10
13-3	Enterasys Discovery Protocol Configuration Commands.....	13-10
13-4	Enterasys Discovery Protocol Show Commands	13-11
13-5	Cisco Discovery Protocol Configuration Commands.....	13-12
13-6	Cisco Discovery Protocol Show Commands	13-12
14-1	Syslog Terms and Definitions.....	14-3
14-2	Syslog Message Components.....	14-6
14-3	Syslog Command Precedence	14-8
14-4	Syslog Server Default Settings.....	14-10
15-1	Maximum SID Capacities Per Platform	15-6
15-2	Spanning Tree Port Roles	15-13
15-3	Spanning Tree Port States	15-13
15-4	Multiple Spanning Tree Instance Support	15-16
15-5	MSTI Characteristics for Figure 15-10.....	15-19
15-6	Spanning Tree Port Default Settings	15-21
15-7	BPDU Interval Defaults.....	15-22
15-8	Commands for Monitoring MSTP	15-29
15-9	Commands for Monitoring SpanGuard.....	15-31
15-10	Commands for Monitoring Loop Protect.....	15-35
15-11	Spanning Tree Terms and Definitions	15-36
16-1	Admin Rule Parameters	16-5
16-2	Policy Rule Traffic Descriptions/Classifications.....	16-6
16-3	Valid Data Values for Traffic Classification Rules	16-6
16-4	Non-Edge Protocols	16-8
16-5	Displaying Policy Configuration and Statistics.....	16-11

16-6	Policy Configuration Terms and Definitions.....	16-18
17-1	CoS Configuration Terminology	17-3
18-1	RMON Monitoring Group Functions and Commands.....	18-3
18-2	Default RMON Parameters.....	18-5
18-3	Managing RMON.....	18-9
18-4	Displaying RMON Information and Statistics.....	18-9
18-5	sFlow Definitions	18-10
18-6	Default sFlow Parameters	18-13
18-7	Displaying sFlow Information.....	18-15
18-8	Managing sFlow	18-15
19-1	PIM-SM Message Types	19-13
19-2	PIM Terms and Definitions	19-14
19-3	Layer 2 IGMP Configuration Commands.....	19-16
19-4	Layer 3 IGMP Configuration Commands.....	19-16
19-5	Layer 2 IGMP Show Commands	19-18
19-6	Layer 3 IGMP Show Commands	19-18
19-7	DVMRP Configuration Commands.....	19-18
19-8	DVMRP Show Commands	19-21
19-9	PIM-SM Set Commands.....	19-21
19-10	PIM-SM Show Commands	19-24
20-1	Router CLI Configuration Modes	20-2
20-2	UDP Broadcast Forwarding Port Default.....	20-8
20-3	IP Routing Terms and Definitions.....	20-10
21-1	Routing Protocol Route Preferences	21-2
21-2	RIP Default Values	21-3
21-3	IRDP Default Values.....	21-5
22-1	Default OSPF Parameters	22-16
22-2	OSPF Management Tasks.	22-19
23-1	Default VRRP Parameters.....	23-3
23-2	VRRP Configuration Terms and Definitions	23-8
24-1	ACL Rule Precedence	24-11
25-1	Monitoring Network Connections at the Switch Level	25-3
25-2	IPv6 Default Conditions	25-4
25-3	Setting Routing General Parameters.....	25-5
25-4	Displaying Routing Information.....	25-10
25-5	Testing Network Connectivity	25-11
25-6	Displaying DHCPv6 Statistics	25-18
26-1	SNMP Commands Affected by Security Mode Settings.....	26-2
26-2	User Account and Password Parameter Defaults by Security Mode	26-3
26-3	Logging Commands Affected by Security Mode Settings	26-4
26-4	File Management Commands Affected by Security Mode Settings	26-4
26-5	IPsec Defaults	26-5
26-6	MAC Locking Defaults	26-9
26-7	TACACS+ Parameters	26-13
26-8	TACACS+ Show Commands.....	26-15
26-9	DHCP Snooping Default Parameters	26-20
26-10	Displaying DHCP Snooping Information.....	26-21
26-11	Managing DHCP Snooping	26-21
26-12	Dynamic ARP Inspection Default Parameters.....	26-24
26-13	Displaying Dynamic ARP Inspection Information	26-24
26-14	Managing Dynamic ARP Inspection	26-25

About This Guide

This guide provides basic configuration information for the Enterasys Networks Fixed Switch platforms using the Command Line Interface (CLI), including procedures and code examples.

For detailed information about the CLI commands used in this book, refer to the *CLI Reference* for your Fixed Switch platform.

Important Notice

Depending on the firmware version used on your Fixed Switch platform, some features described in this document may not be supported. Refer to the most recent Release Notes for your product to determine which features are supported. Release Notes are available at this link: <https://extranet.enterasys.com/downloads>

How to Use This Guide

Read through this guide completely to familiarize yourself with its contents and to gain an understanding of the features and capabilities of the Enterasys Networks Fixed Switches. A general working knowledge of data communications networks is helpful when setting up these switches.

Related Documents

The *CLI Reference* manuals and *Hardware Installation Guides* for each platform can be obtained from the World Wide Web in Adobe Acrobat Portable Document Format (PDF) at the following site:

<http://extranet.enterasys.com/downloads/>

Conventions Used in This Guide

The following conventions are used in the text of this document:

Convention	Description
Bold font	Indicates mandatory keywords, parameters or keyboard keys.
<i>italic font</i>	Indicates complete document titles.
<code>Courier font</code>	Used for examples of information displayed on the screen.
<i>Courier font in italics</i>	Indicates a user-supplied value, either required or optional.
[]	Square brackets indicate an optional value.
{ }	Braces indicate required values. One or more values may be required.
	A vertical bar indicates a choice in values.
[x y z]	Square brackets with a vertical bar indicates a choice of a value.
{x y z}	Braces with a vertical bar indicate a choice of a required value.
[x {y z}]	A combination of square brackets with braces and vertical bars indicates a required choice of an optional value.

The following icons are used in this guide:



Note: Calls the reader's attention to any item of information that may be of special importance.



Router: Calls the reader's attention to router-specific commands and information.



Caution: Contains information essential to avoid damage to the equipment.

Precaución: Contiene información esencial para prevenir dañar el equipo.

Achtung: Verweist auf wichtige Informationen zum Schutz gegen Beschädigungen.

Getting Help

For additional support related to the product or this document, contact Enterasys Networks using one of the following methods:

World Wide Web	www.enterasys.com/support
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-978-684-1000 To find the Enterasys Networks Support toll-free number in your country: www.enterasys.com/support
Email	support@enterasys.com To expedite your message, type [insert correct indicator here] in the subject line.

Before contacting Enterasys Networks for technical support, have the following data ready:

- Your Enterasys Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of all involved Enterasys Networks products in the network
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load and frame size at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

Setting Up a Switch for the First Time

This chapter describes how to configure an Enterasys stackable or standalone Fixed Switch received from the factory that has not been previously configured. Most of the procedures assume that you are configuring a single switch that has not been connected to a network, and they require that you have physical access to the console port on the switch.

If you are configuring multiple new switches in a stack, review the procedures that apply to a single switch first, then refer to “[Configuring a Stack of New Switches](#)” on page 1-8.

For information about...	Refer to page...
Before You Begin	1-1
Connecting to the Switch	1-2
Downloading New Firmware	1-3
Additional Configuration Tasks	1-5
Saving the Configuration and Connecting Devices	1-7
Configuring a Stack of New Switches	1-8
Where to Go Next	1-9
Getting Help	1-10
Downloading Firmware via the Serial Port	1-10

Before You Begin

The procedures in this chapter assume that:

- You have installed a terminal emulation program on the PC or laptop computer that you will use to configure the switch. Commonly used (and often free) terminal emulation programs available on the Internet include:
 - HyperTerminal
 - Tera Term
 - PuTTY
- You can connect your PC or laptop to the (DB9 male) console port on the switch.

If your PC or laptop has a DB9 communications port, use the DB9 female-to-DB9 female cable that was shipped with the switch to connect your computer to the switch console port.

If your PC or laptop does not have a DB9 communications port but does provide a USB port:

- Obtain a USB to RS 232 DB9 (Male) Serial Interface adapter cable.

If the adapter cable requires a driver, install the driver on your computer. (These drivers are usually provided by the vendor of the adapter cable.)

- Connect the adapter cable's USB connector to a USB port on your PC or laptop and determine which COM port has been assigned to that USB port.

(On Windows 7, this information is displayed in the Device Manager window.)

- Connect the adapter cable's DB9 male connector to the DB9 female-to-DB9 female cable shipped with the switch.
- Connect the free end of the DB9 female-to-DB9 female cable to the switch console port.
- You have access to a TFTP server. Since this procedure assumes that the switch is not connected to a network, the TFTP server application should be locally installed on your PC or laptop. TFTP servers are available on the Internet for purchase or free download.

Review your TFTP server documentation for information about how to configure the server. In particular, you must configure the upload/download directory used by the TFTP server.

- You have downloaded the latest firmware for the switch from the Enterasys web site to your computer, unzipped/uncompressed the firmware, and copied the firmware to the upload/download directory configured for your TFTP server (see previous bullet). The firmware is available at this Enterasys location:

<https://extranet.enterasys.com/downloads>

Review the Release Notes for the downloaded firmware to check for any upgrade notices or limitations that may apply to your switch.



Note: Using TFTP to copy the latest firmware to the switch is recommended because it is faster. However, if you cannot use a TFTP server, you can download the firmware over the console port. That procedure is described in “[Downloading Firmware via the Serial Port](#)” on page 1-10.

Connecting to the Switch

Follow these steps to connect to the switch and set its IP address:

1. Connect your PC or laptop to the console port of the switch, as described above.
2. On your computer, start your terminal emulation program and set the serial session parameters, including the following:
 - Transmit speed or baud rate = 9600
 - Data bits = 8
 - Parity = None
 - Stop bits = 1
 - Mode = 7 bit control, if available
 - Specify the appropriate COM port
3. Open the terminal emulation session, then power up the switch.
4. In the window of the terminal emulation session, you will see switch boot up output.
5. When the boot up output is complete, the system prints a Username prompt.
6. Log in to the system by typing the default username **admin**, then pressing the Enter key at the Password prompt. You will see a Welcome screen similar to the following.

```
Username : admin
Password :
```

Enterasys C5
 Command Line Interface

Enterasys Networks, Inc.
 50 Minuteman Rd.
 Andover, MA 01810-1008 U.S.A.

Phone: +1 978 684 1000
 E-mail: support@enterasys.com
 WWW: http://www.enterasys.com

(c) Copyright Enterasys Networks, Inc. 2011

Chassis Serial Number: 093103209001
Chassis Firmware Revision: 06.61.01.0017

Last successful login : WED DEC 07 20:23:20 2011
 Failed login attempts since last login : 0

C5(su)->

7. Note the firmware version displayed in the Welcome screen — it is most likely earlier than the latest version you downloaded from the Enterasys web site, so you will need to upgrade the firmware on the switch.
8. Set a static system IP address on the switch to be used to download the new firmware. For example:

```
C5(su)->set ip address 192.168.1.1 mask 255.255.255.0
```

Setting a mask and gateway address are optional. If they are not specified, **mask** will be set to the natural mask of the address and **gateway** will stay at the default value of 0.0.0.0.

9. On your computer, set an IP address in the same subnet you gave to the switch. For example: 192.168.1.2.
10. Set up in-band access between your computer and the switch by connecting an Ethernet cable from the network port on your computer to one of the front panel fixed ports on the switch. (Pings and the TFTP transfer will occur via this in-band connection.)
11. From within the switch session, ping the IP address you gave to your computer, to ensure connectivity between the switch and your computer. For example:

```
C5(su)->ping 192.168.1.2
```

Then, from your computer, ping the switch.



Note: If the pings are unsuccessful, there may be fire wall or other configuration issues on your computer. As a first step, try disabling the fire wall on your computer. If that does not resolve the problem, contact your IT group for assistance.

Downloading New Firmware

On stackable and standalone switches, the system Flash can store up to two firmware images at a time. A new switch should have only one firmware image installed, which allows you to download the new firmware image as described below. If you are installing a replacement switch

or just want to verify the contents of the **images** directory, refer to [“Deleting a Backup Image File”](#) on page 1-5 for more information.



Note: If this switch will be added to an existing stack, you should install the primary and backup firmware versions that are currently installed on the stack units.

After you have established your connection to the switch, follow these steps to download the latest firmware:

1. Start the TFTP application.
2. In the terminal emulation session window, use the **copy** command to TFTP transfer the firmware file from the TFTP server location to the **images** directory on the switch. For example:

```
C5(su)->copy tftp://192.168.1.2/c5-series_06.61.01.0031 system:image
```



Note: If you receive the error message “Error: No space left on the device. Please remove backup file.”, refer to [“Deleting a Backup Image File”](#) on page 1-5 before proceeding.

3. Set the new firmware to be active and reboot the system with the **set boot system** command. When the command asks if you want to reset the system now, reply **y**. For example:

```
C5(su)->set boot system c5-series_06.61.01.0031
This command can optionally reset the system to boot the new image.
Do you want to reset now (y/n) [n]y
```

```
Resetting system ...
```

4. After the switch reboots, log in again and use the **dir** command to confirm that the new firmware is the “active” and “boot” firmware. For example:

```
C5(su)->dir
Images:
=====
Filename:      c5-series_06.42.06.0008
Version:      06.42.06.0008
Size:         6862848 (bytes)
Date:         Thu Apr 14 18:46:53 2011
Checksum:     120a983d5fe5d1514553b585557b32cd
Compatibility: C5G124-24, C5G124-24P2, C5G124-48, C5G124-48P2, C5K125-24
               C5K125-24P2, C5K125-48, C5K125-48P2, C5K175-24

Filename:      c5-series_06.61.01.0031 (Active) (Boot)
Version:      06.61.01.0031
Size:         7213056 (bytes)
Date:         Thu Dec 22 18:19:16 2011
Checksum:     7d7e4851337db5088094764c7ba2b05a
Compatibility: C5G124-24, C5G124-24P2, C5G124-48, C5G124-48P2, C5K125-24
               C5K125-24P2, C5K125-48, C5K125-48P2, C5K175-24

Files:                Size
=====
configs:
logs:
```

```
current.log
```

Deleting a Backup Image File

Since the stackable and standalone switches can store only two firmware images at a time, you may have to delete a backup image, if one exists, before you can manually download a new firmware image.

1. Use the **dir** command to display the contents of the images directory. For example:

```
C5(su)->dir
Images:
=====
Filename:      c5-series_06.42.06.0008
Version:       06.42.06.0008
Size:          6862848 (bytes)
Date:          Thu Apr 14 18:46:53 2011
Checksum:      120a983d5fe5d1514553b585557b32cd
Compatibility: C5G124-24, C5G124-24P2, C5G124-48, C5G124-48P2, C5K125-24
               C5K125-24P2, C5K125-48, C5K125-48P2, C5K175-24

Filename:      c5-series_06.42.10.0016 (Active) (Boot)
Version:       06.42.10.0016
Size:          7213056 (bytes)
Date:          Thu Dec 15 18:19:16 2011
Checksum:      7d7e4851337db5088094764c7ba2b05a
Compatibility: C5G124-24, C5G124-24P2, C5G124-48, C5G124-48P2, C5K125-24
               C5K125-24P2, C5K125-48, C5K125-48P2, C5K175-24

Files:          Size
=====
configs:
logs:
current.log
```

2. Use the **delete** command to delete the firmware version that is not chosen as Active. For example:

```
C5(su)->delete c5-series_06.42.06.0008
```

3. If desired, use the **dir** command again to confirm that the backup firmware image has been removed.
4. Continue downloading the latest firmware image, as described in [“Downloading New Firmware”](#) on page 1-3.

Additional Configuration Tasks

After loading the latest firmware and resetting the switch, you may wish to perform the following configuration tasks before connecting the switch to your network or connecting devices to the switch.

If the switch will be added to an existing stack, no further configuration is needed. Refer to [“Adding a New Unit to an Existing Stack”](#) on page 2-3.

Setting User Accounts and Passwords

Enterasys switches are shipped with three default user accounts:

- A super-user access account with a username of **admin** and no password
- A read-write access account with a username of **rw** and no password
- A read-only access account with a username of **ro** and no password

Enterasys recommends that, for security purposes, you set up one or more unique user accounts with passwords and disable the default login accounts.

1. Create a new super-user account. This example uses username "NewAdmin":

```
C5(su)->set system login NewAdmin super-user enable
```

2. Set the password for the new super-user account. By default, passwords must be at least 8 characters in length. The interface does not echo the password characters as you enter them.

```
C5(su)->set password NewAdmin
Please enter new password:
Please re-enter new password:
Password Changed.
```

3. Verify the new super-user account with the **show system login** command.

```
C5(su)->show system login
Username   Access      State   Aging  Simul  Local  Login  Access  Allowed
          Access      State   Aging  Simul  Local  Login  Access  Allowed
          Login Only? Start  End    Days
admin      super-user enabled  0      0      no     ***access always allowed***
ro         read-only  enabled  0      0      no     ***access always allowed***
rw         read-write enabled  0      0      no     ***access always allowed***
NewAdmin  super-user enabled  0      0      no     00:00 24:00 sun mon tue
wed thu fri sat
```

4. Repeat steps 1 and 2 to create additional read-write and read-only user accounts as desired. To create read-write or read-only accounts, use these commands:

```
set system login <user-name> read-write enable
set system login <user-name> read-only enable
```

Use the **set password** command to set passwords for the new accounts.

5. Disable the default login accounts.

```
C5(su)->set system login admin super-user disable
C5(su)->set system login rw read-write disable
C5(su)->set system login ro read-only disable
```

For more information about configuring user accounts and passwords, refer to [Chapter 5, User Account and Password Management](#).

Controlling In-band Access to the Switch

By default, SSH is disabled and Telnet is enabled. You may want to require that SSH be used for in-band access to the switch. In addition, WebView, the Enterasys embedded web-server for switch configuration, is enabled on TCP port 80 by default. You may want to disable this browser access also.

1. Enable SSH and show the current state.

```
C5(su)->set ssh enable
```



```
C5(su)->show ssh
SSH Server status: Enabled
```

2. Disable Telnet inbound while leaving Telnet outbound enabled, and show the current state.

```
C5(su)->set telnet disable inbound
C5(su)->show telnet
Telnet inbound is currently: DISABLED
Telnet outbound is currently: ENABLED
```

3. Disable WebView and show the current state.

```
C5(su)->set webview disable
C5(su)->show webview
WebView is Disabled.
```

4. Set the time (in minutes) an idle console, Telnet, or SSH CLI session will remain connected before timing out. The default idle timeout is 5 minutes.

```
C5(su)->set logout 20
C5(su)->show logout
Logout currently set to: 20 minutes.
```

Changing SNMP Defaults

By default, SNMP Version 1 (SNMPv1) is configured on Enterasys switches. The default configuration includes a single community name “public” which grants read-write access to the whole MIB tree for both SNMPv1 and SNMPv2c.

For security reasons, you should plan to change the default SNMP settings to ones suitable for your network. Refer to [Chapter 12, Configuring SNMP](#) for detailed information.

As a minimum step, Enterasys recommends that you remove the default community name “public” from the switch’s configuration.

1. Remove the “public” community name.

```
C5(su)->clear snmp community public
```

2. Map a new community name to the security name of “public.”

```
C5(su)->set snmp community <new-community-name> securityname public
```

This step allows you to keep the public view group and group access, and therefore ensure SNMP access to the switch, until you are ready to change all the default SNMP settings to more appropriate values.

Saving the Configuration and Connecting Devices

When you enter CLI configuration commands, the configuration is saved to NVRAM on the switch automatically at the following intervals:

- On a standalone unit, the configuration is checked every two minutes and saved if there has been a change.
- On a stack, the configuration is saved across the stack every 5 minutes if there has been a change.

To save a running configuration to NVRAM more often than the automatic intervals, execute the **save config** command and wait for the system prompt to return. After the prompt returns, the configuration will be persistent.

When you have completed your initial configuration:

1. Save the running configuration.

```
C5(su)save config
Saving Configuration to stacking members
Configuration saved
C5(su)->
```

2. Optionally, save the configuration to a backup file named “myconfig” in the **configs** directory and copy the file to your computer using TFTP. You can use this backup configuration file to quickly restore the configuration if you need to replace the switch or change to a different firmware version.

```
C5(su)->show config outfile configs/myconfig
C5(su)->copy configs/myconfig tftp://192.168.1.2/myconfig
```

3. Connect the switch ports to the network or to user devices, following the instructions in the *Installation Guide* for your switch.

Configuring a Stack of New Switches

For more information about configuring a stack of switches, refer to [Chapter 2, Configuring Switches in a Stack](#).

To set up multiple new stackable switches in a stack:

1. Before applying power to the switches, connect the stacking cables, as described in your products' *Installation Guide*.
2. Power on the switches one at a time, starting with the switch you want to be the manager switch.
3. Connect to the console port of the manager unit, as described in “[Before You Begin](#)” on page 1-1, and “[Connecting to the Switch](#)” on page 1-2 and log in to the CLI.
4. Check that the stacking process has completed as you expected it to, using the **show switch** command.
5. If necessary, renumber the stack units, as described in [Chapter 2, Configuring Switches in a Stack](#).
6. Set the IP address of the stack as described in “[Connecting to the Switch](#)” on page 1-2.
7. Connect the network port on your computer to a front panel port on the manager unit with an Ethernet cable (described in [Connecting to the Switch](#)) and use TFTP to download the firmware to the manager unit, as described in “[Downloading New Firmware](#)” on page 1-3.

The manager unit copies the new firmware to the members of the stack automatically as part of the download process.
8. Set the new firmware to be active and reboot the entire system with the **set boot system** command. When the command asks if you want to reset the system now, reply **y**.
9. After the switches in the stack reboot, log back in and confirm that the new firmware has been applied, using the **show switch** command.
10. Apply any advanced feature licenses, if required. Refer to “[Licensing Advanced Features](#)” on page 4-8 for more information.
11. Refer to “[Additional Configuration Tasks](#)” on page 1-5.

Where to Go Next

For information about...	Refer to ...
Configuring switches in a stack	Chapter 2, Configuring Switches in a Stack
User accounts and passwords	Chapter 5, User Account and Password Management
Setting up authentication	Chapter 10, Configuring User Authentication
Configuring system services, including licensing of advanced features, SNTP, DHCP, Telnet, SSH, MAC address settings, and node aliases	Chapter 4, System Configuration
How to use the command line interface	Chapter 3, CLI Basics
Firmware and file management, including how to upgrade the firmware, how to create and save configuration backup files, and how to revert to a saved configuration	Chapter 6, Firmware Image and File Management
Configuring system power and PoE	Chapter 7, Configuring System Power and PoE
Port configuration	Chapter 8, Port Configuration
Configuring VLANs	Chapter 9, Configuring VLANs
Configuring link aggregation	Chapter 11, Configuring Link Aggregation
Configuring SNMP	Chapter 12, Configuring SNMP
Configuring neighbor discovery protocols	Chapter 13, Configuring Neighbor Discovery
Configuring system logging	Chapter 14, Configuring Syslog
Configuring spanning tree	Chapter 15, Configuring Spanning Tree
Configuring policy using the CLI	Chapter 16, Configuring Policy
Configuring multicast protocols, including IGMP, DVMRP, and PIM-SM	Chapter 19, Configuring Multicast
Enabling router configuration modes, configuring IPv4 addresses and static routes	Chapter 20, IP Configuration
Configuring RIP and IRDP	Chapter 21, IPv4 Basic Routing Protocols
Configuring OSPFv2 and VRRP	Chapter 22, Configuring OSPFv2 Chapter 23, Configuring VRRP
Configuring access control lists (ACLs)	Chapter 24, Configuring Access Control Lists
Managing IPv6 at the switch level, configuring IPv6 routing and Neighbor Discovery, and configuring DHCPv6	Chapter 25, Configuring and Managing IPv6
Configuring security features, including the security mode of the switch, IPsec, RADIUS management authentication, MAC locking, TACAC+, and service ACLs	Chapter 26, Configuring Security Features

Getting Help

For additional support, contact Enterasys Networks using one of the following methods:

World Wide Web	www.enterasys.com/support
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-978-684-1000 To find the Enterasys Networks Support toll-free number in your country: www.enterasys.com/support
Email	support@enterasys.com To expedite your message, type [switching] in the subject line.

Enterasys provides an extensive online Knowledge base that can be accessed from the corporate Support page:

<http://www.enterasys.com/support/>

Downloading Firmware via the Serial Port

This procedure describes how to download switch firmware via the serial (console) port, instead of using TFTP. This procedure assumes that you are using either HyperTerminal or TeraTerm (which support XMODEM transfer) as your terminal emulation software and that you have downloaded the latest firmware for the switch from the Enterasys web site to your computer, and unzipped/uncompressed the firmware.

1. Connect your PC or laptop to the console port of the switch, as described above in “[Before You Begin](#)” on page 1-1.
2. On your computer, start your terminal emulation program and set the serial session parameters, including the following:
 - Transmit speed or baud rate = 9600
 - Data bits = 8
 - Parity = None
 - Stop bits = 1
 - Mode = 7 bit control, if available
 - Serial line to connect to = COM1 typically
3. Open the terminal emulation session, then power up the switch.
4. In the window of the terminal emulation session, you will see switch boot up output. A message similar to the following displays.

Within 2 seconds, type **2** to select “Start Boot Menu”. Use “administrator” for the Password.

```
Version 06.61.xx 12-09-2011
```

```
Computing MD5 Checksum of operational code...
Select an option. If no selection in 2 seconds then
operational code will start.
```

```
1 - Start operational code.
2 - Start Boot Menu.
Select (1, 2):2
```

```
Password: *****
```

```
Boot Menu Version 06.61.xx 12-09-2011
```

```
Options available
```

- 1 - Start operational code
 - 2 - Change baud rate
 - 3 - Retrieve event log using XMODEM (64KB).
 - 4 - Load new operational code using XMODEM
 - 5 - Display operational code vital product data
 - 6 - Run Flash Diagnostics
 - 7 - Update Boot Code
 - 8 - Delete operational code
 - 9 - Reset the system
 - 10 - Restore Configuration to factory defaults (delete config files)
 - 11 - Set new Boot Code password
- ```
[Boot Menu] 2
```

5. Type **2**. The following baud rate selection screen displays:

- 1 - 1200
- 2 - 2400
- 3 - 4800
- 4 - 9600
- 5 - 19200
- 6 - 38400
- 7 - 57600
- 8 - 115200
- 0 - no change

6. Type **8** to set the switch baud rate to 115200. The following message displays:

```
Setting baud rate to 115200, you must change your terminal baud rate.
```

7. In your terminal emulation program, set the terminal baud rate to **115200**:

- HyperTerminal: File > Properties > Configure > Bits per Second > Apply > OK > OK
- TeraTerm: Setup > Serial port > Baud rate > OK

8. Press ENTER. The switch will complete the baud rate change, displaying a new boot menu prompt.

9. From the boot menu options screen, type **4** to load new operational code using XMODEM.

10. Set up for XMODEM file transmission:

- HyperTerminal: Transfer > Send File > Browse > Open > Protocol Xmodem > Send > bps/cps
- TeraTerm: File > Transfer > XMODEM > Send > Browse > Open

11. Progress messages will indicate the status of the file transfer.

```
[Boot Menu] 4
Ready to receive the file with XMODEM/CRC....
Ready to RECEIVE File xcode.bin in binary mode
Send several Control-X characters to cCKCKCKCKCKCKCK
```

```
XMODEM transfer complete, checking CRC....
Verified operational code CRC.
```

```
The following Enterasys Header is in the image:
```

```
MD5 Checksum.....fe967970996c4c8c43a10cd1cd7be99a
Boot File Identifier.....0x0517
```

```

Header Version.....0x0100
Image Type.....0x82
Image Offset.....0x004d
Image length.....0x006053b3
Ident Strings Length.....0x0028
Ident Strings.....
<platform specific>

Image Version Length.....0x8
Image Version Bytes.....0x30 0x2e 0x35 0x2e 0x30 0x2e 0x34 (x.xx.xx)

The following secondary header is in the image:
CRC.....0xe6aa (59050)
Target Device.....0x00a08245
Size.....0x58f210 (5829136)
Number of Components.....2
Operational Code Size.....0x51d5b8 (5363128)
Operational Code Offset.....0x0 (0)
Operational Code CRC.....0x1FC1
Boot Code Version.....29
Boot Code Size.....0x71a08 (465416)
Boot Code Offset.....0x51d5b8 (5363128)
Boot Code CRC.....0x4CCD

VPD - rel 6 ver 61 maint_lvl xx
 Timestamp - Wed Jul 27 12:24:04 2011
 File - c5-series_06.61.xx

Operational code update completed successfully.
Verifying Operational Code CRC..... CRC is OK.

```

12. Press ENTER so the switch will complete the file transfer operation, displaying a fresh prompt.

```
[Boot Menu] 2
```

13. Type **2** to display the baud rate selection screen again.

14. Type **4** to set the switch baud rate to **9600**. The following message displays:

```
Setting baud rate to 9600, you must change your terminal baud rate.
```

15. In your terminal emulation program, set the terminal baud rate to **9600**.

- HyperTerminal: File > Properties > Configure > Bits per Second > Apply > OK > OK
- TeraTerm: Setup > Serial port > Baud rate > OK

16. Press ENTER so the switch will complete the baud rate change and display a fresh prompt.

```
[Boot Menu] 1
```

17. Type **1** to start the new operational code. A message similar to the following displays:

```
Operational Code Date: Tue Jun 29 08:34:05 2011
Uncompressing.....
```

18. After the switch comes back up, log in and confirm that the new image has been detected and is now running. You can use either the "show boot system" command or the "dir" command.

```
C5(rw)->show boot system
Current system image to boot: c5-series_06.61.xx
C5(rw)->
```

## Configuring Switches in a Stack

This chapter provides information about configuring Enterasys switches in a stack. For information about upgrading firmware on a new stack, refer to “[Configuring a Stack of New Switches](#)” on page 1-8.

| For information about...                                               | Refer to page... |
|------------------------------------------------------------------------|------------------|
| <a href="#">About Switch Operation in a Stack</a>                      | 2-1              |
| <a href="#">Installing a New Stackable System of Up to Eight Units</a> | 2-2              |
| <a href="#">Installing Previously-Configured Systems in a Stack</a>    | 2-3              |
| <a href="#">Adding a New Unit to an Existing Stack</a>                 | 2-3              |
| <a href="#">Removing Units from an Existing Stack</a>                  | 2-4              |
| <a href="#">Creating a Virtual Switch Configuration</a>                | 2-4              |
| <a href="#">Considerations About Using “clear config” in a Stack</a>   | 2-5              |
| <a href="#">Configuring Standalone A4 Stack Ports</a>                  | 2-6              |

### About Switch Operation in a Stack

Enterasys stackable switches can be adapted and scaled to help meet your network needs. These switches provide a management platform and uplink to a network backbone for a stacked group of up to eight switches.

Once installed in a stack, the switches behave and perform as a single switch product. As such, you can start with a single unit and add more units as your network expands. You can also mix different products in the family in a single stack to provide a desired combination of port types and functions to match the requirements of individual applications. In all cases, a stack of units performs as one large product, and is managed as a single network entity.

### Stack Initialization

When switches are installed and connected as described in your products’ *Installation Guide*, the following occurs during initialization:

- The switch that will manage the stack is automatically established. This is known as the *manager* switch. The manager switch organizes all the reachability information for bridging and routing, including keeping the address tables in the stack units (including itself) coherent.
- All other switches are established as *members* in the stack. Each individual stack member processes its own packets, rather than pushing them to the manager for processing.

- The hierarchy of the switches that will assume the function of backup manager is also determined in case the current manager malfunctions, is powered down, or is disconnected from the stack.
- The console port on the manager switch remains active for out-of-band (local) switch management, but the console port on each member switch is deactivated. This enables you to set the IP address and system password using a single console port. Each switch can be configured locally using only the manager's console port, or inband using the stack's IP address from a remote device.

Once a stack is created (more than one switch is interconnected), the following procedure occurs:

1. By default, unit IDs are arbitrarily assigned on a first-come, first-served basis.
2. Unit IDs are saved against each module. Then, every time a board is power-cycled, it will initialize with the same unit ID. This is important for port-specific information (for example: ge.4.12 is the 12th Gigabit Ethernet port on Unit # 4).
3. The management election process uses the following precedence to assign a management switch:
  - a. Previously assigned / elected management unit
  - b. Management assigned priority (values 1-15)
  - c. Hardware preference level
  - d. Highest MAC Address

The management designation is written to the manager unit. Thereafter, every time the manager is power-cycled, it will initialize with that role.

## Configuration Management

When switches are stacked, the only file structure and configuration information that is viewable or configurable is that of the manager unit, which pushes its configuration to the member units every 5 minutes if there has been a change. To avoid possible configuration loss in the event of manager unit failure after a configuration change, execute the **save config** command and wait for the system prompt to return. After the prompt returns, the configuration will be persistent.

## Installing a New Stackable System of Up to Eight Units

Use the following procedure for installing a new stack of up to eight units out of the box.



**Note:** The following procedure assumes that all units have a clean configuration from manufacturing, all units are running the same primary and backup firmware image versions, and all units are in the same licensing state.

1. Before applying power, make **all** physical connections with the stack cables as described in your product's *Installation Guide*.
2. Once all of the stack cables have been connected, individually power on each unit, starting with the switch you want to be the manager switch.

Ensure that each switch is fully operational before applying power to the next switch. Since unit IDs are assigned on a first-come, first-served basis, this will ensure that unit IDs are ordered sequentially.

3. Establish a CLI session on the manager unit and use the **show switch** command to display stacking information.



4. (Optional) If desired, change the management unit using the **set switch movemanagement** command, and/or change the unit numbering with the **set switch member** command.
5. Once the desired master unit has been selected, reset the system using the **reset** command.
6. After the stack has been configured, you can use the **show switch unit** command to physically identify each unit. When you enter the command with a unit number, the MGR LED of the specified switch will blink for 10 seconds. The normal state of this LED is off for member units and steady green for the manager unit.

## Installing Previously-Configured Systems in a Stack

If member units in a stack have been previous members of a different stack, you may need to configure the renumbering of the stack. All units must be running the same primary and backup firmware images.

1. Power down the switches in the existing stack.
2. Stack the units in the method desired, and connect the stack cables.
3. Power up only the unit you wish to be manager.
4. Once the management unit is powered up, log into the CLI, and use the **show switch** command to display stacking information.
5. Clear any switches which are listed as “unassigned” using the **clear switch member** command.
6. Power up the member of the stack you wish to become unit 2. Once the second unit is fully powered, the COM session of the CLI will state that a new CPU was added.
7. Use the **show switch** command to redisplay stacking information.
  - a. If the new member displays as unit 2, you can proceed to repeat this step with the next unit.
  - b. If the new member displays a different unit number, you must:
    - (1) Renumber the stack using the **set switch renumber** command, then
    - (2) Clear the original unit number using the **clear switch member** command.

Avoid directly reassigning a different unit number to the stack manager, or by design, the stack configuration will revert to defaults.

8. Repeat [Step 7](#) until all members have been renumbered in the order you desire.
9. After the stack has been reconfigured, you can use the **show switch unit** command to physically confirm the identity of each unit. When you enter the command with a unit number, the MGR LED of the specified switch will blink for 10 seconds. The normal state of this LED is off for member units and steady green for the manager unit.

## Adding a New Unit to an Existing Stack

Use the following procedure for installing a new unit into an existing stack configuration. This procedure assumes that the new unit being added has a clean configuration from manufacturing and is running the same primary and backup firmware image versions as other units in the stack.

1. Ensure that power is off on the new unit being installed.
2. Use one of the following methods to complete stack cable connections:

- If the running stack uses a daisy chain topology, make the stack cable connections from the bottom of the stack to the new unit (that is, STACK DOWN port from the bottom unit of the running stack to the STACK UP port on the new unit).
  - If the running stack uses a ring stack topology, break the ring and make the stack cable connections to the new unit to close the ring.
3. Apply power to the new unit.
  4. Log into the CLI through the management unit and use the **show switch** command to display stacking information.
  5. If the stacking setup does not appear to be correct, use the commands described in the previous procedure to readjust the configuration.

Insertion of new units into a stack is handled dynamically. Normally, the integration is a fairly rapid process. However, be aware that integration is a background task. If the stack is extremely busy handling user traffic, integrating the new unit into the stack could take a long time (possibly hours).

## Removing Units from an Existing Stack

Use the following procedure to remove one or more units from an existing stack.



**Note:** Stacking cables are hot-swappable. In most cases, it is not necessary to power down stacked units before attaching or detaching cables.

1. Use the **save config** command to ensure that all units have full configuration knowledge.
2. Remove the stacking cables associated with the switches you want to remove.
  - a. Operation of the sub-stack that retains the previous manager unit will be disrupted for 2 to 3 seconds.
  - b. Operation of any sub-stacks that now lack a manager unit will be disrupted for 30 to 40 seconds while a new manager unit is elected and comes online.
  - c. In all cases, units will retain their unit numbers.
3. You can power down one or more units either before or after removing stacking cables. Disruption times will be as described in [Stack Disruption Times](#) below.
4. After removal of stack units, you can optionally use the **clear switch member** command to remove any “Unassigned” units.

### Stack Disruption Times

Upon manager unit failure, removal, or reassignment (with the **set switch movemanagement** command), the operation of the stack, including the Ethernet link state of all ports, will be interrupted for about 30 to 40 seconds.

Upon member unit failure or removal, the operation of the stack will be interrupted for about 2 to 3 seconds.

## Creating a Virtual Switch Configuration

You can create a configuration for a stackable switch before adding the actual physical device to a stack. This preconfiguration feature includes configuring protocols on the ports of the “virtual switch.”

To create a virtual switch configuration in a stack environment:

1. Display the types of switches supported in the stack, using the **show switch switchtype** command.
2. Using the output of the **show switch switchtype** command, determine the switch index (SID) of the model of switch being configured.
3. Add the virtual switch to the stack using the **set switch member** command. Use the SID of the switch model, determined in the previous step, and the unit ID that you want to assign to this switch member.
4. Proceed to configure the ports of the virtual switch as you would do for physically present devices.



**Note:** If you preconfigure a virtual switch and then add a physical switch of a different type to the stack as that unit number, any configured functionality that cannot be supported on the physical switch will cause a configuration mismatch status for that device and the ports of the new device will join detached. You must clear the mismatch before the new device will properly join the stack.

## Example

The following example adds a virtual switch configuration to a stack of C5 switches. The switch type being added is a C5G124-24 (SID 1), and it is being added as member unit 4. Port number 1 of the virtual switch (ge.4.1) is then configured in the same way that a physically present port would be configured.

```
C5(su)->show switch switchtype
```

| SID | Switch Model ID | Mgmt Pref | Code Version |
|-----|-----------------|-----------|--------------|
| 1   | C5G124-24       | 1         | 0xa08245     |
| 2   | C5K125-24       | 1         | 0xa08245     |
| 3   | C5K175-24       | 1         | 0xa08245     |
| 4   | C5K125-24P2     | 1         | 0xa08245     |
| 5   | C5G124-24P2     | 1         | 0xa08245     |
| 6   | C5G124-48       | 1         | 0xa08245     |
| 7   | C5K125-48       | 1         | 0xa08245     |
| 8   | C5K125-48P2     | 1         | 0xa08245     |
| 9   | C5G124-48P2     | 1         | 0xa08245     |

```
C5(su)->set switch member 4 1
C5(su)->set vlan create 555
C5(su)->set port vlan ge.4.1 555 modify-egress
C5(su)->show port vlan ge.4.1
ge.4.1 is set to 555
```

## Considerations About Using “clear config” in a Stack

When using the **clear config** command to clear configuration parameters in a stack, it is important to remember the following:

- Use **clear config** to clear configuration parameters without clearing stack unit IDs. This command WILL NOT clear stack parameters or the IP address and avoids the process of renumbering the stack.
- Use **clear config all** when it is necessary to clear all configuration parameters, including stack unit IDs and switch priority values. This command will not clear the IP address nor will it remove an applied advanced feature license.

- Use **clear ip address** to remove the IP address of the stack.
- Use **clear license** to remove an applied license from a switch.

Configuration parameters and stacking information can also be cleared **on the master unit only** by selecting the “restore configuration to factory defaults” option from the boot menu on switch startup. This selection will leave stacking priorities on all other units.

## Configuring Standalone A4 Stack Ports

It is possible on a standalone A4 switch to configure the two stack ports as standard gigabit Ethernet ports with the **set switch stack-port** command. By default, the two front panel uplink ports are in stack mode. Changing the mode causes the switch to reset.

This command should be used only on standalone (non-stacked) A4 switches. Do not stack A4 switches with uplink ports that are in Ethernet mode.

To change front panel uplink ports to Ethernet mode:

```
A4(su)->set switch stack-port ethernet
This command will reset the entire system.
Do you want to continue (y/n) [n]
```

### When Uplink Ports are Configured as Ethernet Ports

When using the **clear config** command to clear configuration parameters on a standalone A4 switch with the uplink ports configured as standard Ethernet ports, it is important to remember the following:

- The **clear config** command WILL NOT set the front panel uplink ports back to stack ports.
- The **clear config all** command WILL set the front panel uplink ports back to stack ports.

This chapter provides information about CLI conventions for stackable and standalone switches and CLI properties that you can configure.

| For information about...                         | Refer to page... |
|--------------------------------------------------|------------------|
| <a href="#">Switch Management Methods</a>        | 3-1              |
| <a href="#">Using the Command Line Interface</a> | 3-1              |
| <a href="#">Configuring CLI Properties</a>       | 3-6              |

## Switch Management Methods

The Enterasys fixed switches can be managed using the following methods:

- Locally using a VT type terminal or computer running a terminal emulation program connected to the switch's console port. See [Chapter 1, Setting Up a Switch for the First Time](#) for information about setting up this type of connection.
- Remotely using a VT type terminal or computer running a terminal emulation program connected through a modem. Refer to the *Installation Guide* for your product for information about setting up this type of connection.
- Remotely using an SNMP management station.
- In-band through a Telnet or SSH connection.
- In-band using the Enterasys NetSight® management application.
- Remotely using WebView™, Enterasys Networks' embedded web server application.

When you connect to the console port or connect through a Telnet connection, you use the Command Line Interface (CLI) to manage the switch.

## Using the Command Line Interface

This section describes how to start a CLI session, how to log in, and how to navigate the CLI.

### Starting a CLI Session

There are two ways to start a CLI session — an out-of-band connection through the console port or an in-band connection using Telnet or SSH.

## Connecting Using the Console Port

Connect a terminal to the local console port as described in “[Connecting to the Switch](#)” on page 1-2. When the boot up output is complete, the system prints a Username prompt. You can now log in to the Command Line Interface (CLI) by

- using a default user account, as described in “[Using a Default User Account](#)” on page 3-3, or
- using an administratively-assigned user account as described in “[Using an Administratively Configured User Account](#)” on page 3-3.

## Connecting Using Telnet or SSH

Once the switch has a valid IP address, you can establish a Telnet or SSH session from any TCP/IP based node on the network. For information about setting the switch’s IP address, refer to the **set ip address** command in the CLI Reference for your product.



**Note:** By default on the fixed switches, Telnet is enabled and SSH is disabled. Refer to “[Controlling In-band Access to the Switch](#)” on page 1-6 for information about enabling SSH.

To establish a Telnet or SSH session:

1. Telnet or SSH to the switch’s IP address.
2. Enter login (user name) and password information in one of the following ways:
  - If the switch’s default login and password settings have not been changed, follow the steps listed in “[Using a Default User Account](#)” on page 3-3, or
  - Enter an administratively-configured user name and password.
3. The startup screen, [Figure 3-1](#), will display on the terminal. The notice of authorization and the prompt displays as shown in [Figure 3-1](#).

**Figure 3-1 CLI Startup Screen**

```
Username:admin
Password:

Enterasys C5
Command Line Interface

Enterasys Networks, Inc.
50 Minuteman Rd.
Andover, MA 01810-1008 U.S.A.

Phone: +1 978 684 1000
E-mail: support@enterasys.com
WWW: http://www.enterasys.com

(c) Copyright Enterasys Networks, Inc. 2012

Chassis Serial Number: 041800249041
Chassis Firmware Revision: x.xx.xx

C5(su)->
```

## Logging In

By default, the switch is configured with three user login accounts—**ro** for Read-Only access, **rw** for Read-Write access, and **admin** for super-user access to all modifiable parameters. The default password is set to a blank string. For information on changing these default settings, refer to [Chapter 5, User Account and Password Management](#).

### Using a Default User Account

If this is the first time you are logging in to the switch, or if the default user accounts have not been administratively changed, proceed as follows:

1. At the login prompt, enter one of the following default user names:
  - **ro** for Read-Only access.
  - **rw** for Read-Write access.
  - **admin** for Super User access.
2. Press ENTER. The Password prompt displays.
3. Leave this string blank and press ENTER. The switch information and prompt displays as shown in [Figure 3-1](#).

### Using an Administratively Configured User Account

If the switch's default user account settings have been changed, proceed as follows:

1. At the login prompt, enter your administratively-assigned user name and press ENTER.
2. At the Password prompt, enter your password and press ENTER.

The notice of authorization and the prompt displays as shown in [Figure 3-1](#) on page 3-2.



**Note:** Users with read-write and read-only access can use the [set password](#) command (page 4-9) to change their own account passwords. Administrators with Super User (su) access can use the [set system login](#) command (page 4-6) to create and change user accounts, and the [set password](#) command to change any local account password.

## Clearing and Closing the CLI

Use the **cls** command to clear the session screen.

Use the **exit** command to leave a CLI session. This command is also used to move to a lower router mode.

## Navigating the Command Line Interface

### Getting Help with CLI Syntax

The switch allows you to display usage and syntax information for individual commands by typing **help** or **?** after the command.

### CLI Command Defaults Descriptions

Each command description in the CLI Reference Guide for your product includes a section entitled “Defaults” which contains different information from the factory default settings on the switch described in [Chapter 4, System Configuration](#). The section defines CLI behavior if the user enters a command without typing optional parameters (indicated by square brackets [ ]). For

commands without optional parameters, the defaults section lists “None”. For commands with optional parameters, this section describes how the CLI responds if the user opts to enter only the keywords of the command syntax. [Figure 3-2](#) provides an example.

**Figure 3-2 Sample CLI Defaults Description**

### Syntax

```
show port status [port-string]
```

### Defaults

If *port-string* is not specified, status information for all ports will be displayed.

## CLI Command Modes

Each command description in this guide includes a section entitled “Mode” which states whether the command is executable in Admin (Super User), Read-Write, or Read-Only mode. Users with Read-Only access will only be permitted to view Read-Only (**show**) commands. Users with Read-Write access will be able to modify all modifiable parameters in **set** and **show** commands, as well as view Read-Only commands. Administrators or Super Users will be allowed all Read-Write and Read-Only privileges, and will be able to modify local user accounts. The A4 switch indicates which mode a user is logged in as by displaying one of the following prompts:

- Admin: A4(su)->
- Read-Write: A4(rw)->
- Read-Only: A4(ro)->

## Performing Keyword Lookups

Entering a space and a question mark (?) after a keyword will display all commands beginning with the keyword. [Figure 3-3](#) shows how to perform a keyword lookup for the **show snmp** command. In this case, four additional keywords are used by the **show snmp** command. Entering a space and a question mark (?) after any of these parameters (such as **show snmp community**) will display additional parameters nested within the syntax.

**Figure 3-3 Performing a Keyword Lookup**

```
A4(su)->show snmp ?
community SNMP v1/v2c community name configuration
notify SNMP notify configuration
targetaddr SNMP target address configuration
targetparams SNMP target parameters configuration
```

Entering a question mark (?) without a space after a partial keyword will display a list of commands that begin with the partial keyword. [Figure 3-4](#) shows how to use this function for all commands beginning with **co**:

**Figure 3-4 Performing a Partial Keyword Lookup**

```
A4(rw)->co?
configure copy
A4(su)->co
```





**Note:** At the end of the lookup display, the system will repeat the command you entered without the ?.

## Displaying Scrolling Screens

If the CLI screen length has been set using the **set length** command, CLI output requiring more than one screen will display `--More--` to indicate continuing screens. To display additional screen output:

- Press any key other than ENTER to advance the output one screen at a time.
- Press ENTER to advance the output one line at a time.

The example in [Figure 3-5](#) shows how the **show mac** command indicates that output continues on more than one screen.

**Figure 3-5 Scrolling Screen Output**

```
A4(su)->show mac

MAC Address FID Port Type

00-00-1d-67-68-69 1 host Management
00-00-02-00-00-00 1 fe.1.2 Learned
00-00-02-00-00-01 1 fe.1.3 Learned
00-00-02-00-00-02 1 fe.1.4 Learned
00-00-02-00-00-03 1 fe.1.5 Learned
00-00-02-00-00-04 1 fe.1.6 Learned
00-00-02-00-00-05 1 fe.1.7 Learned
00-00-02-00-00-06 1 fe.1.8 Learned
00-00-02-00-00-07 1 fe.1.9 Learned
00-00-02-00-00-08 1 fe.1.10 Learned
--More--
```

## Abbreviating and Completing Commands

The switch allows you to abbreviate CLI commands and keywords down to the number of characters that will allow for a unique abbreviation. [Figure 3-6](#) shows how to abbreviate the **show netstat** command to **sh net**.

**Figure 3-6 Abbreviating a Command**

```
A4(su)->sh net
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address Foreign Address State

TCP 0 0 10.21.73.13.23 134.141.190.94.51246 ESTABLISHED
TCP 0 275 10.21.73.13.23 134.141.192.119.4724 ESTABLISHED
TCP 0 0 *.80 *.* LISTEN
TCP 0 0 *.23 *.* LISTEN
UDP 0 0 10.21.73.13.1030 134.141.89.113.514 *
UDP 0 0 *.161 *.* *
UDP 0 0 *.1025 *.* *
UDP 0 0 *.123 *.* *
```

## Basic Line Editing Commands

The CLI supports EMACs-like line editing commands. [Table 3-1](#) lists some commonly used commands.

**Table 3-1 Basic Line Editing Commands**

| Key Sequence     | Command                                                                                         |
|------------------|-------------------------------------------------------------------------------------------------|
| Ctrl+A           | Move cursor to beginning of line.                                                               |
| Ctrl+B           | Move cursor back one character.                                                                 |
| Ctrl+D           | Delete a character.                                                                             |
| Ctrl+E           | Move cursor to end of line.                                                                     |
| Ctrl+F           | Move cursor forward one character.                                                              |
| Ctrl+H           | Delete character to left of cursor.                                                             |
| Ctrl+I or TAB    | Complete word.                                                                                  |
| Ctrl+K           | Delete all characters after cursor.                                                             |
| Ctrl+N           | Scroll to next command in command history (use the CLI history command to display the history). |
| Ctrl+P           | Scroll to previous command in command history.                                                  |
| Ctrl+Q           | Resume the CLI process.                                                                         |
| Ctrl+S           | Pause the CLI process (for scrolling).                                                          |
| Ctrl+T           | Transpose characters.                                                                           |
| Ctrl+U or Ctrl+X | Delete all characters before cursor.                                                            |
| Ctrl+W           | Delete word to the left of cursor.                                                              |
| Ctrl+Y           | Restore the most recently deleted item.                                                         |

## Configuring CLI Properties

CLI properties are options that you can configure and customize in the CLI, such as the command prompt, command completion, banner messages, and session idle timeout.

[Table 3-2](#) lists CLI properties configuration commands.

**Table 3-2 CLI Properties Configuration Commands**

| Task                                                                                       | Command                                                                        |
|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Modify the command prompt                                                                  | <b>set prompt</b> <i>prompt-string</i>                                         |
| Set the banner message for pre- and post-session login.                                    | <b>set banner</b> { <b>login</b> <i>message</i>   <b>motd</b> <i>message</i> } |
| Clear the banner message displayed at pre- and post-session login to a blank string.       | <b>clear banner</b> { <b>login</b>   <b>motd</b> }                             |
| Set the number of columns for the terminal connected to the device's console port.         | <b>set width</b> <i>screenwidth</i> [ <i>default</i> ]                         |
| Set the number of lines the CLI will display before pausing with a "----More ----" prompt. | <b>set length</b> <i>screenlength</i>                                          |

**Table 3-2 CLI Properties Configuration Commands (continued)**

| Task                                                                                                     | Command                          |
|----------------------------------------------------------------------------------------------------------|----------------------------------|
| Set the time (in minutes) an idle console or Telnet CLI session will remain connected before timing out. | <b>set logout <i>timeout</i></b> |

Refer to the *CLI Reference* for your switch model for more information about each command.

## Example CLI Properties Configuration

In this example, the prompt is changed and a login banner is added.

```
C5(rw)->set prompt "Switch 1"
Switch 1(rw)->
Switch 1(rw)->set banner login "There is nothing more important than our
customers."
```

## CLI Properties Display Commands

[Table 3-3](#) lists CLI properties show commands.

**Table 3-3 CLI Properties Show Commands**

| Task                                                                                                         | Command            |
|--------------------------------------------------------------------------------------------------------------|--------------------|
| Display the banner message that will display at pre and post session login.                                  | <b>show banner</b> |
| Display the number of columns for the terminal connected to the device's console port.                       | <b>show width</b>  |
| Display the current screen length.                                                                           | <b>show length</b> |
| Display the time (in seconds) an idle console or Telnet CLI session will remain connected before timing out. | <b>show logout</b> |

Refer to the *CLI Reference* for your switch model for a description of the output of each command.



## System Configuration

This chapter provides basic system configuration information in the following areas:

| For information about...                        | Refer to page... |
|-------------------------------------------------|------------------|
| <a href="#">Factory Default Settings</a>        | 4-1              |
| <a href="#">Initial Configuration Overview</a>  | 4-5              |
| <a href="#">Advanced Configuration Overview</a> | 4-6              |
| <a href="#">Licensing Advanced Features</a>     | 4-8              |
| <a href="#">SNTP Configuration</a>              | 4-11             |
| <a href="#">DHCP Configuration</a>              | 4-16             |
| <a href="#">Telnet Overview</a>                 | 4-23             |
| <a href="#">SSH Overview</a>                    | 4-24             |
| <a href="#">MAC Address Settings</a>            | 4-24             |
| <a href="#">Configuring Node Aliases</a>        | 4-26             |

### Factory Default Settings

The following tables list factory default settings available on the Enterasys fixed switches.

**Table 4-1 Default Settings for Basic Switch Operation**

| Feature                     | Default Setting                                       |
|-----------------------------|-------------------------------------------------------|
| <b>Switch Mode Defaults</b> |                                                       |
| CDP discovery protocol      | Auto enabled on all ports.                            |
| CDP authentication code     | Set to 00-00-00-00-00-00-00-00                        |
| CDP hold time               | Set to 180 seconds.                                   |
| CDP interval                | Transmit frequency of CDP messages set to 60 seconds. |
| Cisco discovery protocol    | Auto enabled on all ports.                            |
| Cisco DP hold time          | Set to 180 seconds.                                   |
| Cisco DP interval timer     | Set to 60 seconds.                                    |
| Community name              | Public.                                               |

**Table 4-1 Default Settings for Basic Switch Operation (continued)**

| Feature                                  | Default Setting                                                                                                                                     |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Console (serial) port required settings  | Baud rate: 9600<br>Data bits: 8<br>Flow control: disabled<br>Stop bits: 1<br>Parity: none                                                           |
| DHCP server                              | Disabled.                                                                                                                                           |
| Diffserv                                 | Disabled. (B3 platforms only)                                                                                                                       |
| EAPOL                                    | Disabled.                                                                                                                                           |
| EAPOL authentication mode                | When enabled, set to auto for all ports.                                                                                                            |
| GARP timer                               | Join timer set to 20 centiseconds; leave timer set to 60 centiseconds; leaveall timer set to 1000 centiseconds.                                     |
| GVRP                                     | Globally enabled. Disabled per port.                                                                                                                |
| History buffer size                      | 20 lines.                                                                                                                                           |
| IEEE 802.1 authentication                | Disabled.                                                                                                                                           |
| IGMP snooping                            | Disabled. When enabled, query interval is set to 260 seconds and response time is set to 10 seconds.                                                |
| IP mask and gateway                      | Subnet mask set to 0.0.0.0; default gateway set to 0.0.0.0.                                                                                         |
| IP routes                                | No static routes configured.                                                                                                                        |
| Jumbo frame support                      | Enabled on all ports. (Not supported on I-Series switches.)                                                                                         |
| Link aggregation control protocol (LACP) | Globally enabled.<br>Disabled per port on B5 and C5 switches.<br>Enabled per port on A4, B3, C3, G-Series, and I-Series switches.                   |
| Link aggregation admin key               | Set to 32768 for all ports.                                                                                                                         |
| Link aggregation flow regeneration       | Disabled.                                                                                                                                           |
| Link aggregation system priority         | Set to 32768 for all ports.                                                                                                                         |
| Link aggregation output algorithm        | Set to DIP-SIP.                                                                                                                                     |
| Lockout                                  | Set to disable Read-Write and Read-Only users, and to lockout the default admin (Super User) account for 15 minutes, after 3 failed login attempts. |
| Logging                                  | Syslog port set to UDP port number 514. Logging severity level set to 6 (significant conditions) for all applications.                              |
| MAC aging time                           | Set to 300 seconds.                                                                                                                                 |
| MAC locking                              | Disabled (globally and on all ports).                                                                                                               |
| Passwords                                | Set to an empty string for all default user accounts. User must press ENTER at the password prompt to access CLI.                                   |
| Password aging                           | Disabled.                                                                                                                                           |

**Table 4-1 Default Settings for Basic Switch Operation (continued)**

| Feature                                       | Default Setting                                                                                                                                                                                                                           |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Password history                              | No passwords are checked for duplication.                                                                                                                                                                                                 |
| Policy classification                         | Classification rules are automatically enabled when created.                                                                                                                                                                              |
| Port auto-negotiation                         | Enabled on all ports.                                                                                                                                                                                                                     |
| Port advertised ability                       | Maximum ability advertised on all ports.                                                                                                                                                                                                  |
| Port broadcast suppression                    | Enabled and set to limit broadcast packets to 14,881 per second on all switch ports.                                                                                                                                                      |
| Port duplex mode                              | Set to half duplex, except for 100BASE-FX and 1000BASE-X, which is set to full duplex.                                                                                                                                                    |
| Port enable/disable                           | Enabled.                                                                                                                                                                                                                                  |
| Port priority                                 | Set to 0.                                                                                                                                                                                                                                 |
| Port speed                                    | Set to 10 Mbps, except for 1000BASE-X, which is set to 1000 Mbps, and 100BASE-FX, which is set to 100 Mbps.                                                                                                                               |
| Port trap                                     | All ports are enabled to send link traps.                                                                                                                                                                                                 |
| Power over Ethernet port admin state          | Administrative state is on (auto).<br>Supported only on switches with PoE.                                                                                                                                                                |
| Priority classification                       | Classification rules are automatically enabled when created.                                                                                                                                                                              |
| RADIUS client                                 | Disabled.                                                                                                                                                                                                                                 |
| RADIUS retries                                | When the client is enabled, set to 3.                                                                                                                                                                                                     |
| RADIUS timeout                                | When the client is enabled, set to 20 seconds.                                                                                                                                                                                            |
| Rate limiting                                 | Disabled globally and on all ports. (Available only on A4 switches.)                                                                                                                                                                      |
| Security mode                                 | Normal.                                                                                                                                                                                                                                   |
| SNMP                                          | Enabled.                                                                                                                                                                                                                                  |
| SNTP                                          | Disabled.                                                                                                                                                                                                                                 |
| Spanning Tree                                 | Globally enabled and enabled on all ports.                                                                                                                                                                                                |
| Spanning Tree edge port administrative status | Edge port administrative status begins with the value set to <b>false</b> initially after the device is powered up. If a Spanning Tree BPDU is not received on the port within a few seconds, the status setting changes to <b>true</b> . |
| Spanning Tree edge port delay                 | Enabled.                                                                                                                                                                                                                                  |
| Spanning Tree forward delay                   | Set to 15 seconds.                                                                                                                                                                                                                        |
| Spanning Tree hello interval                  | Set to 2 seconds.                                                                                                                                                                                                                         |
| Spanning Tree ID (SID)                        | Set to 0.                                                                                                                                                                                                                                 |
| Spanning Tree maximum aging time              | Set to 20 seconds.                                                                                                                                                                                                                        |
| Spanning Tree port priority                   | All ports with bridge priority are set to 128 (medium priority).                                                                                                                                                                          |
| Spanning Tree priority                        | Bridge priority is set to 32768.                                                                                                                                                                                                          |

**Table 4-1 Default Settings for Basic Switch Operation (continued)**

| Feature                                        | Default Setting                                                                                                                |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Spanning Tree topology change trap suppression | Enabled.                                                                                                                       |
| Spanning Tree version                          | Set to mstp (Multiple Spanning Tree Protocol).                                                                                 |
| SSH                                            | Disabled.                                                                                                                      |
| System baud rate                               | Set to 9600 baud.                                                                                                              |
| System contact                                 | Set to empty string.                                                                                                           |
| System location                                | Set to empty string.                                                                                                           |
| System name                                    | Set to empty string.                                                                                                           |
| Telnet                                         | Enabled inbound and outbound.                                                                                                  |
| Telnet port (IP)                               | Set to port number 23.                                                                                                         |
| Terminal                                       | CLI display set to 80 columns and 24 rows.                                                                                     |
| Timeout                                        | Set to 5 minutes.                                                                                                              |
| User names                                     | Login accounts set to <b>ro</b> for Read-Only access; <b>rw</b> for Read-Write access; and <b>admin</b> for Super User access. |
| VLAN dynamic egress                            | Disabled on all VLANs.                                                                                                         |
| VLAN ID                                        | All ports use a VLAN identifier of 1.                                                                                          |
| Host VLAN                                      | Default host VLAN is 1.                                                                                                        |

Not all of the following routing features are available on all platforms. Some routing protocols require a separate license to become operable. Check the Release Notes for your specific platforms for details.

**Table 4-2 Default Settings for Router Operation**

| Feature                            | Default Setting                  |
|------------------------------------|----------------------------------|
| Access groups (IP security)        | None configured.                 |
| Access control lists               | None configured.                 |
| Area authentication (OSPF)         | Disabled.                        |
| Area default cost (OSPF)           | Set to 1.                        |
| Area NSSA (OSPF)                   | None configured.                 |
| Area range (OSPF)                  | None configured.                 |
| ARP table                          | No permanent entries configured. |
| ARP timeout                        | Set to 14,400 seconds.           |
| Authentication key (RIP and OSPF)  | None configured.                 |
| Authentication mode (RIP and OSPF) | None configured.                 |
| Dead interval (OSPF)               | Set to 40 seconds.               |
| Disable triggered updates (RIP)    | Triggered updates allowed.       |
| Distribute list (RIP)              | No filters applied.              |
| DVMRP                              | Disabled. Metric set to 1.       |



**Table 4-2 Default Settings for Router Operation (continued)**

| Feature                    | Default Setting                                                                                                                                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hello interval (OSPF)      | Set to 10 seconds for broadcast and point-to-point networks. Set to 30 seconds for non-broadcast networks.                                                                                                                 |
| ICMP                       | Enabled for echo-reply and mask-reply modes.                                                                                                                                                                               |
| IP-directed broadcasts     | Disabled.                                                                                                                                                                                                                  |
| IP forward-protocol        | Enabled with no port specified.                                                                                                                                                                                            |
| IP interfaces              | Disabled with no IP addresses specified.                                                                                                                                                                                   |
| IRDP                       | Disabled on all interfaces. When enabled, maximum advertisement interval is set to 600 seconds, minimum advertisement interval is set to 450 seconds, holdtime is set to 1800 seconds, and address preference is set to 0. |
| MD5 authentication (OSPF)  | Disabled with no password set.                                                                                                                                                                                             |
| MTU size                   | Set to 1500 bytes on all interfaces.                                                                                                                                                                                       |
| OSPF                       | Disabled.                                                                                                                                                                                                                  |
| OSPF cost                  | Set to 10 for all interfaces.                                                                                                                                                                                              |
| OSPF network               | None configured.                                                                                                                                                                                                           |
| OSPF priority              | Set to 1.                                                                                                                                                                                                                  |
| Passive interfaces (RIP)   | None configured.                                                                                                                                                                                                           |
| Proxy ARP                  | Enabled on all interfaces.                                                                                                                                                                                                 |
| Receive interfaces (RIP)   | Enabled on all interfaces.                                                                                                                                                                                                 |
| Retransmit delay (OSPF)    | Set to 1 second.                                                                                                                                                                                                           |
| Retransmit interval (OSPF) | Set to 5 seconds.                                                                                                                                                                                                          |
| RIP receive version        | Set to accept both version 1 and version 2.                                                                                                                                                                                |
| RIP send version           | Set to version 1.                                                                                                                                                                                                          |
| RIP offset                 | No value applied.                                                                                                                                                                                                          |
| SNMP                       | Enabled.                                                                                                                                                                                                                   |
| Split horizon              | Enabled for RIP packets without poison reverse.                                                                                                                                                                            |
| Stub area (OSPF)           | None configured.                                                                                                                                                                                                           |
| Timers (OSPF)              | SPF delay set to 5 seconds. SPF holdtime set to 10 seconds.                                                                                                                                                                |
| Transmit delay (OSPF)      | Set to 1 second.                                                                                                                                                                                                           |
| VRRP                       | Disabled.                                                                                                                                                                                                                  |

## Initial Configuration Overview

To configure your stackable or standalone switch for the first time, see [Chapter 1, Setting Up a Switch for the First Time](#). That chapter includes information about how to directly connect to the switch via the console port and an Ethernet cable to set the switch's IP address and to download the latest firmware. The procedures in this chapter assume an in-band connection over the network to the switch using Telnet or SSH to establish a CLI session on the switch.

[Procedure 4-1](#) contains the steps to assign an IP address and configure basic system parameters. Some of these steps are also covered in [Chapter 1, Setting Up a Switch for the First Time](#). For information on the command syntax and parameters, refer to the online help or the *CLL Reference* for your platform.



**Note:** When configuring any string or name parameter input for any command, do not use any letters with diacritical marks (an ancillary glyph added to a letter). Diacritical marked letters are not supported by SNMP.

#### Procedure 4-1 Initial Setup

| Step | Task                                                                                                                                                                                                                                                            | Command                                                                                                                                                                  |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Log in as an administrator.                                                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>At the login prompt, enter <b>admin</b>.</li> <li>Press <b>Enter</b> for the password (no password string by default).</li> </ul> |
| 2    | For security, change the password.                                                                                                                                                                                                                              | <b>set password</b>                                                                                                                                                      |
| 3    | Optionally, check the version of the firmware image then check the Enterasys Networks web site to verify that you have the latest version.                                                                                                                      | <b>show version</b>                                                                                                                                                      |
| 4    | Optionally, define a name for the system, the location of the system, and contact information for system issues.                                                                                                                                                | <b>set system name</b> [ <i>string</i> ]<br><b>set system location</b> [ <i>string</i> ]<br><b>set system contact</b> [ <i>string</i> ]                                  |
| 5    | Optionally, define a pre- or post-login message to be displayed.                                                                                                                                                                                                | <b>set banner</b> { <b>motd</b>   <b>login</b> } <i>message</i>                                                                                                          |
| 6    | Optionally, change the default prompt.                                                                                                                                                                                                                          | <b>set prompt</b> " <i>prompt_string</i> "                                                                                                                               |
| 7    | Display the system's setting for the date and time. If necessary, change the setting.<br><br><b>NOTE:</b> Instead of manually setting the time, you can configure the system as an SNTP client, as described in " <a href="#">SNTP Overview</a> " on page 7-10. | <b>show time</b><br><b>set time</b> [ <i>mm/dd/yyyy</i> ] [ <i>hh:mm:ss</i> ]                                                                                            |
| 8    | Assign a switch IP address.                                                                                                                                                                                                                                     | <b>set ip address</b>                                                                                                                                                    |
| 9    | If desired, configure additional user accounts and passwords. Up to 32 user accounts may be registered with the local database.                                                                                                                                 | <b>set system login</b> <i>username</i><br><b>set</b>                                                                                                                    |

## Advanced Configuration Overview

The switch can be configured to provide various system services, Layer 2 switching, Layer 3 routing, and security. [Table 4-3](#) provides an overview of configuring the switch for each area.



**Note:** Though it is possible to configure policy by using the CLI, Enterasys Networks recommends that you use NetSight instead.

**Table 4-3 Advanced Configuration**

| Task                                                      | Refer to ...                                        |
|-----------------------------------------------------------|-----------------------------------------------------|
| <b>System Services</b>                                    |                                                     |
| Configure the Simple Network Time Protocol (SNTP) client. | " <a href="#">SNTP Configuration</a> " on page 4-11 |

**Table 4-3 Advanced Configuration (continued)**

| Task                                                                                                                                                                                                  | Refer to ...                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Configure the Telnet client and server. (Telnet client is enabled by default.)<br><b>Note:</b> For security, you may wish to disable Telnet and only use SSH.                                         | “ <a href="#">Telnet Overview</a> ” on page 4-23                                 |
| Configure the Secure Shell V2 (SSHv2) client and server.                                                                                                                                              | “ <a href="#">SSH Overview</a> ” on page 4-24                                    |
| Configure the Dynamic Host Configuration Protocol (DHCP) server.                                                                                                                                      | “ <a href="#">DHCP Configuration</a> ” on page 4-16                              |
| Configure the port parameters, such as speed and duplex mode.                                                                                                                                         | “ <a href="#">Port Configuration Overview</a> ” on page 8-1                      |
| Enable SNMP and create a community string.z                                                                                                                                                           | “ <a href="#">Configuring SNMP</a> ” on page 12-7                                |
| Configure RMON to provide comprehensive network fault diagnosis, planning, and performance tuning information, and allow for interoperability between SNMP management stations and monitoring agents. | Chapter 18, <a href="#">Configuring Network Monitoring</a>                       |
| Change the interactive login authentication method, from local to remote (RADIUS authentication).                                                                                                     | “ <a href="#">User Authentication Overview</a> ” on page 10-1                    |
| If RADIUS authentication is configured, configure the remote RADIUS servers to be used by the RADIUS client on the switch                                                                             | “ <a href="#">Configuring RADIUS</a> ” on page 10-21                             |
| <b>Layer 2 Switching</b>                                                                                                                                                                              |                                                                                  |
| Set port configurations and port-based Virtual Local Area Networks (VLANs). VLANs can be created statically or dynamically.                                                                           | Chapter 9, <a href="#">Configuring VLANs</a>                                     |
| Configure ports to prioritize traffic based on Class of Service.                                                                                                                                      | “ <a href="#">Port Priority and Transmit Queue Configuration</a> ” on page 17-15 |
| Configure Spanning Trees using STP, RSTP, or MSTP.                                                                                                                                                    | Chapter 15, <a href="#">Configuring Spanning Tree</a>                            |
| Configure LLDP or CDP.                                                                                                                                                                                | Chapter 13, <a href="#">Configuring Neighbor Discovery</a>                       |
| <b>Layer 3 Routing</b>                                                                                                                                                                                |                                                                                  |
| Configure the router id.<br>Refer to the <b>router id</b> command in your platform’s <i>CLI Reference</i> .                                                                                           |                                                                                  |
| Configure interfaces for IP routing.                                                                                                                                                                  | “ <a href="#">Routing Interfaces</a> ” on page 20-3                              |
| Configure the ARP table.                                                                                                                                                                              | “ <a href="#">The ARP Table</a> ” on page 20-6                                   |
| Configure UDP broadcast forwarding, including DHCP/BOOTP relay agent.                                                                                                                                 | “ <a href="#">IP Broadcast Settings</a> ” on page 20-7                           |
| Configure static routes.                                                                                                                                                                              | “ <a href="#">IP Static Routes</a> ” on page 20-4                                |
| Configure ICMP Router Discovery Protocol (IRDP).                                                                                                                                                      | “ <a href="#">Configuring IRDP</a> ” on page 21-5                                |

**Table 4-3 Advanced Configuration (continued)**

| <b>Task</b>                                                                           | <b>Refer to ...</b>                                    |
|---------------------------------------------------------------------------------------|--------------------------------------------------------|
| Configure RIP.                                                                        | "Configuring RIP" on page 21-1                         |
| Configure OSPFv2.                                                                     | Chapter 22,<br><b>Configuring OSPFv2</b>               |
| Configure multicast protocols IGMP, DVMRP, and PIM, and general multicast parameters. | Chapter 19,<br><b>Configuring Multicast</b>            |
| Configure VRRP.                                                                       | Chapter 23,<br><b>Configuring VRRP</b>                 |
| Configure IPv6                                                                        | Chapter 25,<br><b>Configuring and Managing IPv6</b>    |
| <b>Security and General Management</b>                                                |                                                        |
| Configure Access Control Lists (ACLs).                                                | Chapter 24,<br><b>Configuring Access Control Lists</b> |
| Manage user accounts and passwords.                                                   | Chapter 5, <b>User Account and Password Management</b> |
| Configure system logging.                                                             | Chapter 14,<br><b>Configuring Syslog</b>               |
| Configure the switch using text files.                                                | "Managing Switch Configuration and Files" on page 6-4  |
| Upgrade system firmware.                                                              | "Managing the Firmware Image" on page 6-1              |
| Configure QoS features.                                                               | Chapter 17,<br><b>Configuring Quality of Service</b>   |
| Configure policy.                                                                     | Chapter 16,<br><b>Configuring Policy</b>               |

## Licensing Advanced Features

In order to enable certain advanced features on some of the Fixed Switching platforms, you must purchase and activate a license key. If you have purchased a license, follow the instructions on Licensed Product Entitlement ID sheet to obtain the license activation key from the Enterasys customer site.

If you wish to obtain a license, contact the Enterasys Networks Sales Department.

This section describes how to apply advanced feature licenses to Fixed Switching platforms.

### License Implementation Differences

Licensing is implemented differently on the C5 platform from the previous implementation that is used on the C3, B3, and G3 platforms.

## Node-Locked Licensing

On the C3, B3, and G3 platforms, licenses are locked to the serial number of the switch to which the license applies. Therefore, you must know the serial number of the switch to be licensed when you activate the license on the Enterasys customer site, and also when you apply the license to the switch as described below. Each switch to be licensed must have its own license and key and all members of a stack must be licensed in order to support licensed features in a stack environment.

If you need to move a license from one hardware platform to another, you must contact Enterasys Customer Support to arrange for re-hosting of the license.

### Node-Locked License Key Fields

When Enterasys supplies a license, it will be sent to you as a character string similar to the following:

```
INCREMENT advrouter 2010.0127 permanent 0123456789AB 0123456789AB
```

The contents of the six fields, from the left, indicate:

- Type—the type of license. The value in this field is always “INCREMENT.”
- Feature—description of the feature being licensed. For example, “advrouter” as shown in the character string above.
- Date-based version (DBV)—a date-related string. The value in this field is not significant.
- Expiration type—indicates whether the license is a permanent or an evaluation license. If the license is an evaluation license, this field will contain the expiration date of the license. If the license is a permanent license, this field will contain the word “permanent.”
- Key—the license key.
- Host ID—the serial number of the switch to which this license applies.

When activating licenses on stackable devices, we recommend that you copy and paste the license character string, rather than entering the text manually.

## Non-Node-Locked Licensing

On the C5 platform, licenses are not locked to individual switches. When you activate your licenses on the Enterasys customer site, the key that is generated contains information about how many licenses you have purchased and therefore, how many switches the license key can be applied to. For example, if you buy 8 C5 licenses, when you activate your licenses on the Enterasys customer site, one key is generated that can enable the licensed feature on up to 8 C5 switches.

If you apply a license to a stack that has more members than the license key allows, applying the license will fail on the extra members. For example, if you buy 6 C5 licenses and apply that key to a stack of 8 C5 switches, licensing will fail on members 7 and 8.



**Note:** Multi-node non-node-locked licenses are not currently available. You should buy individual licenses for all switches on which you want to enable the advanced features.

## Licensing in a Stack Environment

All members of a stack must be licensed in order to support licensed features in a stack environment. If the master unit in a stack has an activated license, all member units also must have an activated license in order to operate. If the master unit in a stack does not have an activated license, then the licensed functionality will not be available to member units, even if they have licenses installed.

When adding a new unit to an existing stack, the ports on a switch lacking a licensed feature that has been enabled on the master will not pass traffic until the license has been enabled on the added switch. (The ports are in the “ConfigMismatch” state.)

If you clear a license from a member unit in a stack while the master unit has a activated license, the status of the member will change to “ConfigMismatch” and its ports will be detached from the stack. If you clear a license from the master unit of a stack, the member units will remain attached to the stack, but the licensed functionality will no longer be available.

## Applying Node-Locked Licenses in a Stack

The licenses for all members of an operating stack can be activated during a single CLI session, by following these steps:

1. Obtain valid licenses for all members of the stack from the Enterasys customer site.
2. Optionally, note the serial numbers of the switches in the stack. You can use the **show system hardware** command to display the switch serial numbers.



**Caution:** Since license keys are applied to the correct stack member switch automatically, based on the switch serial number that is part of the license string, you should know the serial numbers of the switches in order to enable the licenses of the member switches first, before the master unit.

3. Enable the licenses on the stack members first, before enabling the master unit, using the **set license** command. For example:

```
B3(rw)->set license INCREMENT policy 2006.0127 permanent 0123456789AB
0123456789AB
```

4. Enable the license on the switch master unit last, using the **set license** command.

## Applying Non-Node-Locked Licenses in a Stack

When applying non-node-locked licenses, ensure that you have purchased enough licenses for all members of the stack. All members of the stack do not need to use the same license key, but all switches in the stack must have a license applied in order to support the licensed feature. Note that the license key itself contains information about how many switches the license key can be applied to.

1. Obtain valid license keys for all members of the stack from the Enterasys customer site.
2. Activate one or more licenses on the stack.
  - a. If you have a license with a license quantity that is equal to or greater than the number of switches in the stack, use the **set license** command with no optional **unit** number. For example:

```
C5(su)->set license advrouter "0001:C5L3-LIC:2:4a76f2c8:0:Your
Company Name Here:000E0C0973C5:150a9501:bec749e9ec095844d727a2db8
8a31514"
```

```
Validating license on unit 1
License successfully validated and set on unit 1
```

```
Validating license on unit 2
License successfully validated and set on unit 2
```

```
Validating license on unit 3
License successfully validated and set on unit 3
```

- b. If you need to use multiple license keys on members of a stack, use the optional **unit** number parameter with the **set license** command. The following example applies two different license keys to members of the stack.

```
C5(su)->set license advrouter "0001:C5L3-LIC:2:4a76f2c8:0: Enterasys Networks:000E0C0973C5:150a9501:bec749e9ec095844d727a2db88a31514" unit 1
```

```
Validating license on unit 1
License successfully validated and set on unit 1
```

```
C5(su)->set license advrouter "0001:C5L3-LIC:2:4a76f2c8:A: Enterasys Networks:A00E0C0973D9:150a9501:098749e9ec095844d727a2db88a31514" unit 2
```

```
Validating license on unit 2
License successfully validated and set on unit 2
```

## Adding a New Member to a Licensed Stack

When adding a new unit to an existing stack, the ports on a switch lacking a licensed feature that has been enabled on the master will not pass traffic until the license has been enabled on the added switch. (The ports are in the “ConfigMismatch” state.)

1. For B3 or C3 switches, obtain a node-locked license for the new switch. For C5 switches, check that you have a non-node-locked license that can be applied to the new switch.
2. Add the new unit to the stack, following the procedure in [“Adding a New Unit to an Existing Stack”](#) on page 2-3.
3. Use the **set license** command to install and activate the new switch’s license. The new switch will then join the stack and its ports will be attached.

Alternatively, you can install and activate the new switch’s license first, before adding the switch to the stack.

## Displaying and Clearing Licenses

Licenses can be displayed and cleared only with the **show license** and **clear license** commands. General configuration commands such as **show config** or **clear config** do not apply to licenses.

If you clear a license from a member unit in a stack while the master unit has an activated license, the status of the member will change to “ConfigMismatch” and its ports will be detached from the stack.

If you clear a license from the master unit of a stack, the member units will remain attached to the stack but the licensed functionality will no longer be available.

## SNTP Configuration

Simple Network Time Protocol (SNTP) provides for the synchronizing of system time for managed devices across a network. The Fixed Switch implementation supports unicast polling and broadcast listening modes of operation to obtain the time from an SNTP server. SNTP is a subset of the Network Time Protocol (NTP) as specified in RFC 1305. The most recent version of SNTP is specified in RFC 2030. Since SNTP is a subset of NTP, all NTP servers are capable of servicing SNTP clients. The SNTP mode is set on the client using the **set sntp client** command.

## Unicast Polling Mode

When an SNTP client is operating in unicast mode, SNTP update requests are made directly to a server, configured using the **set sntp server** command. The client queries these configured SNTP servers at a fixed poll-interval configured using the **set sntp poll-interval** command. The order in which servers are queried is based on a precedence value optionally specified when you configure the server. The lower the configured precedence value, the higher the precedence for that server. The default is for all servers to have the same precedence. In this case, the server ordering is based upon the indexing of the server table.

The SNTP client makes a request to the SNTP server. The client waits a period of time configured using the **set sntp poll-timeout** command for a response from the server. If the poll timeout timer expires, the client will resend another request, up to the number of retries specified by the **set sntp poll-retry** command. If the retries have been exhausted, the client request is sent to the next server with the lowest configured precedence value or the next server in the server table, if precedence values are the same. If no server responds, the client waits the configured poll-interval time period and the process starts over again.

## Broadcast Listening Mode

With SNTP configured for broadcast listening mode, the client is passive and it is the broadcast server that broadcasts the time to the client. Broadcast listening uses the same poll-interval, poll-timeout and poll-retry values as unicast polling.

## SNTP Authentication

The Simple Network Time Protocol (SNTP) is used to provide a precise time reference for time critical applications. Therefore, SNTP can pose a security risk if malicious users attempt to corrupt a SNTP timestamp to create a false time on network equipment. SNTP security mechanisms ensure that only authorized servers are allowed to distribute time samples to the SNTP clients.

SNTP provides increased security in the form of authentication. Authentication is intended to overcome security risks by ensuring that any response received from an SNTP time server has come from the intended reference. The user defines a key on the switch and enables authentication. The same key must be defined on the server in order for the switch to accept timestamp information from the server.

The client sends a request for time to an SNTP server. The server then responds to the client with a time sample, along with the encrypted keys configured on the SNTP server. Upon receipt of the time sample, the client un-encrypts the key and verifies the key against the trusted key configured on the switch for a specified SNTP server. The client can then be sure that the received time sample was indeed transmitted from the authorized SNTP server.

SNTP utilizes MD5 authentication (Message Digest Encryption 5), which safeguards device synchronization paths to SNTP servers. MD5 is 128-bit cryptographic hash function, which outputs a fingerprint of the key. MD5 verifies the integrity of the communication and authenticates the origin of the communication.

### Authentication Key and Trusted Key List

The SNTP authentication key specifies the authentication instance to be used by the SNTP client when authenticating with the SNTP server. The SNTP client supports the configuration of up to 5 authentication keys. The authentication key instance ID is a numeric value. Each authentication key instance specifies the authentication type and password. SNTP authentication supports the MD5 authentication algorithm. The password is known to both the SNTP client and server. The password consists of an ASCII string of up to 32 non-white characters.



Use the **set sntp authentication key** command to configure an authentication key instance.

The SNTP authentication key is associated with an SNTP server using the **set sntp server** command.

An authentication key has to be trusted to be used with an SNTP server. Use the **set sntp trusted-key** command to add an authentication key to the trusted key list.

Refer to [Procedure 4-3](#) on page 4-14 to configure the switch SNTP client for authentication.

## SNTP Defaults

[Table 4-4](#) lists SNTP parameters and their default values.

**Table 4-4 Default SNTP Parameters**

| Parameter                 | Description                                                                                                              | Default Value          |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------|------------------------|
| SNTP client mode          | Specifies whether the current SNTP state is broadcast, unicast, or disabled.                                             | disabled               |
| unicast server precedence | Specifies a value that determines the order in which SNTP servers are polled if the precedence values are not the same.  | 1 (highest precedence) |
| poll-interval             | Specifies the interval between unicast SNTP requests by the client to the server.                                        | 512 seconds            |
| poll-retry                | Specifies the number of times the client will resend the SNTP request to the server before moving on to the next server. | 1                      |
| poll-timeout              | Specifies the amount of time a client will wait for a response from the the SNTP server before retrying.                 | 5 seconds              |
| timezone offset           | Specifies the offset in hours and minutes from UTC for this device                                                       | 0 hours, 0 minutes     |
| SNTP authentication mode  | Specifies whether authentication for all SNTP client communications is enabled or disabled.                              | disabled               |

## Configuring SNTP

[Procedure 4-2](#) describes how to configure general SNTP parameters. [Procedure 4-3](#) describes how to configure SNTP authentication. Refer to the *CLI Reference* for your platform for details about the commands listed.

**Procedure 4-2 Configuring SNTP**

| Step | Task                                                                                                                         | Command(s)                                                             |
|------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| 1.   | Set the SNTP operation mode on the client.                                                                                   | <b>set sntp client</b> {broadcast   unicast   disable}                 |
| 2.   | When operating in unicast mode, set the SNTP server(s) for this client, optionally specifying a precedence value per server. | <b>set sntp server</b> ip-address [precedence precedence] [key key-id] |

**Procedure 4-2 Configuring SNTP (continued)**

| Step | Task                                                                                                                                                                                                                                                                           | Command(s)                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| 3.   | When operating in unicast mode, optionally change the poll interval between SNTP unicast requests.<br><br>The poll interval is 2 to the power of value in seconds, where value can range from 6 to 10.                                                                         | <b>set sntp poll-interval</b> <i>value</i>                                  |
| 4.   | When operating in unicast mode, optionally change the number of poll retries to a unicast SNTP server.                                                                                                                                                                         | <b>set sntp poll-retry</b> <i>retry</i>                                     |
| 5.   | When operating in unicast mode, optionally change the poll timeout for a response to a unicast SNTP request.                                                                                                                                                                   | <b>set sntp poll-timeout</b> <i>timeout</i>                                 |
| 6.   | Optionally, set the SNTP time zone name and the hours and minutes it is offset from Coordinated Universal Time (UTC).<br><br><b>Note:</b> The daylight savings time function can be enabled and associated with the timezone set here using the <b>set summertime</b> command. | <b>set timezone</b> <i>name</i> [ <i>hours</i> ] [ <i>minutes</i> ]         |
| 7.   | Optionally, specify the interface used for the source IP address of the SNTP client. If no interface is specified, then the IP address of the Host interface is used.                                                                                                          | <b>set sntp interface</b> { <i>loopback loop-ID</i>   <i>vlan vlan-ID</i> } |

[Procedure 4-3](#) describes how to configure SNTP authentication. Refer to the *CLI Reference* for your platform for details about the commands listed.

**Procedure 4-3 Configuring SNTP Authentication**

| Step | Task                                                                                                              | Command(s)                                                                                                    |
|------|-------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| 1.   | Configure up to five authentication keys.                                                                         | <b>set sntp authentication-key</b> <i>key-id</i> <b>md5</b> <i>key-value</i>                                  |
| 2.   | Add the configured authentication keys to the trusted key list.                                                   | <b>set sntp trusted-key</b> <i>key-id</i>                                                                     |
| 3.   | Enable authentication on the switch.                                                                              | <b>set sntp authenticate enable</b>                                                                           |
| 4.   | Add the keys to the switch's NTP/SNTP server configurations.                                                      | <b>set sntp server</b> <i>ip-address</i> [ <b>precedence</b> <i>precedence</i> ] [ <b>key</b> <i>key-id</i> ] |
| 5.   | Ensure that the key information configured on the switch is added to the "ntp.keys" file on the NTP/SNTP servers. | N/A                                                                                                           |

[Table 4-5](#) describes how to manage and display SNTP information.

**Table 4-5 Managing and Displaying SNTP**

| Task                                                    | Command(s)                                                  |
|---------------------------------------------------------|-------------------------------------------------------------|
| To display SNTP client, server, and time zone settings: | <b>show sntp</b>                                            |
| To set the SNTP client's operational mode to disable:   | <b>clear sntp client</b>                                    |
| To remove one or all servers from the SNTP server list: | <b>clear sntp server</b> { <i>ip-address</i>   <b>all</b> } |

**Table 4-5 Managing and Displaying SNTP (continued)**

| Task                                                                               | Command(s)                                         |
|------------------------------------------------------------------------------------|----------------------------------------------------|
| To reset the poll interval between unicast SNTP requests to its default value:     | <b>clear sntp poll-interval</b>                    |
| To reset the number of poll retries to a unicast SNTP server to its default value: | <b>clear sntp poll-retry</b>                       |
| To reset the SNTP poll timeout to its default value:                               | <b>clear sntp poll-timeout</b>                     |
| To clear an SNTP authentication key:                                               | <b>clear sntp authentication-key</b> <i>key-id</i> |
| To remove an authentication key from the trusted key list:                         | <b>clear sntp trusted-key</b> <i>key-id</i>        |

## SNTP Configuration Example

The following example configures the SNTP client for unicast mode, generates two authentication keys and adds them to the trusted key list, enables authentication, and configures two SNTP servers with different precedence and authentication keys for the SNTP client to contact.

All the rest of the SNTP parameters are left at their default values. The **show sntp** command displays the current settings.

```
B3(su)->set sntp authentication-key 1 md5 mykey
B3(su)->set sntp trusted-key 1
B3(su)->set sntp authentication-key 2 md5 keytwo
B3(su)->set sntp trusted-key 2
B3(su)->set sntp authenticate enable
B3(su)->set sntp client unicast
B3(su)->set sntp server 192.168.10.10 precedence 1 key 1
B3(su)->set sntp server 192.168.10.20 precedence 2 key 2
```

```
B3(su)->show sntp
SNTP Version: 3
Current Time: SAT JUN 29 17:16:38 2002
Timezone: '' offset from UTC is 0 hours and 0 minutes
Client Mode: unicast
Trusted Keys : 1 2
Broadcast Count: 2
Poll Interval: 9 (512 seconds)
Poll Retry: 1
Poll Timeout: 5 seconds
SNTP Poll Requests: 4
Last SNTP Update: THU JAN 01 00:00:00 1970
Last SNTP Request: SAT JUN 29 17:16:36 2002
Last SNTP Status: Timed Out
```

```
SNTP-Server Precedence Key Status

192.168.10.20 2 2 Active
```

192.168.10.10

1

1

Active

## DHCP Configuration

Dynamic Host Configuration Protocol (DHCP) for IPv4 is a network layer protocol that implements automatic or manual assignment of IP addresses and other configuration information to client devices by servers. A DHCP server manages a user-configured pool of IP addresses from which it can make assignments upon client requests. A relay agent passes DHCP messages between clients and servers which are on different physical subnets.

### DHCP Relay Agent

The DHCP/BOOTP relay agent function can be configured on all of the switch's routing interfaces. The relay agent can forward a DHCP client's request to a DHCP server located on a different network if the address of the server is configured as a helper address on the receiving interface. The relay agent interface must be a VLAN which is configured with an IP address. Refer to the **ip helper-address** command in the *CLI Reference* for your platform for more information.



**Note:** DHCP Relay Agent is not supported on the I-Series platform because the I-Series does not support routing.

### DHCP Server

DHCP server functionality allows the switch to provide basic IP configuration information to a client on the network who requests such information using the DHCP protocol.

DHCP provides the following mechanisms for IP address allocation by a DHCP server:

- Automatic—DHCP server assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address) from a defined pool of IP addresses configured on the server.
- Manual—A client's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the client. This is managed by means of "static" address pools configured on the server.

The amount of time that a particular IP address is valid for a system is called a lease. The switch maintains a lease database which contains information about each assigned IP address, the MAC address to which it is assigned, the lease expiration, and whether the address assignment is dynamic (automatic) or static (manual). The DHCP lease database is stored in flash memory.

In addition to assigning IP addresses, the DHCP server can also be configured to assign the following to requesting clients:

- Default router(s)
- DNS server(s) and domain name
- NetBIOS WINS server(s) and node name
- Boot file
- DHCP options as defined by RFC 2132



**Note:** A total of 16 address pools, dynamic and/or static, and a maximum of 256 addresses for the entire switch, can be configured on the Fixed Switch platforms.

## IP Address Pools

IP address pools must be configured for both automatic and manual IP address allocation by a DHCP server.

### Automatic IP Address Pools

When configuring an IP address pool for dynamic IP address assignment, the only *required* steps are to name the pool and define the network number and mask for the pool using the **set dhcp pool network** command. Note that:

- When the switch is configured for routing and the IP address pool is associated with a routing interface, the pool has to be in the same subnet as the routed interface and use the same mask configured on the routed interface
- When the switch is not configured for routing, the pool has to be in the same subnet and use the same mask as the system host port IP address.
- You can limit the scope of addresses assigned to a pool for dynamic address assignment with the **set dhcp exclude** command. Up to 128 non-overlapping address ranges can be excluded on the Fixed Switches. For example:

```
set dhcp exclude 192.0.0.1 192.0.0.10
```



**Note:** The IP address of the system's host port or the routed interface is automatically excluded.

For more information about configuring automatic IP address pools, see “[Configuring DHCP IP Address Pools](#)” on page 4-21.

### Manual IP Address Pools

When you are configuring static address pools for manual address assignment with **set dhcp pool** commands, the only *required* steps are to name the pool, configure either the hardware address of the client or the client identifier, and configure the IP address and mask for the manual binding.

For more information about configuring manual IP address pools, see “[Configuring DHCP IP Address Pools](#)” on page 4-21.

## Configuring a DHCP Server

On Fixed Switch platforms that support basic routing, there are two ways to configure a DHCP server: one is to associate the DHCP address pool with the switch's host port IP address, and the other is to associate the DHCP address pool with a routed interface.

Since on a Fixed Switch platform that supports routing, the host port IP address cannot fall within a configured routed interface on the system, a typical system configured with routing interfaces will not have a host port IP address. Therefore, all DHCP pools would be associated with routed interfaces.

On the I-Series, which does not support routing, the DHCP address pool must be associated with the switch's host port IP address.

Refer to [Table 4-7](#) on page 4-20 for a list of default DHCP server settings.

## DHCP Configuration on a Non-Routing System

The following procedure provides basic DHCP server functionality when the DHCP pool is associated with the system's host IP address. This procedure would typically be used when the system is NOT configured for routing.

Refer to the *CLI Reference* for your platform for details about the commands listed below.

### Procedure 4-4 DHCP Server Configuration on a Non-Routing System

| Step | Task                                                                                                                                                                                                                                                                                                                                                      | Command(s)                                                                                                                                         |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Configure the system (or stack) host port IP address.                                                                                                                                                                                                                                                                                                     | <b>set ip address</b> <i>ip-address</i> [ <b>mask</b> <i>ip-mask</i> ] [ <b>gateway</b> <i>ip-gateway</i> ]                                        |
| 2.   | Enable DHCP server functionality on the system.                                                                                                                                                                                                                                                                                                           | <b>set dhcp enable</b>                                                                                                                             |
| 3.   | Configure an IP address pool for dynamic IP address assignment. Note that the pool has to be in the same subnet and use the same mask as the system host port IP address.<br><br>Refer to “ <a href="#">Manual IP Pool Configuration</a> ” on page 4-21 for information about configuring a manual pool and for additional IP address pool configuration. | <b>set dhcp pool</b> <i>poolname</i> <b>network</b> <i>subnet</i> { <i>mask</i>   <i>prefix-length</i> }                                           |
| 4.   | Optionally, limit the scope of addresses assigned to the pool.<br><br>Remove address exclusions with the <b>clear dhcp exclude</b> command.                                                                                                                                                                                                               | <b>set dhcp exclude</b> <i>low-ipaddr</i> [ <i>high-ipaddr</i> ]<br><br><b>clear dhcp exclude</b> <i>low-ipaddr</i> [ <i>high-ipaddr</i> ]         |
| 5.   | Optionally, set other DHCP server parameters.                                                                                                                                                                                                                                                                                                             | <b>set dhcp conflict logging</b><br><br><b>set dhcp bootp</b> { <i>enable</i>   <i>disable</i> }<br><br><b>set dhcp ping packets</b> <i>number</i> |

### Example

The following example configures the switch's host port IP address, enables DHCP, and creates a dynamic IP address pool named “autopool1” in the same subnet as the host port IP address. All DHCP clients served by this switch must be in the same VLAN as the system's host port.

```
B3(su)->set ip address 192.0.0.50 mask 255.255.255.0
B3(su)->set dhcp enable
B3(su)->set dhcp pool autopool1 network 192.0.0.0 255.255.255.0
B3(su)->set dhcp exclude 192.0.0.20 192.0.0.28
```

## DHCP Configuration on a Routing System

The following procedure provides basic DHCP server functionality when the DHCP pool is associated with a routed interface.

Refer to the *CLI Reference* for your platform for details about the commands listed below.

### Procedure 4-5 DHCP Server Configuration on a Routing System

| Step | Task                                                                                                                                                                                                                                                                                                                                                                              | Command(s)                                                                                                                            |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Create a VLAN and add ports to the VLAN. Only DHCP clients associated with this VLAN will be served IP addresses from the DHCP address pool associated with this routed interface (VLAN).                                                                                                                                                                                         | <code>set vlan create vlan-id</code><br><code>set port vlan port-string vlan-id</code>                                                |
| 2.   | Create a routed interface for the VLAN in router configuration mode.                                                                                                                                                                                                                                                                                                              | <code>interface vlan vlan-id</code><br><code>no shutdown</code><br><code>ip address ip-addr ip-mask</code>                            |
| 3.   | Enable DHCP server functionality in switch mode.                                                                                                                                                                                                                                                                                                                                  | <code>set dhcp enable</code>                                                                                                          |
| 4.   | Configure an IP address pool for dynamic IP address assignment. Note that the pool has to be in the same subnet as the routed interface and use the same mask configured on the routed interface.<br><br>Refer to “ <a href="#">Manual IP Pool Configuration</a> ” on page 4-21 for information about configuring a manual pool and for additional IP address pool configuration. | <code>set dhcp pool poolname network subnet {mask   prefix-length}</code>                                                             |
| 5.   | Optionally, limit the scope of addresses assigned to the dynamic pool.<br><br>Remove address exclusions with the <b>clear dhcp exclude</b> command.                                                                                                                                                                                                                               | <code>set dhcp exclude low-ipaddr [high-ipaddr]</code><br><code>clear dhcp exclude low-ipaddr [high-ipaddr]</code>                    |
| 6.   | Optionally, set other DHCP server parameters.                                                                                                                                                                                                                                                                                                                                     | <code>set dhcp conflict logging</code><br><code>set dhcp bootp {enable   disable}</code><br><code>set dhcp ping packets number</code> |

### Example

In this example, VLAN 6 is created and ports ge.1.1 through ge.1.10 are added to VLAN 6. An IP address is associated with routed interface VLAN 6 in router configuration mode. Returning to switch mode, DHCP is enabled and a dynamic IP address pool is configured in the same subnet as the routed interface. DHCP clients in VLAN 6 will be served IP addresses from this DHCP address pool.

```
C5(su)->set vlan create 6
```

```
C5(su)->set port vlan ge.1.1-10 6
```

```
C5(su)->router
```

```
C5(su)->router>enable
```

```
C5(su)->router#configure
```

```
Enter configuration commands:
```

```
C5(su)->router(Config)#interface vlan 6
```

```
C5(su)->router(Config-if(Vlan 6))#no shutdown
```

```
C5(su)->router(Config-if(Vlan 6))#ip address 6.6.1.1 255.255.0.0
```

```
C5(su)->router(Config-if(Vlan 6))#exit
```

```

C5(su)->router(Config)#exit
C5(su)->router#exit
C5(su)->router>exit
C5(su)->set dhcp enable
C5(su)->set dhcp pool autopool2 network 6.6.0.0 255.255.0.0

```

## Managing and Displaying DHCP Server Parameters

Table 4-6 lists additional DHCP server tasks. Refer to Table 4-7 on page 4-20 for default DHCP server settings.

**Table 4-6 Managing and Displaying DHCP Server**

| Task                                                                                                                             | Commands                                          |
|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| To enable or disable automatic address allocation for BOOTP clients                                                              | <code>set dhcp bootp {enable   disable}</code>    |
| To enable logging of address conflict information                                                                                | <code>set dhcp conflict logging</code>            |
| To disable logging of address conflict information                                                                               | <code>clear dhcp conflict logging</code>          |
| To display conflict information for one or all addresses                                                                         | <code>show dhcp conflict [ip-address]</code>      |
| To clear conflict information for one or all addresses                                                                           | <code>clear dhcp conflict {ip-address   *}</code> |
| To set the number of ping packets sent by the DHCP server to an IP address before assigning that address to a requesting client. | <code>set dhcp ping packets number</code>         |
| To return the number of ping packets sent to the default of 2                                                                    | <code>clear dhcp ping packets</code>              |
| To display binding information for one or all IP addresses                                                                       | <code>show dhcp binding [ip-address]</code>       |
| To delete one or all dynamic (automatic) address bindings                                                                        | <code>clear dhcp binding {ip-addr   *}</code>     |
| To display DHCP server statistics                                                                                                | <code>show dhcp server statistics</code>          |
| To clear all DHCP server counters                                                                                                | <code>clear dhcp server statistics</code>         |

## DHCP Server Defaults

**Table 4-7 Default DHCP Server Parameters**

| Parameter        | Description                                                                    | Default Value |
|------------------|--------------------------------------------------------------------------------|---------------|
| DHCP server      | Whether DHCP server functionality is enabled or disabled on the switch         | Disabled      |
| BOOTP clients    | Whether automatic address allocation for BOOTP clients is enabled or disabled. | Disabled      |
| Conflict logging | Whether address conflict information should be logged.                         | Enabled       |



**Table 4-7 Default DHCP Server Parameters**

| Parameter              | Description                                                                                                                     | Default Value |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------|---------------|
| Number of ping packets | Specifies the number of ping packets the DHCP server sends to an IP address before assigning the address to a requesting client | 2 packets     |

## Configuring DHCP IP Address Pools

This section provides procedures for the basic configuration of automatic (dynamic) and manual (static) IP address pools, as well as a list of the commands to configure other optional pool parameters.

Pool names can be up to 31 characters in length.



**Note:** A total of 16 address pools, dynamic and/or static, and a maximum of 256 addresses for the entire switch, can be configured on the Fixed Switch platforms.

### Automatic IP Address Pool Configuration

The only required steps to configure an automatic pool for dynamic address allocation is to give the pool a name and define the network number and mask for the pool. As noted previously (page 4-17):

- When the switch is configured for routing and the IP address pool is associated with a routing interface, the pool has to be in the same subnet as the routed interface and use the same mask configured on the routed interface
- When the switch is not configured for routing, the pool has to be in the same subnet and use the same mask as the system host port IP address.

Refer to the *CLI Reference* for your platform for details about the commands listed below.

#### Procedure 4-6 Automatic IP Address Pool Configuration

| Step | Task                                                                                                                                                  | Command(s)                                                                    |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| 1.   | Create the IP address pool and specify the subnet and mask (or prefix length) to be used by the pool.                                                 | <code>set dhcp pool poolname network subnet {mask   prefix-length}</code>     |
| 2.   | If desired, specify the duration of the lease for an IP address assigned from this address pool. If not specified, the default lease time is one day. | <code>set dhcp pool poolname lease {days [hours [minutes]]   infinite}</code> |
| 3.   | Optionally, configure other pool parameters                                                                                                           | See <a href="#">Table 4-8</a> on page 4-23                                    |
| 4.   | Display the pool configuration.                                                                                                                       | <code>show dhcp pool configuration {poolname   all}</code>                    |

### Manual IP Pool Configuration

The only required steps to configure a manual pool for static address allocation are to name the pool, configure either the hardware address of the client or the client identifier, and configure the IP address and mask for the manual binding.

- The subnet of the IP address being issued should be on the same subnet as the ingress interface (that is, the subnet of the host IP address of the switch, or if routing interfaces are configured, the subnet of the routing interface).
- A manual pool can be configured using either the client's hardware address (**set dhcp pool hardware-address**) or the client's client-identifier (**set dhcp pool client-identifier**), but using both is not recommended.
- If the incoming DHCP request packet contains a client-identifier, then a manual pool configured with that client-identifier must exist on the switch in order for the request to be processed. The hardware address is not checked.
- A hardware address and type (Ethernet or IEEE 802) configured in a manual pool is checked only when a client-identifier is not also configured for the pool and the incoming DHCP request packet does not include a client-identifier option.

Refer to the *CLI Reference* for your platform for details about the commands listed below.

#### Procedure 4-7 Manual IP Address Pool Configuration

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                              | Command(s)                                                                                                                     |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Create the pool using either the client's hardware address or client-identifier.<br><br>Hardware address = the MAC address of client's hardware platform<br><br>Client identifier = concatenation of media type and MAC address of client's hardware platform<br><br>For a list of media type codes, refer to the "Address Resolution Protocol Parameters" section of RFC 1700, Assigned Numbers. | <b>set dhcp pool poolname hardware-address mac-addr [type]</b><br><br>or<br><b>set dhcp pool poolname client-identifier id</b> |
| 2.   | Specify the IP address and mask to be assigned to that client.                                                                                                                                                                                                                                                                                                                                    | <b>set dhcp pool poolname host ip-address [mask   prefix-length]</b>                                                           |
| 3.   | If desired, assign a name to the client.                                                                                                                                                                                                                                                                                                                                                          | <b>set dhcp pool poolname client-name name</b>                                                                                 |
| 4.   | If desired, specify the duration of the lease for an IP address assigned from this address pool.<br><br>If not specified, the default lease time is one day.                                                                                                                                                                                                                                      | <b>set dhcp pool poolname lease {days [hours [minutes]]   infinite}</b>                                                        |
| 5.   | Optionally, configure other pool parameters                                                                                                                                                                                                                                                                                                                                                       | See <a href="#">Table 4-8</a> on page 4-23                                                                                     |
| 6.   | Display the pool configuration.                                                                                                                                                                                                                                                                                                                                                                   | <b>show dhcp pool configuration {poolname   all}</b>                                                                           |

#### Examples

This example configures a manual pool using 0001.f401.2710 as the Ethernet MAC address for the manual address pool named "manual2." Alternatively, the MAC address could have been entered as 00:01:f4:01:27:10. The default type of 1, Ethernet, is accepted.

The IP address that is to be assigned to this client is then configured, and a lease duration of 12 hours is specified, by entering 0 for days and 12 for hours.

```
B5(su)->set dhcp pool manual2 hardware-address 0001.f401.2710
B5(su)->set dhcp pool manual2 host 192.0.0.200 255.255.255.0
B5(su)->set dhcp pool manual2 lease 0 12
```

This example configures a manual pool using a client identifier for a client whose client hardware type is Ethernet and MAC address is 00:01:22:33:44:55. Concatenating these two values, the client

identifier configured in this example must be 01:00:01:22:33:44:55. We then set the lease duration to infinite.

```
C5(rw)->set dhcp pool manual3 client-identifier 01:00:01:22:33:44:55
C5(rw)->set dhcp pool manual3 host 10.12.1.10 255.255.255.0
C5(rw)->set dhcp pool manual3 lease infinite
```

## Configuring Additional Pool Parameters

Table 4-8 lists the commands that can be used to configure additional IP address pool parameters.

**Table 4-8 Configuring Pool Parameters**

| Task                                                                                                                                             | Commands                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| To specify a default boot image for the clients served by the pool, and specify the file server from which the default boot image can be loaded. | <b>set dhcp pool</b> <i>poolname</i> <b>bootfile</b> <i>filename</i><br><b>set dhcp pool</b> <i>poolname</i> <b>next-server</b> <i>ip-address</i>                                                                                                         |
| To specify a default router list for the clients served by the pool. Up to 8 routers can be configured.                                          | <b>set dhcp pool</b> <i>poolname</i> <b>default-router</b> <i>address</i> [ <i>address2</i> ... <i>address8</i> ]                                                                                                                                         |
| To specify one or more DNS servers for the clients served by the pool. Up to 8 DNS servers can be configured.                                    | <b>set dhcp pool</b> <i>poolname</i> <b>dns-server</b> <i>address</i> [ <i>address2</i> ... <i>address8</i> ]                                                                                                                                             |
| To specify a domain name to be assigned to the clients served by the pool.                                                                       | <b>set dhcp pool</b> <i>poolname</i> <b>domain-name</b> <i>domain</i>                                                                                                                                                                                     |
| To specify up to 8 NetBIOS name servers and the NetBIOS node type for the clients served by the pool.                                            | <b>set dhcp pool</b> <i>poolname</i> <b>netbios-name-server</b> <i>address</i> [ <i>address2</i> ... <i>address8</i> ]<br><b>set dhcp pool</b> <i>poolname</i> <b>netbios-node-type</b> { <b>b-node</b>   <b>h-node</b>   <b>p-node</b>   <b>m-node</b> } |
| To configure DHCP options, described in RFC 2132.                                                                                                | <b>set dhcp pool</b> <i>poolname</i> <b>option</b> <i>code</i> { <b>ascii</b> <i>string</i>   <b>hex</b> <i>string-list</i>   <b>ip</b> <i>addresslist</i> }                                                                                              |

## Telnet Overview

Telnet provides an unsecured communications method between a client and the switch.

Telnet is activated by enabling Telnet on the device, using the **set telnet enable** command in switch mode. By default, Telnet is enabled both inbound and outbound. Use the **show telnet** command to display whether Telnet is currently enabled or disabled.

The Enterasys fixed switches allow a total of four inbound and / or outbound Telnet session to run simultaneously.

## Configuring Telnet

### Procedure 4-8 Configuring Telnet

| Step | Task                                                                                                                                                                               | Command(s)                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| 1.   | Enable or disable Telnet services, inbound, outbound, or all.<br><br>Inbound = Telnet to the switch from a remote device<br><br>Outbound = Telnet to other devices from the switch | <code>set telnet {enable   disable}<br/>[inbound   outbound   all]</code> |
| 2.   | Display Telnet status                                                                                                                                                              | <code>show telnet</code>                                                  |
| 3.   | Start a Telnet connection to another device                                                                                                                                        | <code>telnet host-ip [port]</code>                                        |

## SSH Overview

The Secure Shell (SSH) protocol provides secure Telnet between a client and the switch. By default, SSH is disabled on the switch.

The switch can support up to two concurrent SSH sessions.

## Configuring SSH

### Procedure 4-9 Configuring SSH

| Step | Task                                                           | Command(s)                                               |
|------|----------------------------------------------------------------|----------------------------------------------------------|
| 1.   | Enable, disable, or reinitialize the SSH server on the switch. | <code>set ssh {enabled   disabled   reinitialize}</code> |
| 2.   | Display SSH server status                                      | <code>show ssh status</code>                             |
| 3.   | Reinitialize new SSH authentication keys.                      | <code>set ssh hostkey reinitialize</code>                |

## MAC Address Settings

MAC address settings configuration provides for the ability to:

- Configure a timeout period for aging learned MAC addresses
- Limit specified layer two multicast addresses to specific ports within a VLAN
- Enable the ability to treat static unicast MAC addresses as a multicast address

## Age Time

Learned MAC addresses can be assigned an age in seconds after which they will be flushed from the FID. The default value is 300 seconds.

Use the `set mac agetime` command to configure the MAC age-time for MAC addresses.

The following example sets the age-time for MAC addresses on this device to 600 seconds:

```
C5(rw)->set mac agetime 600
C5(rw)->show mac agetime
```

Aging time: 600 seconds

## Limiting MAC Addresses to Specific VLANs

Use the **set mac multicast** command to define on what ports within a VLAN a multicast address can be dynamically learned on, or on what ports a frame with the specified MAC address can be flooded. Also, use this command to append ports to or clear ports from the egress ports list.

This example configures multicast MAC address 01-01-22-33-44-55 for VLAN 24, enabling this MAC address to be learned on or flooded out on this VLAN's ports, with the exception of ports ge.1.1 through ge.1.3.

```
C5(su)->set mac multicast 01-01-22-33-44-55 24 clear ge.1.1-3
```

## Setting the MAC Algorithm Mode

You can set the MAC algorithm mode, which determines the hash mechanism used by the device when performing Layer 2 lookups on received frames. Four modes are available:

- MAC CRC 16 lower bits algorithm
- MAC CRC 16 upper bits algorithm (default value)
- MAC CRC 32 lower bits algorithm
- MAC CRC 32 upper bits algorithm

Each algorithm is optimized for a different spread of MAC addresses. When changing this mode, the switch will display a warning message and prompt you to restart the device.

Use the **set mac algorithm** command to change the algorithm from the default, and the **clear mac algorithm** command to return to the default value. The **show mac algorithm** command displays the currently selected algorithm.

## New MAC Address Detection

You can configure the fixed switches to enable SNMP trap messaging globally or per port to send notifications when a new MAC address is first detected. The default is disabled globally and per port.

Use the **set newaddrtrap** command to enable SNMP trap messaging to report the detection of a new MAC address either globally on the device or on a specified port basis. The new MAC address trap feature is disabled by default. If a port is a CDP port, however, traps for new source MAC addresses will not be sent.

The following example enables trap notification globally, then configures SNMP trap messaging to send a notification when a new MAC address is detected on port ge.1.1:

```
C5(rw)->set newaddrtrap enable
C5(rw)->set newaddrtrap ge.1.1 enable
```

[Procedure 4-10](#) describes how to configure MAC address settings. All commands for this feature can be set in any command mode.

**Procedure 4-10 Configuring MAC Address Settings**

| Step | Task                                                                                                                                                                                                                                                                        | Command(s)                                                                                                              |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| 1.   | Display the MAC addresses in the switch's filtering database (FID).                                                                                                                                                                                                         | <code>show mac [address mac-address] [fid fid] [port port-string] [type {other   learned   self   mgmt   mcast}]</code> |
| 2.   | Display the current timeout period for aging learned MAC entries/                                                                                                                                                                                                           | <code>show mac agetime</code>                                                                                           |
| 3.   | Optionally, set the timeout period for aging learned MAC entries.                                                                                                                                                                                                           | <code>set mac agetime time</code>                                                                                       |
| 4.   | Optionally, define on what ports within a VLAN a multicast address can be dynamically learned on, or on what ports a frame with the specified MAC address can be flooded.<br><br>Optionally, use this command to append ports to or clear ports from the egress ports list. | <code>set mac multicast mac-address vlan-id [port-string] [{append   clear} port-string]</code>                         |
| 5.   | Optionally, change the MAC algorithm. Default is MAC CRC 16 upper bits.                                                                                                                                                                                                     | <code>set mac algorithm {mac-crc16-lowerbits   mac-crc16-upperbits   mac-crc32-lowerbits   mac-crc32-upperbits}</code>  |
| 6.   | Optionally, remove a multicast MAC address from the FID.                                                                                                                                                                                                                    | <code>clear mac address mac-address [vlan-id]</code>                                                                    |
| 7.   | Optionally, enable SNMP trap messaging to report the detection of new MAC addresses for the specified port or all ports.                                                                                                                                                    | <code>set newaddrtrap [port-string] {enable   disable}</code>                                                           |

## Configuring Node Aliases

The node alias feature enables administrators to determine the MAC address and location of a given end-station (or node) using the node's Layer 3 alias information (IP address) as a key. With this method, it is possible to determine that, for instance, IP address 123.145.2.23 is located on switch 5 port 3.

The passive accumulation of a network's node/alias information is accomplished by "snooping" on the contents of network traffic as it passes through the switch fabric.

Upon packet reception, node aliases are dynamically assigned to ports enabled with an alias agent, which is the default setting on fixed switches. Node aliases cannot be statically created, but can be deleted using the command **clear nodealias config**.

In the fixed switches, node data is automatically accumulated into the ct-alias mib. The NetSight Console Compass utility and Automated Security Manager (ASM) use the information in the node/alias MIB table.

It's important to make sure that inter-switch links are not learning node/alias information, as it would slow down searches by the NetSight Compass and ASM tools and give inaccurate results. Use the **set nodealias disable** command to disable the node alias agent on a port. The **set nodealias enable** command will re-enable the agent.

The maximum number of node alias entries is configured with the **set nodealias maxentries** command. The default is 32 entries per port.

Use the **clear nodealias config** command to return all values to the default for one or more ports.

The following command displays the nodealias configuration for port ge.1.1:

```
C5(su)->show nodealias config ge.1.1
```

| Port Number | Max Entries | Used Entries | Status |
|-------------|-------------|--------------|--------|
| -----       | -----       | -----        | -----  |
| ge.1.1      | 32          | 32           | Enable |

The following command disables the node alias agent on port ge.1.8:

```
C5(su)->set nodealias disable ge.1.8
```





## User Account and Password Management

This chapter describes user account and password management features, which allow enhanced control of password usage and provide additional reporting of usage.

Account and password feature behavior and defaults differ depending on the security mode of the switch. For information about security modes and profiles, see [Chapter 26, Configuring Security Features](#).

| For information about...                                                 | Refer to page... |
|--------------------------------------------------------------------------|------------------|
| <a href="#">User Account Overview</a>                                    | 5-1              |
| <a href="#">Password Management Overview</a>                             | 5-6              |
| <a href="#">Password Reset Button Functionality</a>                      | 5-9              |
| <a href="#">Management Authentication Notification MIB Functionality</a> | 5-9              |

### User Account Overview

Enterasys switches are shipped with three default user accounts:

- A super-user access account with a username of **admin** and no password
- A read-write access account with a username of **rw** and no password
- A read-only access account with a username of **ro** and no password

A user with super-user access has access to all the functionality on the switch while read-write and read-only accounts have less access to functionality. Command descriptions in the *CLI Reference* indicate the user access level required for each command.

Users with super-user access can create user accounts and passwords. Read-write and read-only accounts can change their own account passwords. User accounts are created, disabled, and enabled with the **set system login** command. Passwords are created and changed with the **set password** command. User accounts are deleted with the **clear system login** command.

The Enterasys Fixed Switch platforms support up to 16 user accounts. When creating a new or editing an existing login account, use the following syntax:

```
set system login username {super-user | read-write | read-only} {enable | disable}
 [allowed-interval HH:MM HH:MM]
 [allowed-days {[Sun] [Mon] [Tue] [Wed] [Thu] [Fri] [Sat]}]
 [local-only {yes|no}]
 [aging days]
 [simultaneous-logins logins]
```

The optional parameters shown indented above allow you to configure:

- The start and end hour and minute time period for which access will be allowed for this user based upon 24 hour time. (Not applicable for super user accounts.)
- The days of the week for which access will be allowed for this user. (Not applicable for super user accounts.)
- The authentication scope for this user — authentication is only by way of the local user database even with RADIUS or TACACS+ configured, or authentication is by way of configured methods, which is the default value.
- The number of days to age the password. A non-zero value supercedes the aging configured in **set system password**, for this user.
- The number of simultaneous logins allowed from the user. The switch is capable of verifying that a specified user is only connected to the product a configurable number of times. Any attempt for a specified user to exceed the configured limit results in a trap.

For example, if simultaneous logins is set to 1, a specific user would not be able to Telnet to the switch, and then simultaneously try to SSH to the switch or access local management via the console port.

Use the **clear system login** command to remove a local user account or to reset any configured parameters to their default values. If none of the optional parameters shown indented below are entered, the user account is deleted.

```
clear system login username
 [allowed-interval]
 [allowed-days]
 [local-only]
 [aging]
 [simultaneous-logins]
```

User account access to features is affected by the security mode of the switch. Differences in access on a command basis are described in the *CLI Reference* for your platform.

For information about security modes and profiles, see [Chapter 26, Configuring Security Features](#). See [Table 5-1](#) on page 5-7 for a list of account and password defaults by security mode.

See “[User Account Configuration](#)” on page 5-3 for procedures and examples for creating user accounts.

## Emergency Access User Account

The fixed switches support the ability to identify an emergency access user with the **set system lockout emergency-access <username>** command. An emergency access user account is allowed emergency access to the switch through the console port.

Before identifying an emergency access user with the **set system lockout** command, the user account must be configured with super-user access rights with the **set system login** and **set password** commands.

- A user account cannot be deleted while it is the emergency access account.
- Only one EA user is supported at a time and one shall always exist. The default **admin** user is the default EA user.
- EA status can only be removed by replacing it with another account.
- EA user access not made through the console port will be subject to normal password handling.
- When the password reset button is enabled, it will restore the default **admin** account as the EA user.

- The emergency access user is still subject to the system lockout interval even on the console port.

## Account Lockout

User accounts can be locked out based on the number of failed login attempts or a period of inactivity. Lockout is configured at the system level, not at the user account level. Use the **set system lockout** command to:

- Set the number of failed login attempts allowed before disabling a read-write or read-only user account or locking out a super-user account.
  - When a read-only or read-write user makes the configured number of failed attempts, that user is disabled, and cannot log back in until re-enabled by a super-user with the **set system login** command.
  - When a super-user makes the configured number of failed attempts, that user is locked out for the configured lockout period. The configurable lockout period for super-user accounts is 0 to 65535 minutes.

Note that only super-user accounts are temporarily locked out for a configured period. Read-only and read-write accounts are disabled and must be enabled by a super-user.

- Configure lockout based on a period of inactivity. Valid values for the period of inactivity are 0 to 65535 days. A value of 0 indicates no inactivity checking.
  - When a read-only or read-write user session is inactive for the configured period of time, that user is disabled, and cannot log back in until re-enabled by a super-user with the **set system login** command.
  - Super-user accounts are not affected by inactivity checking.

## Port Lockout

The account lockout functionality also supports a “port lockout” mechanism (**set system lockout port {enable | disable}**). When enabled, the system monitors the results of all login attempts, including via RADIUS, SSH, or Telnet, and on the console port. Separate counts are maintained for each interface — local and network/remote (SSH, Telnet, or WebView).

When the number of sequential failed attempts equals the maximum configured attempts for any user, the lockout will be applied (as configured) to all login attempts made through the given interface (SSH, Telnet, or the console port). Any successful login will restart the count. By default, port lockout is disabled.

If the default **admin** super user account has been locked out, and if the password reset button functionality is enabled, you can press the reset button on the switch to re-enable the **admin** account with its default values. The emergency-access user is restored as the default, the **admin** account.

If the password reset button functionality has been disabled, you can wait until the lock out time has expired or you can reboot the switch in order to re-enable the **admin** account.

See “[Password Reset Button Functionality](#)” on page 5-9 for more information about password reset button functionality.

## User Account Configuration

[Procedure 5-1](#) on page 5-4 shows how a super-user creates a new read-write or read-only user account and sets the password for the account. All other optional parameters are not shown.

[Procedure 5-2](#) on page 5-4 shows how a super-user creates a new super-user account and assigns it as the emergency access account.

Refer to the *CLI Reference* for your platform for details about the commands listed below.

### Procedure 5-1 Creating a New Read-Write or Read-Only User Account

| Step | Task                                                                                                           | Command(s)                                                                                     |
|------|----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| 1.   | Create a new read-write or read-only user login account and enable it.<br>(All other parameters are optional.) | <code>set system login username {read-write read-only} enable</code>                           |
| 2.   | Set the password for the new account.<br>Respond appropriately to the system prompts.                          | <code>set password username</code>                                                             |
| 3.   | Display the new user account.                                                                                  | <code>show system login</code>                                                                 |
| 4.   | Remove a local login user account<br>or<br>Disable an existing account                                         | <code>clear system login username</code><br><br><code>set system login username disable</code> |

This example enables a new user account named “guest” with read-only privileges and allows access only between 8:00 am and 5:00 pm on Mondays through Wednesdays. The password for this account is then set, and the configured login accounts are displayed.

```
C5(su)->set system login guest read-only enable allowed-interval 08:00 17:00
allowed-days Mon Tue Wed
C5(su)->set password guest
Please enter new password: *****
Please re-enter new password: *****
Password changed.
C5(su)->show system login
Username Access State Aging Simul Local Login Access Allowed
 Access State Aging Login Only? Start End Days

admin super-user enabled 0 0 no ***access always allowed***
ro read-only enabled 0 0 no ***access always allowed***
rw read-write enabled 0 0 no ***access always allowed***
guest read-only enabled 0 0 no 08:00 17:00 mon tue wed
```

[Procedure 5-2](#) creates a new super-user account and assigns it as the emergency access user account. In addition, the default super-user account, admin, is disabled as a security measure.



**Note:** You can delete the default admin account, but deletion of the last remaining super-user account is prevented (that is, a super-user account must be created before the admin account can be deleted).

If the security mode is C2, the last remaining super-user account must also be set as the emergency access user in order to allow the default admin account to be deleted.

### Procedure 5-2 Configuring a New Super-User / Emergency Access User Account

| Step | Task                                                                                         | Command(s)                                               |
|------|----------------------------------------------------------------------------------------------|----------------------------------------------------------|
| 1.   | Create a new super-user login account and enable it.<br>(All other parameters are optional.) | <code>set system login username super-user enable</code> |
| 2.   | Set the password for this account.                                                           | <code>set password username</code>                       |
| 3.   | Display the login user accounts                                                              | <code>show system login</code>                           |

**Procedure 5-2 Configuring a New Super-User / Emergency Access User Account**

| Step | Task                                                               | Command(s)                                          |
|------|--------------------------------------------------------------------|-----------------------------------------------------|
| 4.   | Assign the new super-user account as the emergency access account. | <b>set system lockout emergency-access username</b> |
| 5.   | Display the system lockout settings                                | <b>show system lockout</b>                          |
| 6.   | Disable the default super-user account, admin                      | <b>set system login admin super-user disable</b>    |

This example creates a new super-user account named “usersu” and enables it. The password for this account is set and the configured login accounts are displayed. The new account is assigned as the emergency access account and the system lockout settings are displayed. Then, the default super-user account named “admin” is disabled.

```
C5(su)->set system login usersu super-user enable
C5(su)->set password usersu
Please enter new password: *****
Please re-enter new password: *****
Password changed.
C5(su)->show system login
```

| Username | Access     | State   | Aging | Simul<br>Login | Local<br>Only? | Login<br>Start | Access<br>End | Allowed<br>Days                |
|----------|------------|---------|-------|----------------|----------------|----------------|---------------|--------------------------------|
| admin    | super-user | enabled | 0     | 0              | no             | ***access      | always        | allowed***                     |
| ro       | read-only  | enabled | 0     | 0              | no             | ***access      | always        | allowed***                     |
| rw       | read-write | enabled | 0     | 0              | no             | ***access      | always        | allowed***                     |
| usersu   | super-user | enabled | 0     | 0              | no             | 00:00          | 24:00         | sun mon tue wed<br>thu fri sat |
| guest    | read-only  | enabled | 0     | 0              | no             | 00:00          | 24:00         | mon tue wed                    |

```
C5(su)->set system lockout emergency-access usersu
C5(su)->show system lockout
Unsuccessful login attempts before lockout : 3
Duration of lockout : 15 minutes.
Period of inactivity before account lockout : 0 days
Lockout entire port upon failed logins : disabled
Ports currently locked out due to failed logins : none
Account assigned emergency-access from the console: usersu

C5(su)->set system login admin super-user disable
C5(su)->show system login
```

| Username | Access     | State    | Aging | Simul<br>Login | Local<br>Only? | Login<br>Start | Access<br>End | Allowed<br>Days                |
|----------|------------|----------|-------|----------------|----------------|----------------|---------------|--------------------------------|
| admin    | super-user | disabled | 0     | 0              | no             | ***access      | always        | allowed***                     |
| ro       | read-only  | enabled  | 0     | 0              | no             | ***access      | always        | allowed***                     |
| rw       | read-write | enabled  | 0     | 0              | no             | ***access      | always        | allowed***                     |
| usersu   | super-user | enabled  | 0     | 0              | no             | 00:00          | 24:00         | sun mon tue wed<br>thu fri sat |

guest read-only enabled 0 0 no 00:00 24:00 mon tue wed

## Password Management Overview

Individual user account passwords are configured with the **set password** command. Configured passwords are transmitted and stored in a one-way encrypted form, using a FIPS 140-2 compliant algorithm.

When passwords are entered on the switch using the CLI, the switch automatically suppresses the clear text representation of the password. In addition, the switch ensures that passwords are not available in clear text to any user, including administrators.

The switch ensures that the password does not contain, repeat, or reverse the associated username.

All password changes are logged by the switch.

## System Level Password Settings

At the system level, you can configure password requirements with the **set system password** command. Among other characteristics, the **set system password** command allows you to configure password length, repetition, character usage, password sharing, and aging.

The following list describes in detail the system level password requirements that can be configured:

- Whether the switch maintains and verifies a password history (from 0 to 10) per account (**set system password history**). The previously used passwords for a user account stored in the password history are checked for duplication when a new password is configured for that account with the **set password** command.
- Whether the switch enforces a minimum period of waiting before an existing password can be updated (**set system password change-frequency**). An exception to this requirement is the first time update, which if configured, requires a new user logging in for the first time to change their password (**set system password change-first-login**).
  - A password change-frequency interval of zero means there is no restriction on the frequency of password changes.
  - A configured minimum change-frequency interval applies only to users without super-user privileges attempting to change their own passwords. Users with super-user privileges may change their passwords at any time.
- Whether the switch allows multiple accounts to share the same password. (**set system password allow-duplicates**.)
- Whether the switch enforces a minimum number of characters required for passwords (**set system password length**).
- Whether the switch allows the same character to appear consecutively in the same password (**set system password allow-repeatingchars**).
- Whether the switch enforces a configurable minimum number of characters of a specific type that must be present in a user account password (**set system password min-requiredchars**). The following types are supported:
  - Upper case characters (default 0)
  - Lower case characters (default 0)
  - Numeric characters (default 0)

- Special characters (default 0)

The set of special characters recognized is: ! @ # \$ % ^ & \* ( ) ? = [ ] \ ; , . / ` .

- Whether the switch enforces aging of system passwords.
  - The switch can enforce a system-wide default for password aging (**set system password aging**).
  - The switch can enforce a password aging interval on a per-user basis (**set system login aging**).
  - The switch can notify users at login that their password will expire in a given number of days (**set system password warning-period**).
  - The switch can notify a user upon password expiration, but allow a specified additional number of subsequent logins (1 to 3) within a specified time period (1 to 30 days) before requiring a new password (**set system password grace-period** and **grace-limit**).
- Whether the switch requires that a password be specified at the time of user account creation (**set system password require-at-creation**).
  - If the option is enabled, the **set system login** command will interactively prompt for a password upon creation of a new user account.
 

It will be as if a **set password username** command was implicitly executed. The new account will not be successfully created until a valid password has been specified.
- Whether the switch performs substring matching to prevent any substring present in previous account passwords from being used in a new password (**set system password substring-match-len**).
  - Requires a non-zero password history length.
  - 0 to 40 characters are supported.
  - If a **substring-match-len option** is set to zero, no substring matching will be performed when validating new passwords.
 

If the **substring-match-len** option is configured with a nonzero length, any substring of the specified length appearing in the current password for this user may not appear in a new password.

If the configured history size is nonzero, then all historical passwords up to that size will also be compared with the input of the new password. Any substring of the configured length appearing in any of the historical passwords may not be used in the new password.

Password feature behavior and defaults differ depending on the security mode of the switch. For information about security modes and profiles, see [Chapter 26, Configuring Security Features](#). See [Table 5-1](#) on page 5-7 for a list of account and password defaults by security mode.

[Procedure 5-3](#) on page 5-8 describes the commands used to configure system password settings.

## Defaults

The default values for user account and password parameters are listed in the following table by the security mode of the switch.

**Table 5-1 User Account and Password Parameter Defaults by Security Mode**

| Parameter                 | Normal Mode Default | C2 Mode Default         |
|---------------------------|---------------------|-------------------------|
| Password history          | 0 (no history)      | 8 previous passwords    |
| Password change frequency | 0 (no waiting)      | 1440 minutes (24 hours) |

**Table 5-1 User Account and Password Parameter Defaults by Security Mode (continued)**

| Parameter                                              | Normal Mode Default      | C2 Mode Default       |
|--------------------------------------------------------|--------------------------|-----------------------|
| Minimum number of characters in password               | 8                        | 9                     |
| Allow consecutively repeating characters in password   | yes                      | 2 characters          |
| Aging of system passwords                              | disabled                 | 90 days               |
| Password required at time of new user account creation | no                       | yes                   |
| Substring matching at password validation              | 0 (no checking)          | 0 (no checking)       |
| New users required to change password at first log in  | no                       | yes                   |
| Lockout based on inactivity                            | 0 (no activity checking) | 90 days of inactivity |
| Lockout based on failed login attempts                 | 3 failed attempts        | 3 failed attempts     |
| Lockout period duration after unsuccessful logins      | 15 minutes               | 1 minute              |
| Grace period after password expiration                 | 0                        | 30 days               |
| Grace login limit                                      | 0                        | 3                     |
| Warning period                                         | 20 days                  | 20 days               |

## System Password Settings Configuration

Refer to the *CLI Reference* for your platform for detailed information about the commands listed below in [Procedure 5-3](#).

### Procedure 5-3 Configuring System Password Settings

| Step | Task                                                                                                                        | Command(s)                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Configure system level password settings.<br>All parameters are optional but at least one must be entered with the command. | <pre> set system password [aging {days   disable}] [allow-duplicates {yes   no}] [allow-repeating-chars {num   yes}] [change-first-login {yes   no}] [change-frequency minutes] [grace-limit {logins}] [grace-period {days}] [history {size}] [length {#ofChars}] [min-required-chars   {[uppercase #ofChars]   [lowercase #ofChars]   [numeric #ofChars]   [special #ofChars]}] [require-at-creation {yes   no}] [substring-match-len #ofChars] [warning-period {days}] </pre> |



**Procedure 5-3 Configuring System Password Settings (continued)**

| Step | Task                                       | Command(s)                                                                                                                                                                                                                                                                                                                   |
|------|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.   | Display the current password settings.     | <code>show system password</code>                                                                                                                                                                                                                                                                                            |
| 3.   | Reset password settings to default values. | <pre>clear system password [aging] [allow-duplicates] [allow-repeating-chars] [change-first-login] [change-frequency] [grace-limit] [grace-period] [history] [length] [min-required-chars   { [uppercase]     [lowercase]     [numeric]     [special] } ] [require-at-creation] [substring-match-len] [warning-period]</pre> |

## Password Reset Button Functionality

When the password reset button functionality is enabled with the `set system password-resetbutton enable` command, pressing the password reset button causes the **admin** account, with its default values, to be restored on the switch.

- If the **admin** account has been disabled, it will be re-enabled.
- If the **admin** account has been deleted, it will be restored on the switch with default values.

When the password reset button functionality is disabled by means of the `set system password-resetbutton disable` command, pressing the reset button will have no effect. The password reset button is enabled by default.

## Management Authentication Notification MIB Functionality

Management authentication notification MIB functionality includes enabling/disabling the sending of SNMP notifications when a user login authentication event occurs for various authentication notification types.

SNMP must be correctly configured in order to send these notifications. Refer to [Chapter 12, Configuring SNMP](#), for more information about SNMP.

Use the `set mgmt-auth-notify` command to enable or disable notifications for the authentication notification types specified in the Enterasys Management Authentication Notification MIB.

You can specifically enable or disable a single authentication notification type, multiple authentication notification types or all the authentication notification types. The default setting is that all Management Authentication Notification types are **enabled** for authentication notifications.

When enabled for console, SSH, Telnet, or Webview, the switch will send an SNMP notification for every successful and failed login attempt.

Use the `clear mgmt-auth-notify` to return all current settings to the default state of enabled.

Refer to the CLI Reference for your platform for detailed information about the commands listed below in [Procedure 5-4](#).

#### Procedure 5-4 Configuring Management Authentication Notification MIB Settings

| Step | Task                                                                               | Command(s)                                                                                                                                            |
|------|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Display the current settings for the Management Authentication Notification MIB.   | <code>show mgmt-auth-notify</code>                                                                                                                    |
| 2.   | Enable or disable notifications for one or more authentication notification types. | <code>set mgmt-auth-notify<br/>{enable   disable}<br/>[console] [ssh] [telnet] [webview]<br/>[inactiveUser] [maxUserAttempt]<br/>[maxUserFail]</code> |
| 3.   | Return all settings to the default of enabled                                      | <code>clear mgmt-auth-notify</code>                                                                                                                   |

The following example displays the current MIB settings, then disables notifications for inactive users and WebView connections.

```
C5(su)->show mgmt-auth-notify
```

```
Management Type Status

console Enabled
ssh Enabled
telnet Enabled
webview Enabled
inactiveUser Enabled
maxUserAttempt Enabled
maxUserFail Enabled
```

```
C5(su)->set mgmt-auth-notify disable web inactiveUser
```

## Firmware Image and File Management

This chapter describes how to download and install a firmware image file and how to save and display the system configuration as well as manage files on the switch.

| For information about...                                | Refer to page... |
|---------------------------------------------------------|------------------|
| <a href="#">Managing the Firmware Image</a>             | 6-1              |
| <a href="#">Managing Switch Configuration and Files</a> | 6-4              |

### Managing the Firmware Image

This section describes how to download a firmware image, set the firmware to be used at system startup, revert to a previous image, and set TFTP parameters.

#### Downloading a Firmware Image

You can upgrade the operational firmware in the stackable or standalone switch without physically opening the switch or being in the same location. There are two ways to download firmware to the switch:

- Via TFTP or SFTP download. This procedure uses a TFTP or SFTP server connected to the network and downloads the firmware using the TFTP or SFTP protocol. For details on how to perform a TFTP or SFTP download using the **copy** command, refer to “[Downloading from a TFTP or SFTP Server](#)” on page 6-2. For information on setting TFTP timeout and retry parameters, refer to “[Setting TFTP Parameters](#)” on page 6-4.
- Via the serial (console) port. This procedure is an out-of-band operation that copies the firmware through the serial port to the switch using an XMODEM transfer. It should be used in cases when you cannot connect to the switch to perform the in-band **copy** download procedure via TFTP. Serial console download has been successfully tested with the following applications which support XMODEM transfer:

- HyperTerminal
- Tera Term Pro

Any other terminal applications may work but are not explicitly supported.

Refer to “[Downloading Firmware via the Serial Port](#)” on page 1-10 for instructions.

The stackable and standalone fixed switches allow you to download and store dual images. The backup image can be downloaded and selected as the startup image by using the commands described in this section.

## Downloading from a TFTP or SFTP Server

This procedure assumes that the switch or stack of switches has been assigned an IP address and that it is connected to the network. It also assumes that the network has a TFTP or SFTP server to which you have access. If these assumptions are not true, please refer to [Chapter 1, Setting Up a Switch for the First Time](#) for more information.

To perform a TFTP or SFTP download:

1. Download to your computer the latest firmware for the switch from the Enterasys web site. Unzip/uncompress the firmware, and copy the firmware to the upload/download directory configured for your TFTP server. The firmware is available at this Enterasys location:  
<https://extranet.enterasys.com/downloads>
2. Review the Release Notes for the downloaded firmware to check for any upgrade notices or limitations that may apply to your switch.
3. Using Telnet or SSH, establish a CLI session on the switch and log in.
4. From the CLI session, use the **copy** command to download the new image file from the TFTP or SFTP server to the switch. For example:

```
copy tftp://<TFTP-server-IPaddr>/<path-to-firmware-file> system:image
```

If you receive the error message "Error: No space left on the device. Please remove backup file.", refer to "[Deleting a Backup Image File](#)" on page 1-5 before proceeding.

5. After the copy is complete, use the **dir** command to confirm that the new image file has been copied. The following example shows that the firmware image "a4-series\_06.61.03.0007" was copied to the switch but that firmware image "a4-series\_06.61.00.0026" is still the active and boot image.

```
A4(su)->dir
```

```
Images:
```

```
=====
```

```
Filename: a4-series_06.61.00.0026 (Active)(Boot)
Version: 06.61.00.0026
Size: 9405440 (bytes)
Date: Fri Dec 16 12:48:35 2011
Checksum: f1626ccf10d8f48cd6c3e79ab602342a
Compatibility: <platform specific>
```

```
Filename: a4-series_06.61.03.0007
Version: 06.61.03.0007
Size: 8290304 (bytes)
Date: Fri Jan 27 11:35:27 2012
Checksum: 9f820d79239f10890442f8ff1f2bc914
Compatibility: <platform specific>
```

6. To set the new image to the boot image, refer to "[Setting the Boot Firmware](#)" on page 6-3 below.

## Setting the Boot Firmware

Use the **show boot system** command to display the image file currently configured to be loaded at startup. For example:

```
A4(su)->show boot system
Current system image to boot: a4-series_06.61.00.0026
```

Use the **set boot system** command to set the firmware image to be loaded at startup. You can choose to reset the system to use the new firmware image immediately, or you can choose to only specify the new image to be loaded the next time the switch is rebooted. For example:

```
A4(su)->set boot system a4-series_06.61.03.0007
This command can optionally reset the system to boot the new image.
Do you want to reset now (y/n) [n]
```

If you respond **y** (yes), the system will reboot immediately using the new image, and the new image will be the active image. If you respond **n** (no), the new image will be set as the Boot image but the currently Active image will remain active.

You can use the **dir** command to display the “Active” image and the “Boot” image, which will be the image loaded at the next system reboot.



**Note:** If you are changing the firmware image to a version *earlier* than the current version, refer to [“Reverting to a Previous Image”](#) on page 6-3 for the correct steps to follow.

## Reverting to a Previous Image

In the event that you need to downgrade to a previous version of code, you can do so by completing the steps described below.



**Caution:** Before reverting to a previous image, always back up your configuration by saving it to a file with the **show config outfile** command. You can then copy the file to a remote location with the **copy** command. Refer to [“Creating a Backup Configuration File”](#) on page 6-6 for more information.

1. Save your running configuration with the **save config** command.
2. Make a copy of the current configuration with the **show config outfile configs/filename** command. Use the **dir** command to confirm that the file was created.
3. If desired, copy the file to a remote TFTP server with the **copy** command:

```
copy configs/<filename> tftp://server_ipaddr/<filename>
```

4. If necessary, load the previous version of code on the device, as described in [“Downloading a Firmware Image”](#) (page 6-1).
5. Set this older version of code to be the boot code with the **set boot system** command. When the system asks if you want to reset the device, specify no (**n**).
6. Reload the saved configuration onto the device with the **configure** command. Do not use the **append** parameter. You will be prompted to respond whether you want to reset the system. Enter y (yes).

```
configure configs/<filename>
This command will reset the system and clear current configuration.
Are you sure you want to continue (y/n) [n]? y
```

7. After the system resets, establish a new CLI session with the switch and log in.



**Caution:** If you do not follow the steps above, you may lose remote connectivity to the switch.

## Setting TFTP Parameters

You can configure some of the settings used by the switch during data transfers using TFTP.

Use the **show tftp settings** command to display current settings.

```
A4(ro)->show tftp settings
TFTP packet timeout (seconds): 2
TFTP max retry: 5
```

Use the **set tftp timeout** command to configure how long TFTP will wait for a reply of either an acknowledgement packet or a data packet during a data transfer. The default value is 2 seconds.

Use the **set tftp retry** command to configure how many times TFTP will resend a packet, either an acknowledgement packet or a data packet. The default value is 5 retries.

Use the **clear tftp timeout** and **clear tftp retry** commands to reset configured values back to their defaults.

# Managing Switch Configuration and Files

## Configuration Persistence Mode

The default state of configuration persistence mode is “auto,” which means that when CLI configuration commands are entered, or when a configuration file stored on the switch is executed, the configuration is saved to NVRAM automatically at the following intervals:

- On a standalone unit, the configuration is checked every two minutes and saved if there has been a change.
- On a stack, the configuration is saved across the stack every 5 minutes if there has been a change.

If you want to save a running configuration to NVRAM more often than the automatic intervals, execute the **save config** command and wait for the system prompt to return. After the prompt returns, the configuration will be persistent.

Use the **show snmp persistmode** command to display the current persistence mode. You can change the persistence mode from “auto” to “manual” with the **set snmp persistmode** command. If the persistence mode is set to “manual,” configuration commands will not be automatically written to NVRAM. Although the configuration commands will actively modify the running configuration, they will not persist across a reset unless the **save config** command has been executed.



**Note:** When your device is configured for manual SNMP persistence mode, and you attempt to change the boot system image, the device will not prompt you to save changes or warn you that changes will be lost.



**Note:** If a memory card is installed on an I-Series switch, “auto” persistence mode is **not** supported. Refer to [Using an I-Series Memory Card](#) below for more information.

## Using an I-Series Memory Card

The I3H-4FX-MEM and I3H-6TX-MEM IOMs provide a memory card slot where a small, separately-purchased memory card (I3H-MEM) may be inserted. The memory card provides a removable, non-volatile means for storing the system configuration and IP address only, and may be used to move the system's configuration to another switch.



**Note:** Only one IOM containing a memory card slot may be installed in an I-Series switch.

The memory card is hot-swappable. If a card is already installed in the switch, when the memory slot cover plate is removed, power is automatically removed from the slot. Once power has been removed from the slot, power will not be returned until the switch is rebooted with a memory card in the slot.

Refer to your *I-Series Installation Guide* for information about inserting and removing memory cards.

### Memory Card Operation

When an I-Series switch is initialized (booted up), the configuration stored on an installed memory card will overwrite the configuration saved in NVRAM. If no configuration is contained on an installed memory card, the activity LED will flash briefly and the boot up will continue without overwriting the configuration in NVRAM.

If a memory card is inserted into a running system (hot swapped), the configuration stored on the memory card will not be applied until the system is rebooted.

When a memory card is installed:

- The **save config** command must be used to save the current configuration to both NVRAM and to the memory card, since “auto” persistence mode is not supported when a card is present.
- The **clear config** command will simultaneously delete the current configuration from both NVRAM and the memory card.
- The **show config** command can display the configuration on the memory card or on NVRAM.

Note that only the system configuration can be stored on the memory card—no files can be stored on the card. The **copy** command should be used to upload files to the switch.



**Note:** The I-Series memory card is not interchangeable with a standard Compact Flash card. A standard Compact Flash card will not work in the I-Series switch, and the I-Series memory card cannot be used in place of a Compact Flash card in other systems.

## Displaying and Saving the Configuration and Creating a Backup

Use the **save config** command to save the running configuration. On a stacked system, this command will save the configuration to all switch members in a stack.

Use the **show config** command to

- Display the system configuration
- Write the configuration to a file

## Displaying the Configuration

Executing **show config** without any parameters will display all the non-default configuration settings. Using the **all** parameter will display all default and non-default configuration settings.

To display non-default information about a particular section of the configuration, such as port or system configuration, use the name of the section (or facility) with the command. For example, to show the configuration of the “system” facility:

```
C5(su)->show config system
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.

begin
!
#***** NON-DEFAULT CONFIGURATION *****
!
!
Firmware Revision: 06.61.01.0032
!

#system
set system name "LAB C5"
set system location "Second Floor South"
set system contact "John Smith"
!
!
end
```

On the I-Series, you can display the configuration information on a memory card with the **show config memcard** command. If a memory card is not installed, a message indicating that the memory card could not be accessed is displayed.

## Creating a Backup Configuration File

You can create a copy of the system configuration using the **show config outfile** command. This configuration file can then be copied to a remote location to be used as a backup configuration file if needed.



### Notes:

When saving a configuration to a file, save only the non-default values — that is, do not use the **all** parameter with **show config outfile**. Including default values is unnecessary and will make the configuration file very large.

You can write only a section of a system configuration to a file by using the *facility* parameter with **show config outfile**.

This example:

- Saves the currently running configuration,
- Saves the configuration to a file named “myconfig” in the “configs” directory on the switch,
- Verifies the location of the file with the **dir** command,
- Then copies that file to a remote TFTP server on the network.

```
B5(su)->save config
B5(su)->show config outfile configs/myconfig
B5(su)->dir
```



```

Images:
=====
Filename: b5-series_06.42.03.0001
Version: 06.42.03.0001
Size: 6856704 (bytes)
Date: Tue Dec 14 14:12:21 2010
Checksum: 043637a2fb61d8303273e16050308927
Compatibility: B5G124-24, B5G124-24P2, B5G124-48, B5G124-48P2, B5K125-24
 B5K125-24P2, B5K125-48, B5K125-48P2

Filename: b5-series_06.61.01.0032 (Active) (Boot)
Version: 06.61.01.0032
Size: 7314432 (bytes)
Date: Fri Jan 6 11:20:00 2012
Checksum: c0ae0ef322317f79309bc64e4c3beca4
Compatibility: B5G124-24, B5G124-24P2, B5G124-48, B5G124-48P2, B5K125-24
 B5K125-24P2, B5K125-48, B5K125-48P2

Files: Size
=====
configs:
myconfig 4237
logs:
current.log 512017
secure:
secure/logs:

```

```
B5(su)->copy configs/myconfig tftp://192.168.10.1/myconfig
```

To use a backup configuration file, refer to [“Reverting to a Previous Image”](#) on page 6-3 and [“Applying a Saved Configuration”](#) on page 6-7 below.

## Applying a Saved Configuration

Use the **configure** command to execute a configuration file stored on the switch. You can **append** the file to the current configuration, to make incremental adjustments to the current configuration, or you can replace the current configuration with the contents of the file. When you replace the current configuration, an automatic reset of the system is required.

This example appends the file “myconfig” located in the configs directory to the current running configuration:

```
B5(su)->configure configs/myconfig append
```

This example replaces the current configuration with the contents of the “myconfig” file. After the system resets, you will have to establish another CLI session and log in to the system again.

```
B5(su)->configure configs/myconfig
```

```
This command will reset the system and clear current configuration.
```

```
Are you sure you want to continue (y/n) [n]? y
```

## Managing Files

Table 6-1 lists the tasks and commands used to manage files.

**Table 6-1 File Management Commands**

| Task                                                                                                   | Command                                                                |
|--------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| List all the files stored on the system, or only a specific file.                                      | <b>dir</b> <i>[filename]</i>                                           |
| Display the system configuration.<br>On I-Series only, display contents of memory card.                | <b>show config</b> [ <b>all</b>   <i>facility</i>   <b>memcard</b> ]   |
| Display the contents of a file located in the configs or logs directory.                               | <b>show file</b> <i>directory/filename</i>                             |
| Delete a file. Can be used to delete image files as well as files in the configs and logs directories. | <b>delete</b> <i>directory/filename</i>                                |
| Copy the configuration or sections of the configuration to a file.                                     | <b>show config</b> [ <i>facility</i> ] <b>outfile configs/filename</b> |

## Configuring System Power and PoE

This chapter describes how to configure Redundant Power Supply mode on the C5 and G-Series switches, and how to configure Power over Ethernet (PoE) on platforms that support PoE.

The information about Power over Ethernet (PoE) applies only to fixed switching platforms that provide PoE support. PoE is not supported on the I-Series switches.

| For information about...                             | Refer to page... |
|------------------------------------------------------|------------------|
| <a href="#">Configuring Redundant Power Supplies</a> | 7-1              |
| <a href="#">Power over Ethernet Overview</a>         | 7-1              |
| <a href="#">Configuring PoE</a>                      | 7-4              |

### Configuring Redundant Power Supplies



**Note:** This feature is supported by the C5 and G-Series switches only

When a C5 or G-Series switch is connected to a redundant power supply, two modes of power supply operation are supported:

- **Redundant** mode, in which the power made available to the system is equal to the maximum output of the lowest rated supply. (This is the default mode.) When two supplies are installed in redundant mode, system power redundancy is guaranteed if one supply is lost.
- **Non-redundant**, or additive, mode, in which the combined output of both supplies is made available to the system. In this mode, the loss of a single supply may result in a system reset.

Power supply redundancy mode can be configured with the **set system power** command.

On G-Series switches, power supply LEDs visible on the front panel of the switch indicate whether the power supplies are present and, if two are present, whether they are in redundant or additive (non-redundant) mode. Refer to your *G-Series Hardware Installation Guide* for more information.

### Power over Ethernet Overview

PoE, defined in IEEE standards 802.3af and 802.3at, refers to the ability to provide 48 Vdc (for 802.3af) or 54 Vdc (for 802.3at) operational power through an Ethernet cable from a switch or other device that can provide a PoE-compliant port connection to a powered device (PD).

Examples of PDs are the following:

- Voice over IP devices such as PoE-compliant digital telephones

- Pan/Tilt/Zoom (PTZ) IP surveillance cameras
- Devices that support Wireless Application Protocol (WAP) such as wireless access points

Ethernet implementations employ differential signals over twisted pair cables. This requires a minimum of two twisted pairs for a single physical link. Both ends of the cable are isolated with transformers blocking any DC or common mode voltage on the signal pair. PoE exploits this fact by using two twisted pairs as the two conductors to supply a direct current to a PD. One pair carries the power supply current and the other pair provides a path for the return current.

Using PoE allows you to operate PDs in locations without local power (that is, without AC outlets). Having such a network setup can reduce the costs associated with installing electrical wiring and AC outlets to power the various devices.

## Implementing PoE

You can configure PoE on your PoE-compliant Enterasys device through the CLI-based procedures presented in the section “[Configuring PoE](#)” on page 7-4. As part of your plan to implement PoE in your network, you should ensure the following:

- The power requirements of your PDs are within the limits of the PoE standards.
- Your PoE-compliant Enterasys device can supply enough power to run your PDs. See [Table 7-1](#) for power ranges based on each device class.

**Table 7-1 PoE Powered Device Classes**

| Class | Power Output at Port                     | Power Range Used by Device                                  |
|-------|------------------------------------------|-------------------------------------------------------------|
| 0     | 15.4 watts                               | 0.44 to 12.95 watts                                         |
| 1     | 4.0 watts                                | 0.44 to 3.84 watts                                          |
| 2     | 7.0 watts                                | 3.84 to 6.49 watts                                          |
| 3     | 15.4 watts                               | 6.49 to 12.95 watts                                         |
| 4     | 34 watts (802.3at)<br>Reserved (802.3af) | 12.95 to 25.5 watts (802.3at)<br>Treat as class 0 (802.3af) |

If SNMP traps are enabled, the Enterasys device generates a trap to notify the network administrator if any of the following occur:

- If the power needed or requested exceeds the power available
- If a power state occurs on a PD (for example, when a PD is powered up or unplugged)

If insufficient power is available for an attached PD, the corresponding port LED on the Enterasys device turns amber. The LED also turns amber if a PoE fault occurs (for example, a short in the Ethernet cable).

## Allocation of PoE Power to Modules



**Note:** This feature is available only on the G-Series.

The switch firmware determines the power available for PoE based on hardware configuration, power supply status, and power supply redundancy mode. The system calculates and reserves the correct amount of power required by the installed hardware components and then makes the

balance of power available for PoE. When any change is made to the hardware configuration, power supply status, or redundancy mode, the firmware recalculates the power available for PoE.

On the S-Series, N-Series, and K-Series switches, you can also manually configure the maximum percentage of PoE power available to the chassis as a percentage of the total installed PoE power with the **set inlinepower available** command. (This feature is not configurable on the G-Series.) If the power needed or requested exceeds the power available, the system will generate a trap to notify the system manager, if traps are enabled.

The power available for PoE is distributed based on the configured allocation mode, set with the **set inlinepower mode** command:

- **Automatic** mode, in which available power is distributed evenly to PoE-capable modules based on PoE port count. (This is the default mode.) Any change in available power, due to a change in power supply status or redundancy mode or to the addition or removal of modules, will trigger an automatic redistribution of power.
- **Manual** mode, in which the power budget for each PoE-capable module is manually configured, using either CLI commands or the MIBs. The sum of the wattage configured for each module cannot exceed the total power available on the switch for PoE.

The power budget for each PoE-capable module can be configured manually on the G-Series with the command **set inlinepower assign**.

The configured wattage assignments are used to calculate each slot's percentage of total available power. If the total available PoE power is reduced, a redistribution of available power will occur, applying the calculated percentages.

## When Manual Mode is Configured

When manual distribution mode is configured, if a PoE module is added to the switch, the PoE power budget for existing modules will **not** be recalculated. The new module will have a power budget of zero until it is manually provisioned. Since the sum of the manually provisioned wattages cannot exceed the total system power available, it may be necessary to adjust existing budgets to free up power for the new module.

When a PoE module is removed from a switch configured with manual power distribution mode, the PoE budget for each module will **not** be recalculated, based on the assumption that the module removed will be replaced with a new module that should receive the same amount of PoE power.

As noted above, if the total available PoE power is reduced, the power will automatically be redistributed based on applying the calculated percentages. If an additional PoE supply is installed, there is no impact on the assigned PoE since specific wattages have been assigned to each module. Only the "Total Power Detected" value will change. The extra PoE power, however, is available for further redistribution manually.

## Management of PoE Power to PDs



**Note:** This feature is available only on B5, C5, and G-Series fixed switch products.

For each PoE-capable module or switch (for the products listed above), you can configure how its PoE controller makes power available to attached powered devices (PDs). On a per module basis, you can configure:

- **Real-time** mode, in which the PoE controller calculates the power needed by a PD based on the actual power consumption of the attached devices.

- **Class** mode, in which the PoE controller manages power based on the IEEE 802.3af/.3at definition of the class limits advertised by the attached devices, with the exception that for class 0 and class 4 devices, actual power consumption will always be used. In this mode, the maximum amount of power required by a device in the advertised class is reserved for the port, regardless of the actual amount of power being used by the device.

Power management to PDs is configured with the command **set inlinepower management**. PoE classes are defined in [Table 7-1](#) on page 7-2.

## Configuring PoE

[Table 7-2](#) lists the PoE settings that you can configure through the CLI on each PoE-compliant Enterasys device.

**Table 7-2 PoE Settings Supported on Enterasys Devices**

| Setting                      | A4 | B3 | B5 | C3 | C5 | G-Series |
|------------------------------|----|----|----|----|----|----------|
| Port-specific PoE parameters | X  | X  | X  | X  | X  | X        |
| SNMP traps                   | X  | X  | X  | X  | X  | X        |
| PoE usage threshold          | X  | X  | X  | X  | X  | X        |
| PD detection method          | X  | X  | X  | X  | X  | X        |
| System power redundancy      |    |    |    |    | X  | X        |
| System power allocation      |    |    |    |    |    | X        |
| Module power allocation      |    |    |    |    |    | X        |
| PD power management          |    |    | X  |    | X  | X        |

Refer to the appropriate device-specific PoE configuration procedure.

- Stackable fixed switches A4, B3, and C3: [Procedure 7-1](#) on page 7-5
- Stackable fixed switches B5 and C5: [Procedure 7-2](#) on page 7-6
- Standalone G-Series: [Procedure 7-3](#) on page 7-7



**Note:** You must be logged on to the Enterasys device with read-write access rights to use the commands shown in the procedures in the following sections.

## Stackable A4, B3, and C3 Devices

### Procedure 7-1 PoE Configuration for Stackable A4, B3, and C3 Devices

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Command(s)                                                                                                                                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Configure PoE parameters on ports to which PDs are attached. <ul style="list-style-type: none"> <li>• <b>admin</b> — Enables (<b>auto</b>) or disables (<b>off</b>) PoE on a port. The default setting is <b>auto</b>.</li> <li>• <b>priority</b> — Sets which ports continue to receive power in a low power situation. If all ports have the same priority and the system has to cut power to the PDs, the PDs attached to the lowest numbered ports have the highest priority for receiving power. The default setting is <b>low</b>.</li> <li>• <b>type</b> — Associates an alias with a PD, such as "siemens phone."</li> </ul> | <b>set port inlinepower</b> <i>port-string</i> {[ <b>admin</b> { <b>off</b>   <b>auto</b> }] [ <b>priority</b> { <b>critical</b>   <b>high</b>   <b>low</b> }] [ <b>type</b> <i>type</i> ]} |
| 2.   | (Optional) Enable SNMP trap messages on the switch. The default setting is <b>enabled</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>set inlinepower trap</b> { <b>disable</b>   <b>enable</b> } <i>unit-number</i>                                                                                                           |
| 3.   | (Optional) Set the PoE usage threshold on the switch. Valid values are 11–100 percent. The default setting is 80 percent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <b>set inlinepower threshold</b> <i>usage-threshold unit-number</i>                                                                                                                         |
| 4.   | (Optional) Specify the method the Enterasys switch uses to detect connected PDs. <ul style="list-style-type: none"> <li>• <b>auto</b> (default) — The Enterasys device first uses the IEEE 802.3af/at standards resistor-based detection method. If that fails, the device uses the proprietary capacitor-based detection method.</li> <li>• <b>ieee</b> — The Enterasys device uses only the IEEE 802.3af/at standards resistor-based detection method.</li> </ul>                                                                                                                                                                  | <b>set inlinepower detectionmode</b> { <b>auto</b>   <b>ieee</b> }                                                                                                                          |

Refer to the switch's *CLI Reference Guide* for more information about each command.

## Stackable B5 and C5 Devices

### Procedure 7-2 PoE Configuration for Stackable B5 and C5 Devices

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Command(s)                                                                                                                      |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| 1.   | <p>Configure PoE parameters on ports to which PDs are attached.</p> <ul style="list-style-type: none"> <li>• <b>admin</b> — Enables (<b>auto</b>) or disables (<b>off</b>) PoE on a port. The default setting is <b>auto</b>.</li> <li>• <b>priority</b> — Sets which ports continue to receive power in a low power situation. If all ports have the same priority and the system has to cut power to the PDs, the PDs attached to the lowest numbered ports have the highest priority for receiving power. The default setting is <b>low</b>.</li> <li>• <b>type</b> — Associates an alias with a PD, such as “siemens phone.”</li> </ul> | <pre>set port inlinepower <i>port-string</i> {[admin {off   auto}] [priority {critical   high   low}] [type <i>type</i>]}</pre> |
| 2.   | <p>(Optional) Enable SNMP trap messages on the device. The default setting is <b>enabled</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <pre>set inlinepower trap {disable   enable} <i>unit-number</i></pre>                                                           |
| 3.   | <p>(Optional) Set the PoE usage threshold on the device. Valid values are 11–100 percent. The default setting is 80 percent.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <pre>set inlinepower threshold <i>usage-threshold</i> <i>unit-number</i></pre>                                                  |
| 4.   | <p>(Optional) Specify the method the Enterasys device uses to detect connected PDs.</p> <ul style="list-style-type: none"> <li>• <b>auto</b> (default) — The Enterasys device first uses the IEEE 802.3af/st standards resistor-based detection method. If that fails, the device uses the proprietary capacitor-based detection method.</li> <li>• <b>ieee</b> — The Enterasys device uses only the IEEE 802.3af/at standards resistor-based detection method.</li> </ul>                                                                                                                                                                  | <pre>set inlinepower detectionmode {auto   ieee}</pre>                                                                          |
| 5.   | <p>(Optional) Set the PoE management mode on a specified module.</p> <ul style="list-style-type: none"> <li>• <b>realtime</b> (default) — Manages power based on the actual power consumption of the ports.</li> <li>• <b>class</b> — Manages power based on the IEEE 802.3af/at definition of the class upper limit for each attached PD, except classes 0 and 4, for which the actual power consumption is used. In this mode, the maximum amount of power required by a PD in the advertised class is reserved for the port, regardless of the actual amount of power being used by the device.</li> </ul>                               | <pre>set inlinepower management {realtime   class} <i>module-number</i></pre>                                                   |



**Procedure 7-2 PoE Configuration for Stackable B5 and C5 Devices (continued)**

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Command(s)                                                          |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| 6.   | <p>(Optional on <b>C5 only</b>) Set the power redundancy mode on the system if two power supplies are installed.</p> <ul style="list-style-type: none"> <li>• <b>redundant</b> (default) — The power available to the system equals the maximum output of the lowest rated supply (400W or 1200W). If two supplies are installed in redundant mode, system power redundancy is guaranteed if one supply fails.</li> <li>• <b>non-redundant</b> — The combined output of both supplies is available to the system. In this mode, a power supply failure may result in a system reset. Also called additive mode.</li> </ul> <p>If two power supplies are installed, the power supply LEDs on the device's front panel indicate whether the power supplies are in redundant mode (green LEDs) or non-redundant mode (amber LEDs).</p> | <b>set system power</b> { <b>redundant</b>   <b>non-redundant</b> } |

Refer to the switch's *CLI Reference Guide* for more information about each command.

**G-Series Devices****Procedure 7-3 PoE Configuration for G-Series Devices**

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Command(s)                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | <p>Configure PoE parameters on ports to which PDs are attached.</p> <ul style="list-style-type: none"> <li>• <b>admin</b> — Enables (<b>auto</b>) or disables (<b>off</b>) PoE on a port. The default setting is <b>auto</b>.</li> <li>• <b>priority</b> — Sets which ports continue to receive power in a low power situation. If all ports have the same priority and the system has to cut power to the PDs, the PDs attached to the lowest numbered ports have the highest priority for receiving power. The default setting is <b>low</b>.</li> <li>• <b>type</b> — Associates an alias with a PD, such as "siemens phone."</li> </ul> | <b>set port inlinpower</b> <i>port-string</i> {[ <b>admin</b> { <b>off</b>   <b>auto</b> }] [ <b>priority</b> { <b>critical</b>   <b>high</b>   <b>low</b> }] [ <b>type</b> <i>type</i> ]} |
| 2.   | (Optional) Enable SNMP trap messages on the module. The default setting is <b>enabled</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>set inlinpower trap</b> { <b>disable</b>   <b>enable</b> } <i>module-number</i>                                                                                                         |
| 3.   | <p>(Optional) Set the PoE usage threshold on the module. Valid values are 11–100 percent.</p> <p>Use the <b>clear</b> command to reset the PoE usage threshold on a specified module to the default value of 80 percent.</p>                                                                                                                                                                                                                                                                                                                                                                                                                | <b>set inlinpower threshold</b> <i>usage-threshold</i> <i>module-number</i><br><b>clear inlinpower threshold</b> <i>module-number</i>                                                      |

### Procedure 7-3 PoE Configuration for G-Series Devices (continued)

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Command(s)                                                         |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| 4.   | <p>(Optional) Specify the method the Enterasys device uses to detect connected PDs.</p> <ul style="list-style-type: none"> <li>• <b>auto</b> (default) — The Enterasys device first uses the IEEE 802.3af/at standards resistor-based detection method. If that fails, the device uses the proprietary capacitor-based detection method.</li> <li>• <b>ieee</b> — The Enterasys device uses only the IEEE 802.3af/at standards resistor-based detection method.</li> </ul>                                                                                                                                                                                                                                                                                                                                        | <b>set inlinepower detectionmode {auto   ieee}</b>                 |
| 5.   | <p>(Optional) Set the power redundancy mode on the system if two power supplies are installed.</p> <ul style="list-style-type: none"> <li>• <b>redundant</b> (default) — The power available to the system equals the maximum output of the lowest rated supply (400W or 1200W). If two supplies are installed in redundant mode, system power redundancy is guaranteed if one supply fails.</li> <li>• <b>non-redundant</b> — The combined output of both supplies is available to the system. In this mode, a power supply failure may result in a system reset. Also called additive mode.</li> </ul> <p>If two power supplies are installed, the power supply LEDs on the device's front panel indicate whether the power supplies are in redundant mode (green LEDs) or non-redundant mode (amber LEDs).</p> | <b>set system power {redundant   non-redundant}</b>                |
| 6.   | <p>(Optional) Set the PoE management mode on a specified module.</p> <ul style="list-style-type: none"> <li>• <b>realtime</b> (default) — Manages power based on the actual power consumption of the ports.</li> <li>• <b>class</b> — Manages power based on the IEEE 802.3af/at definition of the class upper limit for each attached PD, except classes 0 and 4, for which the actual power consumption is used. In this mode, the maximum amount of power required by a PD in the advertised class is reserved for the port, regardless of the actual amount of power being used by the device.</li> </ul>                                                                                                                                                                                                     | <b>set inlinepower management {realtime   class} module-number</b> |



Refer to the switch's *CLI Reference Guide* for more information about each command.

## Example PoE Configuration

A PoE-compliant G-Series device is configured as follows:

- One 400W power supply is installed. The power available for PoE is 150W.
- Two PoE modules are installed.
- The **set inlinpower mode** command is set to **auto**, which means that the power available for PoE (150W) is distributed evenly—75W to each PoE module.
- The power required to run the PDs, which are all connected to this G-Series device through the module in slot 2, is 100W.

To make power available for all the PDs connected to the module in slot 2, the network administrator must first change the setting of the **set inlinpower mode** command:

```
G3(su)->set inlinpower mode manual
```

When this setting for the **set inlinpower mode** command changes to **manual**, none of the 150W available for PoE are assigned to the PoE modules. The network administrator must assign the 150W, or some portion of the 150W to the PoE modules to power the attached PDs.

```
G3(su)->set inlinpower assign 100 2
```

## PoE Display Commands

[Table 7-3](#) lists PoE show commands for Enterasys devices.

**Table 7-3 PoE Show Commands**

| Task                                                                                                                                                                                                                                                                                                  | Command                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| Use this command to display PoE properties for a device.                                                                                                                                                                                                                                              | <b>show inlinpower</b>                             |
| Use this command to display information about the ports that support PoE: <ul style="list-style-type: none"> <li>• Type of PD attached (if specified)</li> <li>• Administrative and operational status</li> <li>• Priority</li> <li>• Class of PD attached</li> <li>• Power used by the PD</li> </ul> | <b>show port inlinpower</b> [ <i>port-string</i> ] |

Refer to the switch's *CLI Reference Guide* for a description of the output of each command.

## Port Configuration

This chapter describes the basic port parameters and how to configure them. Also described in this chapter are port link flap detection, port mirroring, and transmit queue monitoring and how to configure them.

Link Aggregation Control Protocol (LACP) is described in [Chapter 11, Configuring Link Aggregation](#).

| For information about...                             | Refer to page... |
|------------------------------------------------------|------------------|
| <a href="#">Port Configuration Overview</a>          | 8-1              |
| <a href="#">Configuring Port Link Flap Detection</a> | 8-8              |
| <a href="#">Transmit Queue Monitoring</a>            | 8-11             |
| <a href="#">Port Mirroring</a>                       | 8-12             |

### Port Configuration Overview

The Enterasys stackable and standalone switches have fixed front panel switch ports. The I-Series and G-Series standalone switches also have expansion slots where optional I/O modules can be installed. Refer to the data sheet and/or the *Installation Guide* for the standalone switches for information about available optional I/O modules.

The syntax used to identify the switch ports on the front panel and the expansion slots is interface-type dependent and is also dependent on the location of the switch in a stack, for the stackable switches, or on the chassis slot in which the I/O modules are installed, for the standalone switches. See the section entitled “[Port String Syntax Used in the CLI](#)” below for more information.

Port numbering proceeds from 1 to the maximum number of that port type on the switch or module. If there are multiple port types, each port type numbering starts at 1. A port’s number is displayed on the chassis or I/O module next to each port.

### Port String Syntax Used in the CLI

Commands requiring a *port-string* parameter use the following syntax to designate port type, unit or slot location, and port number:

**port type.unit\_or\_slot number.port number**

Where **port type** can be:

- fe** for 100-Mbps Ethernet
- ge** for 1-Gbps Ethernet
- tg** for 10-Gbps Ethernet
- host** for the host port

**vlan** for vlan interfaces  
**lag** for IEEE802.3 link aggregation ports

Where **unit\_or\_slotnumber** can be:

- 1 - 8 for stackable switches (up to 8 units in a stack)
- 1 - 3 for I-Series standalone switches  
(Note that the uplink ports are considered to be slot 3)
- 1 - 4 for G-Series standalone switches

Where **port number** depends on the device. The highest valid port number is dependent on the number of ports in the device and the port type.

## Examples



**Note:** You can use a wildcard (\*) to indicate all of an item. For example, fe.3.\* would represent all 100Mbps Ethernet (fe) ports in slot or unit 3, and ge.3 \* would represent all 1-Gigabit Ethernet (ge) ports in slot or unit 3.

This example shows the *port-string* syntax for specifying the 100-Mbps Ethernet ports 1 through 10 in slot or unit 2.

```
fe.2.1-10
```

This example shows the *port-string* syntax for specifying the 1-Gigabit Ethernet port 14 in slot or unit 3.

```
ge.3.14
```

This example shows the *port-string* syntax for specifying all 1-Gigabit Ethernet ports in slot or unit 3 in the system.

```
ge.3.*
```

This example shows the *port-string* syntax for specifying all ports (of any interface type) in the system.

```
..*
```

## Console Port Settings

Each Enterasys switch includes a console port through which local management of the switch can be accessed using a PC, terminal, or modem.

When switches are stacked, only the console port on the master unit is active. The console ports on the member units of the stack are deactivated.

Default console port settings are:

- Baud rate: 9600
- Data bits: 8
- Flow control: disabled
- Stop bits: 1
- Parity: none
- VT100 terminal mode: disabled

Only the baud rate and VT100 terminal mode can be changed.

Use the **show console** command to display the console port settings. For example:

```
C5(su)->show console
vt100 terminal mode disabled
Baud Flow Bits StopBits Parity

9600 Disable 8 1 none
```

Use the **set console baud** command to change the baud rate of the console port. For example, to set the console port baud rate to 19200:

```
C5(su)->set console baud 19200
```

## VT100 Terminal Mode

VT100 terminal mode supports automatic console session termination on removal of the serial connection (vs. timeout). This mode requires that the device attached to the console port be running VT100 terminal emulation.

In VT100 mode, the switch polls for device status (using the appropriate VT100 escape sequence) to detect an attached device. At any time, if the switch fails to get a status reply, an existing console session is terminated.

On receipt of the first polled status response, the login banner is displayed if it is configured.

VT100 terminal mode is disabled by default on the console port. Use the **set console vt100** command to enable or disable this mode. The **show console** command displays the current setting of Vt100 terminal mode.

## Port Settings

This section describes the port settings that can be configured.

### Port Status

By default, all ports are enabled at device startup. You may want to disable ports for security or to troubleshoot network issues.

Use the **set port disable** command to administratively disable one or more ports. When this command is executed, in addition to disabling the physical Ethernet link, the port will no longer learn entries in the forwarding database.

Use the **set port enable** command to administratively enable one or more ports.

The following example disables Gigabit Ethernet ports 1 through 4 on the switch unit 1:

```
C5(su)->set port disable ge.1.1-4
```

### Port Name or Alias

The port alias feature allows you to associate a name with a port.

Use the **set port alias** command to assign an alias name to a port. If the alias name contains spaces, the text string must be surrounded by double quotes. Maximum length is 60 characters.

You can delete an alias name from a port with the **set port alias** command, by specifying a port string but no text string.

Use the **show port alias** command to display alias names for one or more ports.

## Auto-Negotiation and Advertised Ability

Auto-negotiation is an Ethernet feature that facilitates the selection of port speed, duplex, and flow control between the two members of a link, by first sharing these capabilities and then selecting the fastest transmission mode that both ends of the link support. Auto-negotiation is enabled by default.

Use the **set port negotiation** command to disable or enable auto-negotiation. Use the **show port negotiation** to display the current auto-negotiation status for one or more ports.

The advertised ability feature allows for the port to share its port capabilities with the other end of the link. Advertised capabilities will be used during the auto-negotiation process to select the fastest transmission mode that both ends of the link support. Actual port capabilities, advertised port capability and remote end advertised port capabilities can be displayed using the **show port advertise** command. The following port capabilities can be advertised:

|                |                              |
|----------------|------------------------------|
| <b>10t</b>     | 10BASE-T half duplex mode.   |
| <b>10tfd</b>   | 10BASE-T full duplex mode.   |
| <b>100tx</b>   | 100BASE-TX half duplex mode. |
| <b>100txfd</b> | 100BASE-TX full duplex mode. |
| <b>1000t</b>   | 1000BASE-T half duplex mode. |
| <b>1000tfd</b> | 1000BASE-T full duplex mode. |
| <b>pause</b>   | PAUSE for full-duplex links. |

During auto-negotiation, the port “tells” the device at the other end of the segment what its capabilities and mode of operation are. If auto-negotiation is disabled, the port reverts to the values specified by default speed, default duplex, and the port flow control commands.

In normal operation, with all capabilities enabled, advertised ability enables a port to “advertise” that it has the ability to operate in any mode. You may choose to configure a port so that only a portion of its capabilities are advertised and the others are disabled. Use the **set port advertise** command to configure what a port will advertise for speed/duplex capabilities in auto-negotiation. Use the **clear port advertise** command to configure a port to not advertise a specific speed/duplex capability when auto-negotiating with another port.

For G-Series systems, refer to “[Configuring SFP Ports for 100BASE-FX](#)” on page 8-7 for information on configuring settings for 100 Mb SFP ports.

## Port Speed and Duplex Mode

When auto-negotiation is enabled, the port speed (10, 100, or 1000 Mbps) and duplex mode (full- or half-duplex) are determined automatically based on the established link. Note that auto-negotiation is enabled by default on all ports.

If auto-negotiation is disabled, you can set the default speed for a port with the **set port speed** command and the duplex mode with the **set port duplex** command. Use the **show port speed** and **show port duplex** commands to display current settings.

## MDI / MDIX Cable Type

Switch ports can automatically detect and configure the required cable type, either straight through (MDI) or cross-over (MDIX), or the ports can be configured to only allow one type of cable type, either MDI or MDIX.



By default, Enterasys switch devices are configured to automatically detect the cable type connection, straight through (MDI) or cross-over (MDIX), required by the cable connected to the port. You can configure ports to only use MDI or MDIX connections with the **set port mdix** command.

The **set port mdix** command only configures Ethernet ports, and cannot be used to configure combo ports on the switch. Fiber ports always have a status of MDIX.

Use the **show port mdix** command to display the status of cable connection type configuration mode for one or more ports.

## Port Flow Control

Flow control is used to manage the transmission between two devices as specified by IEEE 802.3x to prevent receiving ports from being overwhelmed by frames from transmitting devices.

It provides a mechanism for the receiver to control the transmission speed. Flow control helps prevent congestion. Flow control should be distinguished from congestion control, which is used for controlling the flow of data when congestion has actually occurred.

When auto-negotiation is enabled, the port flow control setting has no bearing on flow control. Pause is negotiated through the predefined advertised settings. The port flow control setting takes effect when auto-negotiation is disabled.

Use the **show flowcontrol** command to display the current global status, either enabled or disabled. Use the **set flowcontrol** command to globally enable or disable flow control.

## Jumbo Frame Support



**Note:** Jumbo frame support is not supported on I-Series platforms.

Jumbo frame support allows Gigabit Ethernet ports to transmit frames up to 10 KB in size. LAG ports can also be configured for jumbo frame support.

By default, jumbo frame support is enabled on all ports.

Use the **show port jumbo** command to display the status of jumbo frame support and maximum transmission units (MTU) on one or more ports. For example:

```
C5(su)->show port jumbo ge.1.1
```

| Port Number | Jumbo Status | Max Frame Size |
|-------------|--------------|----------------|
| ge.1.1      | Enable       | 9216           |

Use the **set port jumbo** command to enable or disable jumbo frame support on one or more ports. Use the **clear port jumbo** command to reset one or more ports to the default state of enabled.

## Broadcast Suppression Threshold

This feature limits the number of received broadcast frames the switch will accept per port. Broadcast suppression protects against broadcast storms and ARP sweeps.

Broadcast suppression thresholds apply only to broadcast traffic—multicast traffic is not affected. By default, broadcast suppression is enabled on all ports with a threshold of 14881 packets per second (pps), regardless of actual port speed.

Use the **set port broadcast** command to set the threshold to a different value from the default. If you would like to disable broadcast suppression, set the threshold limit for each port to the

maximum number of packets which can be received per second with the **set port broadcast** command: Maximum packet per second values are:

- 148810 for Fast Ethernet ports
- 1488100 for 1-Gigabit ports.
- 14881000 for 10- Gigabit ports

Use the **show port broadcast** command to display current threshold settings. Use the **clear port broadcast** command to return broadcast threshold settings to the default of 14881 packets per second.



**Note:** Class of Service functionality can also be used to control broadcast, unknown unicast, and/or multicast flooding. This feature prevents configured ports from being disrupted by a traffic storm by rate-limiting specific types of packets through those ports. Refer to “[Flood Control](#)” on page 17-9 for more information.

## Protected Port Mode

The Protected Port feature is used to prevent ports from forwarding traffic to each other, even when they are on the same VLAN. Ports may be designated as either protected or unprotected. Ports are unprotected by default. Up to three groups of protected ports are supported.

Ports that are configured to be protected cannot forward traffic to other protected ports in the same group, regardless of having the same VLAN membership. However, protected ports can forward traffic to ports which are unprotected (not listed in any group). Protected ports can also forward traffic to protected ports in a different group, if they are in the same VLAN. Unprotected ports can forward traffic to both protected and unprotected ports. A port may belong to only one group of protected ports.

This feature only applies to ports within a switch or a stack. It does not apply across multiple switches in a network.

Ports are added to a protected port group with the **set port protected** command. Up to three groups may be configured. A name can be assigned to a group with the **set port protected name** command. In the following example, ports 1 through 4 are assigned to group id 1, and the name “group1” is assigned to that group id.

```
C5(su)->set port protected ge.1.1-4 1
C5(su)->set port protected name 1 group1
C5(su)->show port protected ge.1.1-4
```

| Group id | Port   | GroupName |
|----------|--------|-----------|
| 1        | ge.1.1 | group1    |
| 1        | ge.1.2 | group1    |
| 1        | ge.1.3 | group1    |
| 1        | ge.1.4 | group1    |

Use the **clear port protected** command to remove ports from protected mode or to remove a group id from protected mode. Use the **clear port protected name** command to remove a name from a group id.

## Displaying Port Status

[Table 8-1](#) on page 8-7 lists additional commands that can be used to display port status.

**Table 8-1 Displaying Port Status**

| Task                                                                                                                                                                                                                                      | Command                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Display whether or not one or more ports are enabled for switching.                                                                                                                                                                       | <b>show port</b> [ <i>port-string</i> ]                                   |
| Display operating and admin status, speed, duplex mode and port type for one or more ports on the device.                                                                                                                                 | <b>show port status</b> [ <i>port-string</i> ]                            |
| Display port counter statistics detailing traffic through the device and through all MIB2 network devices.                                                                                                                                | <b>show port counters</b> [ <i>port-string</i> ] [ <b>switch   mib2</b> ] |
| Clear port counter statistics for a port or range of ports.                                                                                                                                                                               | <b>clear port counters</b> [ <i>port-string</i> ]                         |
| Troubleshoot and locate faults in copper cable connections on a per port basis. Only available on switch platforms that provide 1 Gigabit Ethernet RJ45 ports.<br>See <a href="#">Displaying Cable Status</a> below for more information. | <b>show port cablestatus</b> [ <i>port-string</i> ]                       |

## Displaying Cable Status

For 1 Gigabit Ethernet RJ45 ports only, the **show port cablestatus** command will display the status of the port's cable connection and the approximate length of the cable attached to the port. If your switch platform does not support 1 GE RJ45 ports, this command will not be available.

If no cable is attached to the port, the status will be "Open" and no length will be shown. If the port is not a 1GE RJ45 port, the command will return a status of "Not Supported." Other status messages include:

- Normal = normal
- Short = detection of an inter-pair short
- Fail = unknown error or crosstalk
- Detach = indicates ports on stack units that are no longer present, but were previously connected Normal

Since running the cable diagnostics may momentarily interrupt packet flow, a warning message is displayed and you are prompted to continue.

## Configuring SFP Ports for 100BASE-FX

By default, SFP ports in the G3G124-24, G3G124-24P, and G3G170-24 base units, and the G3G-24TX and G3G-24SFP optional IOM modules support 1-Gigabit transceivers (Mini-GBICs) for 1000BASE-LX/SX fiber-optic connections and 1000BASE-T copper connections. Optionally, these ports can support a Fast Ethernet transceiver for 100BASE-FX connections when that transceiver is installed and [Procedure 8-1](#) is completed on each applicable port:

**Procedure 8-1 Configuring SFP Ports for 100BASE-FX**

| Step | Task                                                              | Command(s)                                                       |
|------|-------------------------------------------------------------------|------------------------------------------------------------------|
| 1.   | Disable the port's auto-negotiation.                              | <b>set port negotiation</b> <i>port-string</i><br><b>disable</b> |
| 2.   | Set the port's advertised ability to 100BASE-TX full duplex mode. | <b>set port advertise</b> <i>port-string</i><br><b>100txfd</b>   |
| 3.   | Set the port speed to 100 Mbps.                                   | <b>set port speed</b> <i>port-string</i> <b>100</b>              |

**Procedure 8-1 Configuring SFP Ports for 100BASE-FX**

| Step | Task                                | Command(s)                                            |
|------|-------------------------------------|-------------------------------------------------------|
| 4.   | Set the port duplex mode to full.   | <b>set port duplex</b> <i>port-string</i> <b>full</b> |
| 5.   | (Optional) Verify the new settings. | <b>show port status</b> <i>port-string</i>            |

**Example**

This example shows how to configure port ge.2.1 in the G3G-24SFP module to operate with a 100BASE-FX transceiver installed. First, the module is verified as present in Slot 2, and the port status is shown as operating as a 1000BASE-SX port. After the 1-Gigabit transceiver is replaced with the a 100 Mbps transceiver, the port is configured appropriately and the new settings are verified.

```
G3(su)->show version
Slot Status Ports Model Serial Number Hw Version
---- -
1 Present 24 G3G170-24 0011223302 BCM56514 REV 1
2 Present 24 G3G-24SFP H03611239 BCM56512 REV 1
3
4
G3(su)->show port advertise ge.2.1
ge.2.1 capability advertised remote

10BASE-T no no no
10BASE-TFD no no no
100BASE-TX no no no
100BASE-TXFD yes no no
1000BASE-T no no no
1000BASE-TFD yes yes no
pause yes yes no

G3(su)->show port status ge.2.1
Port Alias Oper Admin Speed Duplex Type

ge.2.1 (truncated) Down Up N/A N/A 1000BASE-SX

G3(su)->set port negotiation ge.2.1 disable
G3(su)->set port advertise ge.2.1 100txfd
G3(su)->set port speed ge.2.1 100
G3(su)->set port duplex ge.2.1 full

G3(su)->show port status ge.2.1
Port Alias Oper Admin Speed Duplex Type

ge.2.1 (truncated) Down Up 100.0M full 100BASE-FX
```

For more information, refer to the commands in this chapter and to your fixed switch hardware installation documentation.

## Configuring Port Link Flap Detection

The link flap detection feature monitors link flapping (that is, when a link goes up and down rapidly) on a physical port. Link flapping indicates a Layer 1 (physical layer) problem, such as a faulty cable or GBIC. If link flapping occurs, your Enterasys switch can react by disabling the affected port and generating a syslog entry and an SNMP trap to notify you of the event.

If left unresolved, link flapping can be detrimental to network stability by triggering Spanning Tree and routing table recalculations. By enabling the link flap detection feature on your Enterasys switch, you can monitor and act upon link flapping to avoid these recalculations.

You can enable link flap detection globally on your Enterasys switch or on specific ports, such as uplink ports. The link flap detection feature allows you to specify the action that occurs when a certain number of link flapping instances occur within a certain period of time. By default, if a port on which link flap is enabled experiences ten link flapping instances within a 5-second period, that port will be disabled for 300 seconds and both a syslog entry and an SNMP trap will be generated.

If a port has been disabled because of excessive link flapping, you can reset the port to operational.

Table 8-2 lists the default linkflap parameters.

**Table 8-2 Linkflap Default Parameters**

| Linkflap Parameter                                                                     | Default Condition |
|----------------------------------------------------------------------------------------|-------------------|
| Linkflap global state                                                                  | Disabled          |
| Linkflap port state                                                                    | Disabled          |
| Linkflap action                                                                        | None              |
| Linkflap interval                                                                      | 5                 |
| Linkflap maximum allowed link downs per 10 seconds                                     | 20                |
| Linkflap threshold<br>(number of allowed link down transitions before action is taken) | 10                |
| Linkflap downtime                                                                      | 300 seconds       |

## Basic Link Flap Detection Configuration

Procedure 8-2 describes the basic steps to configure link flap detection on Enterasys stackable and standalone fixed switches.



**Note:** You must be logged in to the Enterasys switch with read-write access rights to use the commands shown in this procedure.

**Procedure 8-2 Link Flap Detection Configuration**

| Step | Task                                                                                                                                                                                                                                           | Command(s)                                                                                                                    |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| 1.   | In switch mode, enable ports for sending SNMP trap messages when their link status changes.<br><br>By default, all ports on your Enterasys switch are enabled to send SNMP trap messages indicating changes in their link status (up or down). | <b>set port trap</b> <i>port-string</i> {enable   disable}                                                                    |
| 2.   | Enable link flap detection either globally or on specific ports. By default, link flap is disabled globally and per port.                                                                                                                      | <b>set linkflap globalstate</b> {disable   enable}<br><b>set linkflap portstate</b> {disable   enable} [ <i>port-string</i> ] |
| 3.   | (Optional) Set the time interval (in seconds) for accumulating link flapping instances. By default, this value is set to 5 seconds.                                                                                                            | <b>set linkflap interval</b> <i>port-string interval_value</i>                                                                |

**Procedure 8-2 Link Flap Detection Configuration (continued)**

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                        | Command(s)                                                                                                                                                                                                                                                                   |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.   | (Optional) Set the number of link flapping instances necessary to trigger the link flap action. By default, this value is 10 link flapping instances.                                                                                                                                                                                                                                                                       | <b>set linkflap threshold</b> <i>port-string</i> <i>threshold_value</i>                                                                                                                                                                                                      |
| 5.   | (Optional) Set how the Enterasys device will react to excessive link flapping: <ul style="list-style-type: none"> <li>• Disable the port</li> <li>• Generate a Syslog entry</li> <li>• Generate an SNMP trap message</li> <li>• All of the above</li> </ul> <p>By default, no actions occur in reaction to excessive link flapping.</p> <p>To clear reactions to excessive link flapping, use the <b>clear</b> command.</p> | <b>set linkflap action</b> <i>port-string</i> { <b>disableInterface</b>   <b>gensyslogentry</b>   <b>gentrap</b>   <b>all</b> }<br><br><b>clear linkflap action</b> [ <i>port-string</i> ] { <b>disableInterface</b>   <b>gensyslogentry</b>   <b>gentrap</b>   <b>all</b> } |
| 6.   | (Optional) Set the time interval, in seconds, that one or more ports will be disabled after excessive link flapping. By default, this value is 300 seconds.                                                                                                                                                                                                                                                                 | <b>set linkflap downtime</b> <i>port-string</i> <i>downtime_value</i>                                                                                                                                                                                                        |
| 7.   | To toggle link flap disabled ports to operational.                                                                                                                                                                                                                                                                                                                                                                          | <b>clear linkflap down</b> [ <i>port-string</i> ]                                                                                                                                                                                                                            |

Refer to your switch platform's *CLI Reference Guide* for more information about each command.

**Example**

PoE devices (for example, VoIP phones or wireless access points) connected to a link flap supported Enterasys device are experiencing intermittent power losses, though the Enterasys device itself has not experienced any corresponding power losses. The network administrator enables link flap detection on a range of PoE ports to which the PoE devices are connected.

```
C5(rw)->set linkflap portstate enable ge.1.1-12
```

The network administrator also sets values for the interval, threshold, and downtime on the ports.

```
C5(rw)->set linkflap action ge.1.1-12 all
```

```
C5(rw)->set linkflap interval ge.1.1-12 20
```

```
C5(rw)->set linkflap threshold ge.1.1-12 8
```

```
C5(rw)->set linkflap downtime ge.1.1-12 600
```

If the link flap threshold is exceeded within the link flap interval (eight link flap conditions within 20 seconds, as configured above), the Enterasys device will, by default, disable the port (for 600 seconds, as configured above) and generate both a syslog entry and an SNMP trap. These default actions can be changed by using the **set linkflap action** command.

The Enterasys device disables ports ge.1.1 and ge.1.2 when excessive link flapping occurs on the ports. The network administrator can check the status of the ports and the number of link flap conditions that occurred by using the **show linkflap metrics** command.

While the ports are disabled, the network administrator replaces the potentially faulty Ethernet cables connecting the ports to the PoE devices. The network administrator then enables the ports.

```
C5(rw)->clear linkflap down ge.1.1-2
```

If no additional power losses occur on the PoE devices and no additional link flapping conditions occur, the network administrator disables link flap detection on the PoE ports.

```
C5(rw)->set linkflap portstate disable ge.1.1-12
```

## Link Flap Detection Display Commands

Table 8-3 lists link flap detection show commands.

**Table 8-3 Link Flap Detection Show Commands**

| Task                                                                                                                                                                                                                       | Command                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display whether the port is enabled for generating an SNMP trap message if its link state changes.                                                                                                                         | <b>show port trap</b> [ <i>port-string</i> ]                                                                                                                                                                                                                                                                                                                                              |
| Display link flap detection state and configuration information.<br>The <b>show linkflap parameters</b> and <b>show linkflap metrics</b> commands provide summary views of your current link flap detection configuration. | <b>show linkflap</b> { <b>globalstate</b>   <b>portstate</b>   <b>parameters</b>   <b>metrics</b>   <b>portsupported</b>   <b>actsupported</b>   <b>maximum</b>   <b>downports</b>   <b>action</b>   <b>operstatus</b>   <b>threshold</b>   <b>interval</b> ]   <b>downtime</b>   <b>currentcount</b>   <b>totalcount</b>   <b>timelapsed</b>   <b>violations</b> [ <i>port-string</i> ]} |

Refer to your switch's *CLI Reference Guide* for a description of the output of each command.

## Transmit Queue Monitoring

The CLI provides a number of commands that can be used to monitor transmit queues and, if a queue is found to be stalled, to take corrective action.

Stalled transmit queues may be caused by a duplex mismatch, hardware error, or by excessive pause frames. Excessive pause frames are not expected under normal conditions but may be the result of a soft or hard failure on an attached device, or even a deliberate denial of service attack.

Transmit queue monitoring periodically samples each port's transmit queue depths (total packets queued) and transmit counters to identify stalled ports and free the resources tied up on the associated transmit queues. This feature allows you to configure a minimum number of transmits for a sample period and to set levels for the number of consecutive failures that will trigger different levels of corrective actions.

Corrective actions that can be configured include logging, discarding received pause frames, and disabling the port. The ability to pause the switch is treated as a privilege — if an attached device violates that privilege, its pause frames can be ignored. When a switch port is in the discarding pause state, the port will be allowed to transmit (including Wake-on-LAN magic packets). The port retains its ability to transmit its own pause frames, and the attached device is still allowed the normal switching of packets. Because disabling a port and discarding pause frames is a punitive action, a port restore interval "downtime" is provided. At the end of the downtime interval, all disabled ports will have complete functionality restored. In addition, any change in a port's link state clears that port's failure count and restores the port to normal operation.

Table 8-4 lists the commands used to perform transmit queue monitoring tasks.

**Table 8-4 Transmit Queue Monitoring Tasks**

| Task                                                                                                        | Command                                                  |
|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| Enable or disable transmit queue monitoring on the switch. Transmit queue monitoring is enabled by default. | <b>set txqmonitor</b> { <b>enable</b>   <b>disable</b> } |



**Table 8-4 Transmit Queue Monitoring Tasks**

| Task                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Command                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure the time interval, in seconds, that ports disabled by the transmit queue monitoring feature remain disabled.<br>The default value is 0, meaning that disabled ports will remain disabled until cleared manually or until their next link state transition.                                                                                                                                                                                      | <code>set txqmonitor downtime <i>seconds</i></code>                                                                                                 |
| Set the minimum rate (in packets per second) of transmitted packets in a sampling interval.<br>The default value is 1 packet per second.                                                                                                                                                                                                                                                                                                                  | <code>set txqmonitor minrate <i>rate</i></code>                                                                                                     |
| Set the transmit queue monitoring threshold levels for triggering actions applied to a stalled port.                                                                                                                                                                                                                                                                                                                                                      | <code>set txqmonitor threshold { [logging   ignorepause   disableinterface] <i>value</i> }</code>                                                   |
| Restore all transmit queue monitoring options to their default values.                                                                                                                                                                                                                                                                                                                                                                                    | <code>clear txqmonitor { all   globalstate   ignorepause [<i>port-string</i>]   down [<i>port-string</i>]   threshold   downtime   minrate }</code> |
| Display information about transmit queue monitoring.                                                                                                                                                                                                                                                                                                                                                                                                      | <code>show txqmonitor [ downports   downtime   globalstate   ignorepause   minrate   operstatus   threshold ]</code>                                |
| Display the flow control information for one or more ports.                                                                                                                                                                                                                                                                                                                                                                                               | <code>show txqmonitor flowcontrol [<i>port-string</i>]</code>                                                                                       |
| Display transmit queue monitoring information for one or more ports, including: <ul style="list-style-type: none"> <li>Status — whether the port is operating normally, or ignoring received pause frames, or disabled due to transmit queue monitoring corrective action</li> <li>Transmit queue sampling counts — the number of consecutive samples showing stalled transmit queues, and the total number of samples showing stalled queues.</li> </ul> | <code>show txqmonitor port [<i>port-string</i>]</code>                                                                                              |

## Port Mirroring



**Caution:** Port mirroring configuration should be performed only by personnel who are knowledgeable about the effects of port mirroring and its impact on network operation.

The fixed switch device allows you to mirror (or redirect) the traffic being switched on a port for the purposes of network traffic analysis and connection assurance. When port mirroring is enabled, one port becomes a monitor port for another port within the device (the stack, if applicable).

## Mirroring Features

The fixed switch devices support the following mirroring features:

- Mirroring can be configured in a many-to-one configuration so that one target (destination) port can monitor traffic on up to 8 source ports. Only one mirror destination port can be configured per stack, if applicable.



- LAG ports can be a mirror source port, but not a mirror destination port. If a LAG port is a mirror source port, no other ports can be configured as source ports.
- Both transmit and receive traffic will be mirrored.
- A destination port will only act as a mirroring port when the session is operationally active.
- When a port mirror is created, the mirror destination port is removed from the egress list of VLAN 1 after a reboot.
- MAC addresses will be learned for packets tagged with the mirror VLAN ID. This will prevent the ability to snoop traffic across multiple hops.



**Caution:** Traffic mirrored to a VLAN may contain control traffic. This may be interpreted by the downstream neighbor as legal control frames. It is recommended that you disable any protocols (such as Spanning Tree) on inter-switch connections that might be affected .

## Configuring Port Mirroring

Use the **set port mirroring** command to create, enable, or disable a mirroring relationship. By default, port mirrors are enabled automatically when created. Up to 8 source ports can be specified. Only one destination port can be configured per stack, if applicable.

```
set port mirroring {create | disable | enable} source destination
```

LAG ports can be mirror source ports. However, if a LAG port is configured as the source port, no other ports can be added as source ports for that mirror.



**Notes:** When a port mirror is created, the mirror destination port is removed from VLAN 1's egress list after a reboot. MAC addresses will be learned for packets tagged with the mirror VLAN ID. This will prevent the ability to snoop traffic across multiple hops.

The following example creates and enables port mirroring with ge.1.4 as the source port, and ge.1.11 as the target port:

```
C5(su)->set port mirroring create ge.1.4 ge.1.11
```

Use the **clear port mirroring** command to remove a port mirroring relationship.

```
clear port mirroring source destination
```

Use the **show port mirroring** command to display the currently configured port mirror relationship.

```
C5(su)->show port mirroring
```

```
Port Mirroring
=====
Source Port = ge.1.4
Target Port = ge.1.11
Frames Mirrored = Rx and Tx
Port Mirroring status enabled.
```

## Remote Port Mirroring



**Note:** Remote port mirroring is not supported on the A4 or I-Series platforms.

Remote port mirroring is an extension to port mirroring which facilitates simultaneous mirroring of multiple source ports on multiple switches across a network to one or more remote destination ports.

Remote port mirroring involves configuration of the following port mirroring related parameters:

1. Configuration of normal port mirroring source ports and one destination port on all switches, as described above.
2. Configuration of a mirror VLAN, which is a unique VLAN on which mirrored packets traverse across the network. The mirror VLAN has to be configured on ALL switches across the network along which mirrored traffic traverses, from the switch where the source ports reside to the switch where the mirrored packets are sniffed and/or captured.

You must ensure that switches involved are properly configured to facilitate correct remote port mirroring operation. The following points in particular need to be observed:

- On the source switch, the correct destination port must be chosen to ensure that there is an egress path from that port to the desired remote destination(s).
- All ports on the path from the source port to the remote destination must be members of the mirror VLAN.
- On switches on the path from the source port to the remote destination, egress tagging has to be enabled on potential egress ports for the mirror VLAN.

With the introduction of remote port mirroring:

- Configured mirror destination ports will NOT lose their switching or routing properties.
- On switches where the mirror VLAN has been configured, any traffic on that VLAN will be flooded on the VLAN. It will never be unicast, even if the source address of the traffic as been learned on the switch.

## Configuring Remote Port Mirroring

Use the **set mirror vlan** command to assign a VLAN to be reserved for mirroring. If a mirrored VLAN is created, all mirrored traffic will egress VLAN tagged. All traffic on the mirror VLAN will be flooded

Use the **show port mirroring** command to display the VLANs configured for remote port mirroring.

Use the **clear mirror vlan** command to clear the VLAN to be reserved for mirroring traffic.

The following example assigns a VLAN for mirroring traffic and then shows the configured port mirroring with the **show port mirror** command.

```
C5(su)->set mirror vlan 2

C5(su)->show port mirroring
Port Mirroring
=====
Source Port = ge.1.1
Target Port = ge.1.10
Frames Mirrored = Rx and Tx
Port Mirroring status enabled

Mirror Vlan = 2
```

## Configuring SMON MIB Port Mirroring

SMON port mirroring support allows you to redirect traffic on ports remotely using SMON MIBs. This is useful for troubleshooting or problem solving when network management through the console port, telnet, or SSH is not feasible.

### Procedures

Perform the following steps to configure and monitor port mirroring using SMON MIB objects.

To create and enable a port mirroring instance:

1. Open a MIB browser, such as Netsight MIB Tools
2. In the MIB directory tree, navigate to the **portCopyEntry** folder and expand it.
3. Select the **portCopyStatus** MIB.
4. Enter a desired source and target port in the **Instance** field using the format *source.target*.

For example, 3.2 would create a relationship where source port ge.1.3 would be mirrored to target port ge.1.2.



**Note:** In order to configure a port mirroring relationship, both source and destination interfaces must be enabled and operational (up).

5. Enter MIB option **4** (createAndGo) and perform an SNMP **Set** operation.
6. (Optional) Use the CLI to verify the port mirroring instance has been created and enabled as shown in the following example:

```
C5(su)->show port mirroring
Port Mirroring
=====
Source Port = ge.1.3
Target Port = ge.1.2
Frames Mirrored = Rx and Tx
Port Mirroring status enabled
```

To create a port mirroring instance without automatically enabling it:

1. Complete steps 1-4 above.
2. Enter MIB option **5** (createAndWait) and perform an SNMP **Set** operation.
3. (Optional) Use the CLI to verify the port mirroring instance has been created set to disabled mode as shown in the following example:

```
C5(su)->show port mirroring
Port Mirroring
=====
Source Port = ge.1.3
Target Port = ge.1.2
Frames Mirrored = Rx and Tx
Port Mirroring status disabled
```

4. When you are ready to enable this instance, enter MIB option **1** (active) and perform an SNMP **Set** operation.
5. (Optional) Use the CLI to verify the port mirroring instance has been enabled.

To delete a port mirroring instance:

1. Select a previously created port mirroring instance in your MIB browser.

2. Enter MIB option **6** (destroy) and perform an SNMP **Set** operation.
3. (Optional) Use the CLI to verify the port mirroring instance has been deleted as shown in the following example:

```
C5(su)->show port mirroring
No Port Mirrors configured.
```

## Configuring VLANs

This chapter describes how to configure VLANs on Enterasys fixed stackable and standalone switches.

| For information about...                           | Refer to page... |
|----------------------------------------------------|------------------|
| <a href="#">VLAN Overview</a>                      | 9-1              |
| <a href="#">Implementing VLANs</a>                 | 9-2              |
| <a href="#">Understanding How VLANs Operate</a>    | 9-3              |
| <a href="#">VLAN Support on Enterasys Switches</a> | 9-6              |
| <a href="#">Configuring VLANs</a>                  | 9-8              |
| <a href="#">Terms and Definitions</a>              | 9-14             |

### VLAN Overview

A VLAN is a Virtual Local Area Network — a grouping of network devices that is logically segmented by functions, project teams, or applications without regard to the physical location of users. For example, several end stations might be grouped as a department, such as Engineering or Finance, having the same attributes as a LAN, even though they are not all on the same physical LAN segment.

To accomplish this logical grouping, the network administrator uses 802.1Q VLAN-capable switching devices and assigns each switch port in a particular group to a VLAN. Ports in a VLAN share broadcast traffic and belong to the same broadcast domain. Broadcast traffic in one VLAN is not transmitted outside that VLAN.

### Using VLANs to Partition Your Network

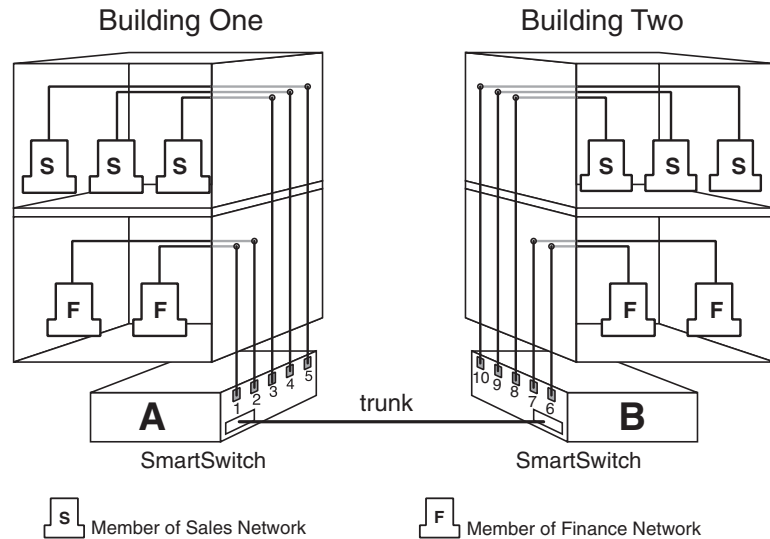
Virtual LANs allow you to partition network traffic into logical groups and control the flow of that traffic through the network. Once the traffic and, in effect, the users creating the traffic, are assigned to a VLAN, then broadcast and multicast traffic is contained within the VLAN and users can be allowed or denied access to any of the network's resources. Also, you have the option of configuring some or all of the ports on a device to allow frames received with a particular VLAN ID and protocol to be transmitted on a limited number of ports. This keeps the traffic associated with a particular VLAN and protocol isolated from the other parts of the network.

The primary benefit of 802.1Q VLAN technology is that it allows you to localize and segregate traffic, improving your administrative efficiency, and enhancing your network security and performance.

[Figure 9-1](#) shows a simple example of using port-based VLANs to achieve these benefits. In this example, two buildings house the Sales and Finance departments of a single company, and each

building has its own internal network. The end stations in each building connect to a switch on the bottom floor. The two switches are connected to one another with a high speed link.

**Figure 9-1 VLAN Business Scenario**



2263-01

Without any VLANs configured, the entire network in the example in [Figure 9-1](#) would be a broadcast domain, and the switches would follow the IEEE 802.1D bridging specification to send data between stations. A broadcast or multicast transmission from a Sales workstation in Building One would propagate to all the switch ports on Switch A, cross the high speed link to Switch B, and then be propagated out all switch ports on Switch B. The switches treat each port as being equivalent to any other port, and have no understanding of the departmental memberships of each workstation.

Once Sales and Finance are placed on two separate VLANs, each switch understands that certain individual ports or frames are members of separate workgroups. In this environment, a broadcast or multicast data transmission from one of the Sales stations in Building One would reach Switch A, be sent to the ports connected to other local members of the Sales VLAN, cross the high speed link to Switch B, and then be sent to any other ports and workstations on Switch B that are members of the Sales VLAN. Separate VLANs also provides unicast separation between Sales and Finance. Finance cannot ping Sales unless there is a routed VLAN configured for both Finance and Sales.

Another benefit to VLAN use in the preceding example would be your ability to leverage existing investments in time and equipment during company reorganization. If, for instance, the Finance users change location but remain in the same VLAN connected to the same switch port, their network addresses do not change, and switch and router configuration is left intact.

## Implementing VLANs

By default, all Enterasys switches run in 802.1Q VLAN operational mode. All ports on all Enterasys switches are assigned to a default VLAN (VLAN ID 1), which is enabled to operate and assigns all ports an egress status of untagged. This means that all ports will be allowed to transmit frames from the switch without a VLAN tag in their header. Also, there are no forbidden ports (prevented from transmitting frames) configured.

You can use the CLI commands described in this document to create additional VLANs, to customize VLANs to support your organizational requirements, and to monitor VLAN configuration.

## Preparing for VLAN Configuration

A little forethought and planning is essential to a successful VLAN implementation. Before attempting to configure a single device for VLAN operation, consider the following:

- What is the purpose of my VLAN design? (For example: security or traffic broadcast containment).
- How many VLANs will be required?
- What stations (end users, servers, etc.) will belong to them?
- What ports on the switch are connected to those stations?
- What ports will be configured as GARP VLAN Registration Protocol (GVRP) aware ports?

Determining how you want information to flow and how your network resources can be best used to accomplish this will help you customize the tasks described in this document to suit your needs and infrastructure.

Once your planning is complete, you would proceed through the steps described in “[Configuring VLANs](#)” on page 9-8.

## Understanding How VLANs Operate

802.1Q VLAN operation differs slightly from how a switched networking system operates. These differences are due to the importance of keeping track of each frame and its VLAN association as it passes from switch to switch, or from port to port within a switch.

VLAN-enabled switches act on how frames are classified into a particular VLAN. Sometimes, VLAN classification is based on tags in the headers of data frames. These VLAN tags are added to data frames by the switch as the frames are transmitted out certain ports, and are later used to make forwarding decisions by the switch and other VLAN aware switches. In the absence of a VLAN tag header, the classification of a frame into a particular VLAN depends upon the configuration of the switch port that received the frame.

| For information about...                               | Refer to page... |
|--------------------------------------------------------|------------------|
| <a href="#">Learning Modes and Filtering Databases</a> | 9-3              |
| <a href="#">VLAN Assignment and Forwarding</a>         | 9-4              |
| <a href="#">Example of a VLAN Switch in Operation</a>  | 9-5              |

## Learning Modes and Filtering Databases

Addressing information the switch learns about a VLAN is stored in the filtering database assigned to that VLAN. This database contains source addresses, their source ports, and VLAN IDs, and is referred to when a switch makes a decision as to where to forward a VLAN tagged frame. Each filtering database is assigned a Filtering Database ID (FID). The FID a VLAN belongs to can be displayed using the **show vlan** command.

A switch learns and uses VLAN addressing information by the following modes:

- **Independent Virtual Local Area Network (VLAN) Learning (IVL):** Each VLAN uses its own filtering database. Transparent source address learning performed as a result of incoming VLAN traffic is not made available to any other VLAN for forwarding purposes. This setting is useful for handling devices (such as servers) with NICs that share a common MAC address. One FID is assigned per VLAN. The FID value is the same as the VID it is assigned to. This is the default mode on Enterasys switches.

- **Shared Virtual Local Area Network (VLAN) Learning (SVL):** Two or more VLANs are grouped to share common source address information. This setting is useful for configuring more complex VLAN traffic patterns, without forcing the switch to flood the unicast traffic in each direction. This allows VLANs to share addressing information. It enables ports or switches in different VLANs to communicate with each other (when their individual ports are configured to allow this to occur). One FID is used by two or more VLANs. The FID value defaults to the lowest VID in the filtering database.



**Note:** SVL is not supported on the stackable and standalone fixed switches.

See “Appendix F” of the *IEEE Std 802.1Q™2011* standard for a detailed discussion of shared and independent VLAN learning modes.

## VLAN Assignment and Forwarding

### Receiving Frames from VLAN Ports

By default, Enterasys switches run in 802.1Q operational mode, which means that every frame received by the switch must belong to, or be assigned to, a VLAN. The type of frame under consideration and the filter setting of the switch determines how it forwards VLAN frames. This involves processing traffic as it enters (ingresses) and exits (egresses) the VLAN switch ports as described below.

#### Untagged Frames

When, for example, the switch receives a frame from Port 1 and determines the frame does not currently have a VLAN tag, but recognizes that Port 1 is a member of VLAN A, it will classify the frame to VLAN A. In this fashion, all untagged frames entering a VLAN switch assume membership in a VLAN.



**Note:** A VLAN ID is always assigned to a port. By default, it is the default VLAN (VLAN ID = 1).

The switch will now decide what to do with the frame, as described in “[Forwarding Decisions](#)” on page 9-5.

#### Tagged Frames

When, for example, the switch receives a tagged frame from Port 4 and determines the frame is tagged for VLAN C, it will classify it to that VLAN regardless of its port VLAN ID (PVID). This frame may have already been through a VLAN aware switch, or originated from a station capable of specifying a VLAN membership. If a switch receives a frame containing a tag, the switch will classify the frame in regard to its tag rather than the PVID for its port, following the ingress precedence rules listed below.

#### Ingress Precedence

VLAN assignment for received (ingress) frames is determined by the following precedence:

1. 802.1Q VLAN tag (tagged frames only).
2. Policy or Traffic Classification (which may overwrite the 802.1Q VLAN tag). For more information, refer to “[Configuring Protocol-Based VLAN Classification](#)” on page 9-13.
3. Port VLAN ID (PVID).



## Forwarding Decisions

VLAN forwarding decisions for transmitting frames is determined by whether or not the traffic being classified is or is not in the VLAN's forwarding database as follows:

- **Unlearned traffic:** When a frame's destination MAC address is not in the VLAN's forwarding database (FDB), it will be forwarded out of every port on the VLAN's egress list with the frame format that is specified. Refer to "[Broadcasts, Multicasts, and Unlearned Unicasts](#)" below for an example.
- **Learned traffic:** When a frame's destination MAC address is in the VLAN's forwarding database, it will be forwarded out of the learned port with the frame format that is specified. Refer to "[Learned Unicasts](#)" below for an example.

### Broadcasts, Multicasts, and Unlearned Unicasts

If a frame with a broadcast, multicast, or other unknown address is received by an 802.1Q VLAN aware switch, the switch checks the VLAN classification of the frame. The switch then forwards the frame out all ports that are identified in the Forwarding List for that VLAN. For example, if Port 3, shown in the example in [Figure 9-2](#), received the frame, the frame would then be sent to all ports that had VLAN 30 in their Port VLAN List.

### Learned Unicasts

When a VLAN switch receives a frame with a known MAC address as its destination address, the action taken by the switch to determine how the frame is transmitted depends on the VLAN, the VLAN associated FID, and if the port identified to send the frame is enabled to do so.

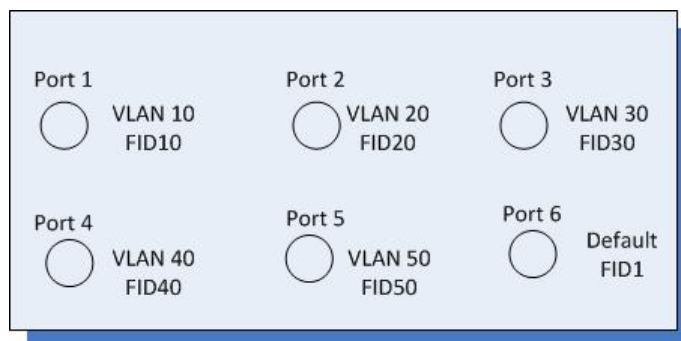
When a frame is received, it is classified into a VLAN. The destination address is looked up in the FID associated with the VLAN. If a match is found, it is forwarded out the port identified in the lookup if, and only if, that port is allowed to transmit frames for that VLAN. If a match is not found, then the frame is flooded out all ports that are allowed to transmit frames belonging to that VLAN.

## Example of a VLAN Switch in Operation

The operation of an 802.1Q VLAN switch is best understood from a point of view of the switch itself. To illustrate this concept, the examples that follow view the switch operations from *inside* the switch.

[Figure 9-2](#) shows the inside of a switch with six ports, numbered 1 through 6. The switch associates VLAN 10 with FID 10, VLAN 20 with FID 20, VLAN 30 with FID 30, VLAN 40 with FID 40, and VLAN 50 with FID 50. It shows how a forwarding decision is made by comparing a frame's destination MAC to the FID to which it is classified.

**Figure 9-2 Inside the Switch**



If a unicast untagged frame is received on Port 5, it would be classified for VLAN 50. Port 5 has its own filtering database and is not aware of what addressing information has been learned by other VLANs. Port 5 looks up the destination MAC address in its FID. If it finds a match, it forwards the frame out the appropriate port, if and only if, that port is allowed to transmit frames for VLAN 50. If a match is not found, the frame is flooded out all ports that are allowed to transmit VLAN 50 frames.

## VLAN Support on Enterasys Switches

### Maximum Active VLANs

The total number of active VLANs supported on Enterasys stackable and standalone fixed switches is up to 1024.

### Configurable Range

The allowable user-configurable range for VLAN IDs (VIDs) is from 2 through 4094. This range is based on the following rules:

- **VID 0** is the null VLAN ID, indicating that the tag header in the frame contains priority information rather than a VLAN identifier. It cannot be configured as a port VLAN ID (PVID).
- **VID 1** is designated the default PVID value for classifying frames on ingress through a switched port. This default can be changed on a per-port basis.
- **VID 4095** is reserved by IEEE for implementation use.



**Notes:** Each VLAN ID in a network must be unique. If you enter a duplicate VLAN ID, the Enterasys switch assumes you intend to modify the existing VLAN.

### VLAN Types

Enterasys switches support traffic classification for the following VLAN types.

#### Static and Dynamic VLANs

All VLANs on an Enterasys switch are categorized as being either static or dynamic. Static VLANs are those that are explicitly created on the switch itself, persistently remaining as part of the configuration, regardless of actual usage. Dynamic VLANs, on the other hand, are not necessarily persistent. Their presence relies on the implementation of GVRP and its effect on egress membership as described in [“GARP VLAN Registration Protocol \(GVRP\) Support”](#) on page 9-7.

#### Port-Based VLANs

Port-based VLANs are configured by associating switch ports to VLANs in two ways: first, by manipulating the port VLAN ID (PVID); and second, by adding the port itself to the egress list of the VLAN corresponding to the PVID. Any traffic received by a port is associated to the VLAN identified by the port's PVID. By virtue of this association, this traffic may egress the switch only on those ports listed on the VLAN's egress list. For example, given a VLAN named “Marketing,” with an ID value of 6, by changing the PVID values of ports 1 through 3 to 6, and adding those ports to the egress list of the VLAN, we effectively restrict the broadcast domain of Marketing to those three ports. If a broadcast frame is received on port 1, it will be transmitted out ports 2 and 3 only. In this sense, VLAN membership is determined by the location of traffic ingress, and from

the perspective of the access layer — where users are most commonly located — egress is generally untagged.

## Policy-Based VLANs

Rather than making VLAN membership decisions simply based on port configuration, each incoming frame can be examined by the classification engine which uses a match-based logic to assign the frame to a desired VLAN. For example, you could set up a policy which designates all e-mail traffic between the management officers of a company to a specific VLAN so that this traffic is restricted to certain portions of the network. With respect to network usage, the administrative advantages of policy classification would be application provisioning, acceptable use policy, and distribution layer policy. All of these provisions may involve simultaneous utilization of inter-switch links by multiple VLANs, requiring particular attention to tagged, forbidden, and untagged egress settings.

As described above, PVID determines the VLAN to which all untagged frames received on associated ports will be classified. Policy classification to a VLAN takes precedence over PVID assignment if:

- policy classification is configured to a VLAN, and
- PVID override has been enabled for a policy profile, and assigned to port(s) associated with the PVID.

For more information, refer to [Chapter 16, Configuring Policy](#) in this manual.

## GARP VLAN Registration Protocol (GVRP) Support

The purpose of the GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol (GVRP) is to dynamically create VLANs across a switched network. GVRP allows GVRP-aware devices to dynamically establish and update their knowledge of the set of VLANs that currently have active members.

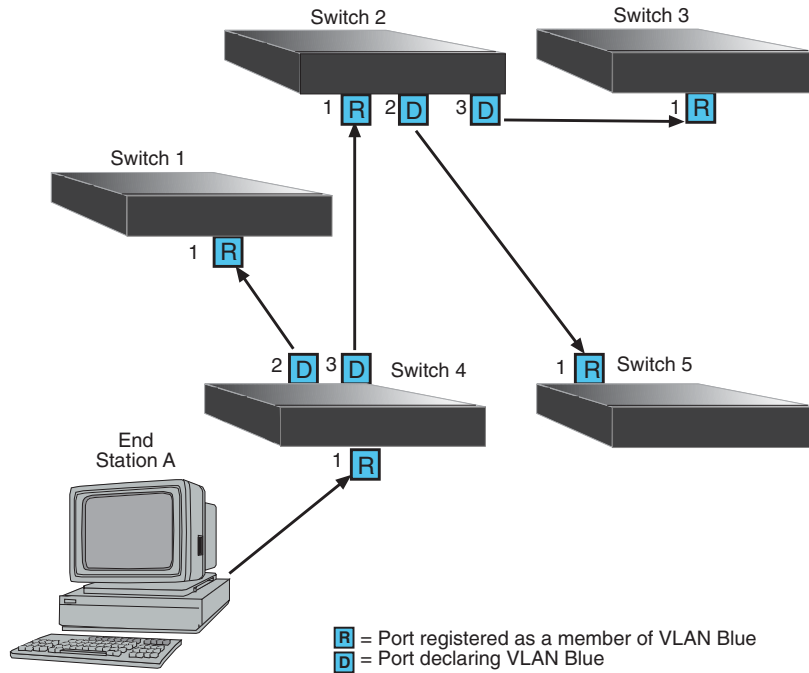
By default, GVRP is globally enabled but disabled at the port level on all Enterasys devices except the N-Series. On the N-Series, GVRP is enabled globally and at the port level. To allow GVRP to dynamically create VLANs, it must be enabled globally and also on each individual port as described in “[Configuring Dynamic VLANs](#)” on page 9-12.

### How It Works

When a VLAN is declared, the information is transmitted out GVRP configured ports on the device in a GARP formatted frame using the GVRP multicast MAC address. A switch that receives this frame examines the frame and extracts the VLAN IDs. GVRP then dynamically registers (creates) the VLANs and adds the receiving port to its tagged member list for the extracted VLAN IDs. The information is then transmitted out the other GVRP configured ports of the device.

[Figure 9-3](#) on page 9-8 shows an example of how VLAN Blue from end station A would be propagated across a switch network. In this figure, port 1 of Switch 4 is registered as being a member of VLAN Blue and Switch 4 declares this fact out all its ports (2 and 3) to Switch 1 and Switch 2. These two switches register this in the port egress lists of the ports (Switch 1, port 1 and Switch 2, port 1) that received the frames with the information. Switch 2, which is connected to Switch 3 and Switch 5 declares the same information to those two switches and the port egress list of each port is updated with the new information, accordingly.

**Figure 9-3 Example of VLAN Propagation Using GVRP**



**Note:** If a port is set to “forbidden” for the egress list of a VLAN, then the VLAN’s egress list will not be dynamically updated with that port.

Administratively configuring a VLAN on an 802.1Q switch creates a static VLAN entry that will always remain registered and will not time out. However, GVRP-created dynamic entries will time out, and their registrations will be removed from the member list if the end station is removed. This ensures that, if switches are disconnected or if end stations are removed, the registered information remains accurate.

The end result of GVRP dynamic VLAN configuration is that each port’s egress list is updated with information about VLANs that reside on that port, even if the actual station on the VLAN is several hops away.

## Configuring VLANs

Once you have planned your implementation strategy as described in “[Preparing for VLAN Configuration](#)” on page 9-3, you can begin configuring VLANs as described in this section.

| For information about...                                       | Refer to page... |
|----------------------------------------------------------------|------------------|
| <a href="#">Default Settings</a>                               | 9-9              |
| <a href="#">Configuring Static VLANs</a>                       | 9-9              |
| <a href="#">Creating a Secure Management VLAN</a>              | 9-11             |
| <a href="#">Configuring Dynamic VLANs</a>                      | 9-12             |
| <a href="#">Configuring Protocol-Based VLAN Classification</a> | 9-13             |
| <a href="#">Monitoring VLANs</a>                               | 9-14             |

## Default Settings

Table 9-1 lists VLAN parameters and their default values.

**Table 9-1 Default VLAN Parameters**

| Parameter           | Description                                                                                                                                                                                       | Default Value                                                                                                                                                  |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| garp timers         | Configures the three GARP timers. The setting is critical and should only be done by someone familiar with the 802.1Q standard.                                                                   | <ul style="list-style-type: none"> <li>Join timer: 20 centiseconds</li> <li>Leave timer: 60 centiseconds</li> <li>Leaveall timer: 1000 centiseconds</li> </ul> |
| GVRP                | Enables or disables the GARP VLAN Registration Protocol (GVRP) on a specific set of ports or all ports. GVRP must be enabled to allow creation of dynamic VLANs.                                  | <ul style="list-style-type: none"> <li>Disabled at the port level</li> <li>Enabled at the global level</li> </ul>                                              |
| port discard        | Ports can be set to discard frames based on whether or not they contain a VLAN tag.                                                                                                               | No frames are discarded                                                                                                                                        |
| port ingress filter | When enabled on a port, the VLAN IDs of incoming frames are compared to the port's egress list. If the received VLAN ID does not match a VLAN ID on the port's egress list, the frame is dropped. | Disabled                                                                                                                                                       |
| port vlan ID (PVID) | 802.1Q VLAN/port association.                                                                                                                                                                     | VLAN1/ Default VLAN                                                                                                                                            |
| vlan dynamic egress | Enables or disables dynamic egress processing for a given VLAN.                                                                                                                                   | Disabled                                                                                                                                                       |
| vlan egress         | Configures the egress ports for a VLAN and the type of egress for the ports. Egress type can be tagged, untagged, or forbidden.                                                                   | Tagged                                                                                                                                                         |
| vlan name           | Associates a text name to one or more VLANs.                                                                                                                                                      | None                                                                                                                                                           |


## Configuring Static VLANs

Procedure 9-1 describes how to create and configure a static VLAN. Unspecified parameters use their default values.

**Procedure 9-1 Static VLAN Configuration**

| Step | Task                                                                                                                                                            | Command(s)                                 |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| 1.   | Show existing VLANs.                                                                                                                                            | <b>show vlan</b>                           |
| 2.   | Create VLAN.<br>VLAN ids can range from 2 to 4094. Each <i>vlan-id</i> must be unique. If an existing <i>vlan-id</i> is entered, the existing VLAN is modified. | <b>set vlan create <i>vlan-id</i></b>      |
| 3.   | Optionally, assign a name to the VLAN.<br>Valid strings are from 1 to 32 characters.                                                                            | <b>set vlan name <i>vlan-id string</i></b> |

**Procedure 9-1 Static VLAN Configuration (continued)**

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Command(s)                                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.   | <p>Assign switch ports to the VLAN. This sets the port VLAN ID (PVID). The PVID determines the VLAN to which all untagged frames received on the port will be classified.</p> <p>Optionally, specify whether or not the ports should be added to the VLAN's untagged egress list and removed from other untagged egress lists.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <pre>set port vlan port-string vlan-id [modify-egress   no-modify-egress]</pre>                                                                                                                            |
|      | <p> <b>Note:</b> If the VLAN specified has not already been created, the <b>set port vlan</b> command will create it. It will also add the VLAN to the port's egress list as untagged, and remove the default VLAN from the port's egress list. This automatically changes the existing untagged VLAN egress permission to match the new PVID value.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                            |
| 5.   | <p>If necessary, configure VLAN egress, which determines which ports a frame belonging to the VLAN may be forwarded out on.</p> <p><b>Static configuration:</b><br/>Add the port to the VLAN egress list for the device.</p> <ul style="list-style-type: none"> <li>• The default setting, <b>tagged</b>, allows the port to transmit frames for a particular VLAN.</li> <li>• The <b>untagged</b> setting allows the port to transmit frames without a VLAN tag. This setting is usually used to configure a port connected to an end user device.</li> <li>• The <b>forbidden</b> setting prevents the port from participating in the specified VLAN and ensures that any dynamic requests for the port to join the VLAN will be ignored.</li> </ul> <p>If necessary, remove ports from the VLAN egress list.</p> <ul style="list-style-type: none"> <li>• If specified, the <b>forbidden</b> setting will be cleared from the designated ports and the ports will be reset as allowed to egress frames, if so configured by either static or dynamic means.</li> <li>• If <b>forbidden</b> is not specified, tagged and untagged egress settings will be cleared from the designated ports.</li> </ul> <p><b>Dynamic configuration:</b><br/>By default, dynamic egress is disabled on all VLANs. If dynamic egress is enabled for a VLAN, the device will add the port receiving a frame to the VLAN's egress list as untagged according to the VLAN ID of the received frame.</p> | <pre>set vlan egress vlan-id port- string forbidden   tagged   untagged</pre> <pre>clear vlan egress vlan-list port- string [forbidden]</pre> <pre>set vlan dynamicegress vlan-id {enable   disable}</pre> |
| 6.   | <p>Optionally, enable ingress filtering on a port to drop those incoming frames that do not have a VLAN ID that matches a VLAN ID on the port's egress list.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <pre>set port ingress-filter port- string enable</pre>                                                                                                                                                     |

**Procedure 9-1 Static VLAN Configuration (continued)**

| Step | Task                                                                                                                                          | Command(s)                                                                                                                         |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| 7.   | Optionally, choose to discard tagged or untagged, (or both) frames on selected ports. Select <b>none</b> to allow all frames to pass through. | <code>set port discard port-string {tagged   untagged   none   both}</code>                                                        |
| 8.   | If the device supports routing, enter router configuration mode and configure an IP address on the VLAN interface.                            | <code>router<br/>enable<br/>configure terminal<br/>interface vlan vlan_id<br/>ip address ip-address ip-mask<br/>no shutdown</code> |



**Note:** Each VLAN interface must be configured for routing separately using the interface command shown above. To end configuration on one interface before configuring another, type **exit** at the command prompt. Enabling interface configuration mode is required for completing interface-specific configuration tasks.

**Example Configuration**

The following shows an example configuration using the steps in [Procedure 9-1](#). In this example, VLAN 100 is created and named VLANRED. Ports ge.1.2, 1.3 and 1.4 are assigned to VLAN 100 and added to its egress list. VLAN 100 is then configured as a routing interface with an IP address of 120.20.20.24.

```
C5(su)->set vlan create 100
C5(su)->set vlan name 100 VLANRED
C5(su)->set port vlan ge.1.2-4 100
```

```
The PVID is used to classify untagged frames as they
ingress into a given port. Would you like to add the selected
port(s) to this VLAN's untagged egress list and remove them
from all other VLANs untagged egress list (y/n) [n]?
NOTE: Choosing 'y' will not remove the port(s) from previously
configured tagged egress lists.
```

y

```
C5(su)->router
C5(su)->router>enable
C5(su)->router#configure
Enter configuration commands:
C5->(su)->router(Config)#
C5->(su)->router(Config)#interface vlan 100
C5->(su)->router(Config-if(Vlan 100))#ip address 120.20.20.1 255.255.255.0
C5->(su)->router(Config-if(Vlan 100))#no shutdown
```

If you want to configure a port to drop incoming frames that do not have a VLAN ID that matches a VLAN ID on the port's egress list, use the **set port ingress-filter** command. For example:

```
C5(su)->set port ingress-filter ge.1.2-4 enable
```

If you want to configure a port to discard tagged or untagged incoming frames, use the **set port discard** command. For example, to configure the ports to drop tagged frames on ingress:

```
C5(su)->set port discard ge.1.2-4 tagged
```

**Creating a Secure Management VLAN**

If you are configuring an Enterasys device for multiple VLANs, it may be desirable to configure a management-only VLAN. This allows a station connected to the management VLAN to manage



the device. It also makes management secure by preventing configuration through ports assigned to other VLANs.

**Procedure 9-2** provides an example of how to create a secure management VLAN. This example, which sets the new VLAN as VLAN 2, assumes the management station is attached to ge.1.1, and wants untagged frames. The process described in this section would be repeated on every device that is connected in the network to ensure that each device has a secure management VLAN.

### Procedure 9-2 Secure Management VLAN Configuration

| Step | Task                                                                                                                                                                                              | Command(s)                                                                                |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| 1.   | Create a new VLAN.                                                                                                                                                                                | <code>set vlan create 2</code>                                                            |
| 2.   | Set the PVID for the host port and the desired switch port to the VLAN created in Step 2.                                                                                                         | <code>set port vlan ge.1.1 2</code>                                                       |
| 3.   | If not done automatically when executing the previous command, add the host port and desired switch port(s) to the new VLAN's egress list and remove the port from the default VLANs egress list. | <code>set vlan egress 2 ge.1.1 untagged</code><br><code>clear vlan egress 1 ge.1.1</code> |
| 4.   | Assign host status to the VLAN.                                                                                                                                                                   | <code>set host vlan 2</code>                                                              |
| 5.   | Set a private community name to assign to this VLAN for which you can configure access rights and policies.                                                                                       | <code>set snmp community private</code>                                                   |



**Note:** By default, community name—which determines remote access for SNMP management—is set to **public** with read-write access. For more information, refer to your device's SNMP documentation.

## Configuring Dynamic VLANs

**Procedure 9-3** describes how to enable the GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol (GVRP), which is needed to create dynamic VLANs. By default, GVRP is enabled globally but disabled at the port level. GVRP must be globally enabled and also enabled on specific ports in order to generate and process GVRP advertisement frames.



**Note:** Refer to “[GARP VLAN Registration Protocol \(GVRP\) Support](#)” on page 9-7 for conceptual information about GVRP.

### Procedure 9-3 Dynamic VLAN Configuration

| Step | Task                                                                                                                                                                                | Command(s)                                        |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| 1.   | Show existing GVRP configuration for a port or list of ports.<br>If no <i>port-string</i> is entered, the global GVRP configuration and all port GVRP configurations are displayed. | <code>show gvrp [<i>port-string</i>]</code>       |
| 2.   | If necessary, enable GVRP on those ports assigned to a VLAN. You must specifically enable GVRP on ports, since it is disabled on ports by default.                                  | <code>set gvrp enable <i>port-string</i></code>   |
| 3.   | Display the existing GARP timer values.                                                                                                                                             | <code>show garp timer [<i>port-string</i>]</code> |



**Procedure 9-3 Dynamic VLAN Configuration (continued)**

| Step | Task                                                                                                  | Command(s)                                                                                              |
|------|-------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| 4.   | Optionally, set the GARP join, leave, and leaveall timer values. Each timer value is in centiseconds. | <code>set garp timer {[join timer-value] [leave timer-value] [leaveall timer-value]} port-string</code> |



**Caution:** The setting of GARP timers is critical and should only be changed by personnel familiar with 802.1Q standards.

## Configuring Protocol-Based VLAN Classification

Protocol-based VLANs can be configured using the policy classification CLI commands, as shown in this section, or by using NetSight Policy Manager.

[Procedure 9-4](#) describes how to define protocol-based frame filtering policies to assign frames to particular VLANs. Refer to [Chapter 16, Configuring Policy](#) for more information.

**Procedure 9-4 Configuring Protocol-Based VLAN Classification**

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                              | Command(s)                                                                                                  |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| 1.   | Create the VLANs to which frames will be assigned by the policy. Valid values are <b>2–4094</b> .                                                                                                                                                                                                                                                                                                                                                 | <code>set vlan create vlan-id</code>                                                                        |
| 2.   | Configure VLAN egress, which determines which ports a frame belonging to the VLAN may be forwarded out on.<br>The default setting, <b>tagged</b> , allows the port to transmit frames for a particular VLAN.                                                                                                                                                                                                                                      | <code>set vlan egress vlan-id port-string [forbidden   tagged   untagged]</code>                            |
| 3.   | Disable ingress filtering on the ingress ports on which the policy will be applied. Disabled is the default ingress filtering setting.                                                                                                                                                                                                                                                                                                            | <code>set port ingress-filter port-string disable</code>                                                    |
| 4.   | Create the policy profile that enables PVID override. This function allows a policy rule classifying a frame to a VLAN to override PVID assignment configured with the <b>set port vlan</b> command.<br>When none of its associated classification rules match, the configuration of the policy profile itself will determine how frames are handled by default. In this case, the default VLAN is specified with the <b>pvid pvid</b> parameter. | <code>set policy profile profile-index [name name] [pvid-status {enable   disable}] [pvid pvid]</code>      |
| 5.   | Configure the administrative rules that will assign the policy profile to all frames received on the desired ingress ports.                                                                                                                                                                                                                                                                                                                       | <code>set policy rule admin-profile port port-string [port-string port-string] [admin-pid admin-pid]</code> |
| 6.   | Configure the classification rules that will define the protocol to filter on and the VLAN ID to which matching frames will be assigned.                                                                                                                                                                                                                                                                                                          | <code>set policy rule profile-index {protocol data [mask mask]} [vlan vlan]</code>                          |

### Example Configuration

This example configures a policy that ensures that IP traffic received on the specified ingress ports will be mapped to VLAN 2, while all other types of traffic will be mapped to VLAN 3.

- Two VLANs are created: VLAN 2 and VLAN 3.

2. Ports 1 through 5 on the switch unit 4 are configured as egress ports for the VLANs while ports 8 through 10 on the switch unit 5 are configured as ingress ports that will do the policy classification.
3. Policy profile number 1 is created that enables PVID override and defines the default behavior (classify to VLAN 3) if none of the classification rules created for the profile are matched.
4. Classification rules are created for policy profile number 1 that assign IP frames to VLAN 2. The rules identify IP frames by using the **ether** protocol parameter, which classifies on the Type field in the headers of Layer 2 Ethernet II frames, and the protocol data of 0x0800 (IP type), 0x0806 (ARP type), and 0x8035 (RARP type).
5. Policy profile 1 is assigned to ports ge.5.8 through ge.5.10.

```
C5(su)->set vlan create 2-3
C5(su)->set vlan egress 2 ge.4.1-2
C5(su)->set vlan egress 3 ge.4.3-5
C5(su)->set port ingress-filter ge.5.8-10 disable
C5(su)->set policy profile 1 name protocol_based_vlan pvid-status enable pvid 3
C5(su)->set policy rule 1 ether 0x0800 mask 16 vlan 2
C5(su)->set policy rule 1 ether 0x0806 mask 16 vlan 2
C5(su)->set policy rule 1 ether 0x8035 mask 16 vlan 2
C5(su)->set policy port ge.5.8-10 1
```

## Monitoring VLANs

[Table 9-2](#) describes the **show** commands that display information about VLAN configurations. Refer to your device’s CLI documentation for a description of the output of each show command.

**Table 9-2 Displaying VLAN Information**

| Task                                     | Command                                   |
|------------------------------------------|-------------------------------------------|
| Display all existing VLANs.              | <b>show vlan</b>                          |
| Display the VLAN dynamic egress setting. | <b>show vlan dynamic</b> egress [vlan id] |
| Display all static VLANs.                | <b>show vlan static</b>                   |
| Display ports assigned to VLANs.         | <b>show port vlan</b> [port-string]       |
| Display existing GVRP settings.          | <b>show gvrp</b> [port-string]            |

## Terms and Definitions

[Table 9-3](#) lists terms and definitions used in VLAN configuration.

**Table 9-3 VLAN Terms and Definitions**

| Term                                | Definition                                                                                                                                                                                                                          |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default VLAN                        | The VLAN to which all ports are assigned upon initialization. The default VLAN has a VLAN ID of 1 and cannot be deleted or renamed.                                                                                                 |
| Filtering Database                  | A database structure within the switch that keeps track of the associations between MAC addresses, VLANs, and interface (port) numbers. The Filtering Database is referred to when a switch makes a forwarding decision on a frame. |
| Filtering Database Identifier (FID) | Addressing information that the device learns about a VLAN is stored in the filtering database assigned to that VLAN. On the fixed switches, each VLAN has its own FID and FID = VID.                                               |

**Table 9-3 VLAN Terms and Definitions (continued)**

| <b>Term</b>                                    | <b>Definition</b>                                                                                                                                                                                                                                                                   |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Forwarding List                                | A list of the ports on a particular device that are eligible to transmit frames for a selected VLAN.                                                                                                                                                                                |
| GARP Multicast Registration Protocol (GMRP)    | A GARP application that functions in a similar fashion as GVRP, except that GMRP registers multicast addresses on ports to control the flooding of multicast frames.                                                                                                                |
| GARP VLAN Registration Protocol (GVRP)         | A GARP application used to dynamically create VLANs across a switched network.                                                                                                                                                                                                      |
| Generic Attribute Registration Protocol (GARP) | GARP is a protocol used to propagate state information throughout a switched network.                                                                                                                                                                                               |
| Port VLAN List                                 | A per port list of all eligible VLANs whose frames can be forwarded out one specific port and the frame format (tagged or untagged) of transmissions for that port. The Port VLAN List specifies what VLANs are associated with a single port for frame transmission purposes.      |
| Tag Header (VLAN Tag)                          | Four bytes of data inserted in a frame that identifies the VLAN/frame classification. The Tag Header is inserted into the frame directly after the Source MAC address field. Twelve bits of the Tag Header represent the VLAN ID. The remaining bits are other control information. |
| Tagged Frame                                   | A data frame that contains a Tag Header. A VLAN aware device can add the Tag Header to any frame it transmits.                                                                                                                                                                      |
| Untagged Frame                                 | A data frame that does not have a Tag Header.                                                                                                                                                                                                                                       |
| VLAN ID                                        | A unique number (between 1 and 4094) that identifies a particular VLAN.                                                                                                                                                                                                             |
| VLAN Name                                      | A 32-character alphanumeric name associated with a VLAN ID. The VLAN Name is intended to make user-defined VLANs easier to identify and remember.                                                                                                                                   |



## Configuring User Authentication

This chapter describes the user authentication methods supported by Enterasys fixed switch platforms.

| For information about...                             | Refer to page... |
|------------------------------------------------------|------------------|
| <a href="#">User Authentication Overview</a>         | 10-1             |
| <a href="#">Configuring Authentication</a>           | 10-12            |
| <a href="#">Authentication Configuration Example</a> | 10-25            |
| <a href="#">Terms and Definitions</a>                | 10-28            |

### User Authentication Overview

Authentication is the ability of a network access server, with a database of valid users and devices, to acquire and verify the appropriate credentials of a user or device (supplicant) attempting to gain access to the network. Enterasys authentication uses the RADIUS protocol to control access to switch ports from an authentication server and to manage the message exchange between the authenticating device and the server.

Both MultiAuth and multi-user authentication are supported. MultiAuth is the ability to configure multiple authentication modes for a user and apply the authentication mode with the highest precedence. Multi-user is the ability to appropriately authenticate multiple supplicants on a single link and provision network resources, based upon an appropriate policy for each supplicant. The Enterasys fixed switch products support the following authentication methods:

- IEEE 802.1x
- MAC-based Authentication (MAC)
- Port Web Authentication (PWA)

Enterasys switch products support the configuration of up to three simultaneous authentication methods per user, with a single authentication method applied based upon MultiAuth authentication precedence.

Network resources represent a major capital investment for your organization and can be vulnerable to both undesired resource usage and malicious intent from outside users. Authentication provides you with a user validation function which assures that the supplicant requesting access has the right to do so and is a known entity. To the degree a supplicant is not a known entity, access can be denied or granted on a limited basis. The ability of authentication to both validate a user's identity and define the resources available to the user assures that valuable network resources are being used for the purposes intended by the network administrator.

## Implementing User Authentication

Take the following steps to implement user authentication:

- Determine the types of devices to be authenticated.
- Determine the correct authentication type for each device.
- Determine an appropriate policy best suited for the use of that device on your network.
- Configure RADIUS user accounts on the authentication server for each device.
- Configure user authentication.

## Authentication Methods

| For information about...                                       | Refer to page... |
|----------------------------------------------------------------|------------------|
| <a href="#">IEEE 802.1x Using EAP</a>                          | 10-2             |
| <a href="#">MAC-Based Authentication (MAC)</a>                 | 10-2             |
| <a href="#">Port Web Authentication (PWA)</a>                  | 10-3             |
| <a href="#">Multi-User And MultiAuth Authentication</a>        | 10-3             |
| <a href="#">Remote Authentication Dial-In Service (RADIUS)</a> | 10-7             |

### IEEE 802.1x Using EAP

The IEEE 802.1x port-based access control standard allows you to authenticate and authorize user access to the network at the port level. Access to the switch ports is centrally controlled from an authentication server using RADIUS. The Extensible Authentication Protocol (EAP), defined in RFC 3748, provides the means for communicating the authentication information.

There are three supported types of EAP:

- **MD5** – EAP-MD5 is a challenge-handshake protocol over EAP that authenticates the user with a normal username and password.
- **TLS** – EAP-TLS provides a transport layer security based upon the presentation and acceptance of digital certificates between the supplicant and the authentication server.
- **Protected** – Protected Extensible Authentication Protocol (PEAP) optionally authenticates the authentication server to the client using an X-509 certificate using a TLS tunnel, after which the client authentication credentials are exchanged.

All Enterasys platforms support IEEE 802.1x, which protects against unauthorized access to a network, DoS attacks, theft of services and defacement of corporate web pages.

802.1x configuration consists of setting port, global 802.1x parameters, and RADIUS parameters on the switches to point the switch to the authentication server. The Filter-ID RADIUS attribute can be configured on the authentication server to direct dynamic policy assignment on the switch to the 802.1x authenticating end system.

### MAC-Based Authentication (MAC)

MAC-based authentication (MAC) authenticates a device using the source MAC address of received packets. The authenticator sends the authentication server a source MAC address as the user name and a password that you configure on the switch. If the authentication server receives valid credentials from the switch, RADIUS returns an Accept message to the switch. MAC authentication enables switches to authenticate end systems, such as printers and camcorder

devices that do not support 802.1x or web authentication. Since MAC-based authentication authenticates the device, not the user, and is subject to MAC address spoofing attacks, it should not be considered a secure authentication method. However, it does provide a level of authentication for a device where otherwise none would be possible.

The stackable fixed switch and standalone fixed switch devices support MAC-based authentication.

## Port Web Authentication (PWA)

Port Web Authentication (PWA) authenticates a user by utilizing a web browser for the login process to authenticate to the network. To log in using PWA, a user opens the web browser requesting a URL that either directly accesses the PWA login page or is automatically redirected to the login page. At the PWA login page, the user enters a login username and password. On the switch, either the Challenge Handshake Authentication Protocol (CHAP) or the Password Authentication Protocol (PAP) verifies the username and password credentials provided to the authentication server. If the credentials are validated, the authentication server returns a RADIUS Accept message, optionally containing Filter-ID or tunnel attributes, to the switch.

PAP uses an unencrypted password. CHAP uses the password to generate a digest that is transmitted to the authentication server. If RADIUS determines that the digest matches the digest generated on the authentication server, access is granted. The acceptance message back to the switch can contain any Filter-ID attribute configured on the authentication server, allowing policy to be applied for the authenticating user.

PWA enhanced mode is supported. PWA enhanced mode allows a user on an unauthenticated PWA port to enter any URL into the browser and be presented the PWA login page on their initial web access. When enhanced mode is disabled, a user must enter the correct URL to access login.

The A4, B-Series, and C-Series stackable fixed switches, and the standalone fixed switches support PWA.



**Note:** For stackable and standalone fixed switches:

- One user per PWA-configured port can be authenticated
- PWA authentication supports RFC 3580 VLAN authorization on A4, B3, B5, C3, C5, G-Series, and I-Series devices

## Multi-User And MultiAuth Authentication

This section discusses multi-user and MultiAuth authentication. Multi-user and MultiAuth are separate concepts.

- **Multi-user authentication** refers to the ability to authenticate multiple users and devices on the same port, with each user or device being provided the appropriate level of network resources based upon policy.
- **MultiAuth authentication** refers to the ability of a single or multiple user(s), device(s), or port(s) to successfully authenticate using multiple authentication methods at the same time, such as 802.1x, PWA, and MAC, with precedence determining which authentication method is actually applied to that user, device, or port.



**Note:** Multi-user authentication is not supported on the A4 or I-Series platforms.

A limited form of multi-user authentication, called “User + IP Phone,” is supported on the A4. See “[User + IP Phone](#)” on page 10-5 for more information.

## Multi-User Authentication

Multi-user authentication provides for the per-user or per-device provisioning of network resources when authenticating. It supports the ability to receive from the authentication server:

- A policy traffic profile, based on the user account's RADIUS Filter-ID configuration
- A base VLAN-ID, based on the RFC 3580 tunnel attributes configuration, also known as dynamic VLAN assignment

When a single supplicant connected to an access layer port authenticates, a policy profile can be dynamically applied to all traffic on the port. When multi-user authentication is not implemented, and more than one supplicant is connected to a port, firmware does not provision network resources on a per-user or per-device basis. Different users or devices may require a different set of network resources. The firmware tracks the source MAC address for each authenticating user regardless of the authenticating protocol being used. Provisioning network resources on a per-user basis is accomplished by applying the policy configured in the RADIUS Filter-ID, or the base VLAN-ID configured in the RFC 3580 tunnel attributes, for a given user's MAC address. The RADIUS Filter-ID and tunnel attributes are part of the RADIUS user account and are included in the RADIUS Accept message response from the authentication server.

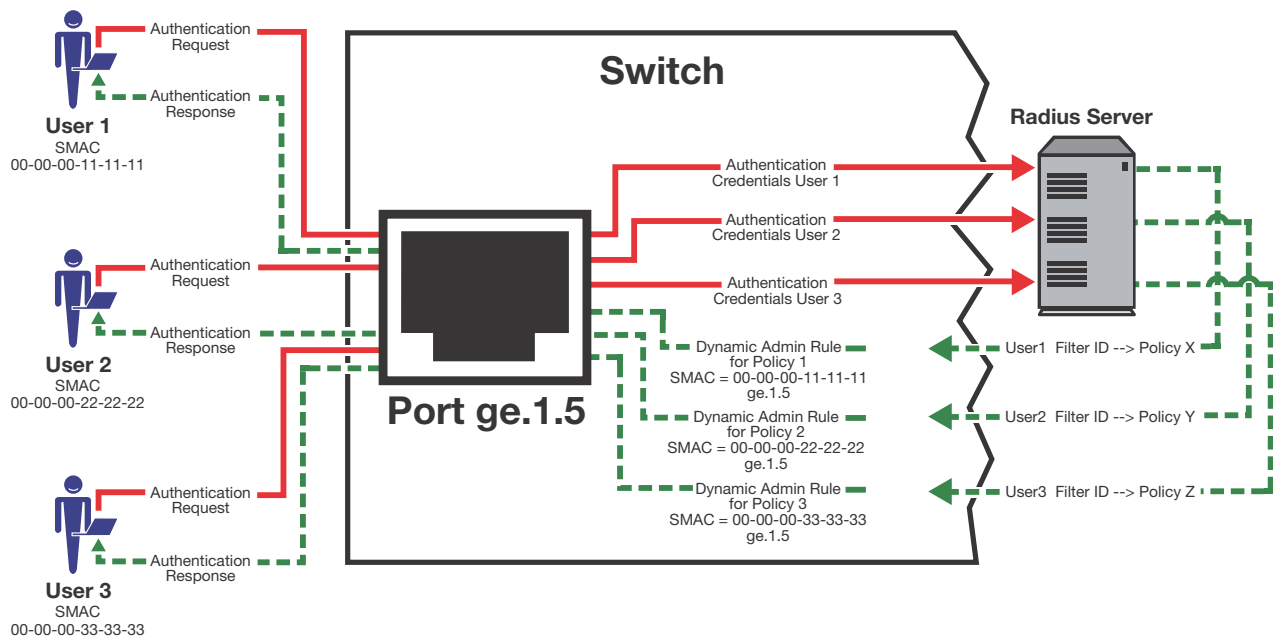
The number of allowed users per port can be configured using the **set multiauth port numusers** command. The **show multiauth port** command displays both the allowed number of users configured and the maximum number of users supported per port for the device. The allowed number of users defaults to 1 for the stackable fixed switch and standalone fixed switch platforms.



**Note:** Multi-user authentication on stackable fixed switch and standalone fixed switch platforms requires that the switch be the point of authentication, in order to apply policy.

In [Figure 10-1](#) each user on port ge.1.5 sends an authentication request to the RADIUS server. Based upon the Source MAC address (SMAC), RADIUS looks up the account for that user and includes the Filter-ID associated with that account in the authentication response back to the switch (see section [“The RADIUS Filter-ID”](#) on page 8 for Filter-ID information). The policy specified in the Filter-ID is then applied to the user. See section [RFC 3580 – VLAN Authorization](#) on page 8 for information on dynamic VLAN assignment and tunnel attribute configuration.



**Figure 10-1 Applying Policy to Multiple Users on a Single Port**

### User + IP Phone

The User + IP Phone authentication feature provides limited support for authentication and authorization of two devices, specifically a PC cascaded with a VLAN-tagging IP phone, on a single port on the switch. The IP phone must authenticate using MAC or 802.1X authentication, but the user may authenticate by any method. This feature allows both the user's PC and IP phone to simultaneously authenticate on a single port and each receive a unique level of network access. For details, refer to [“Configuring User + IP Phone Authentication”](#) on page 10-22.

### MultiAuth Authentication

Authentication mode support provides for the global setting of a single authentication mode 802.1X (strict-mode) or multiple modes (MultiAuth) per user or port when authenticating.

Strict mode is the appropriate mode when authenticating a single 802.1X user. All traffic on the port receives the same policy in strict mode. When authenticating PWA or MAC, you must use MultiAuth authentication, whether authenticating a single or multiple supplicants.

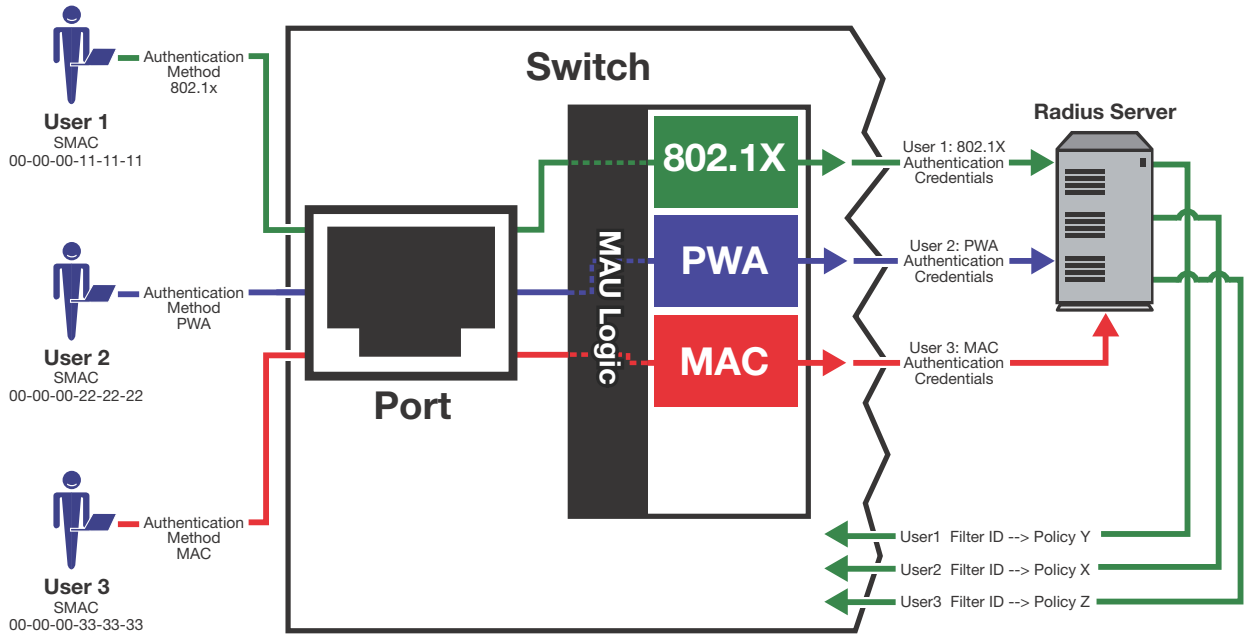
MultiAuth authentication supports the simultaneous configuration of up to three authentication methods per user on the same port, but only one method per user is actually applied. When MultiAuth authentication ports have a combination of authentication methods enabled, and a user is successfully authenticated for more than one method at the same time, the configured authentication method precedence will determine which RADIUS-returned Filter-ID will be processed and result in an applied traffic policy profile. See [“Setting MultiAuth Authentication Precedence”](#) on page 10-18 for authentication method precedence details.

The number of users or devices MultiAuth authentication supports depends upon the type of switch. See the firmware customer release note that comes with your switch for details on the number of users or devices supported per port.

In [Figure 10-2](#), multiple users are authenticated on a single port each with a different authentication method. In this case, each user on a single port successfully authenticates with a different authentication type. The authentication method is included in the authentication

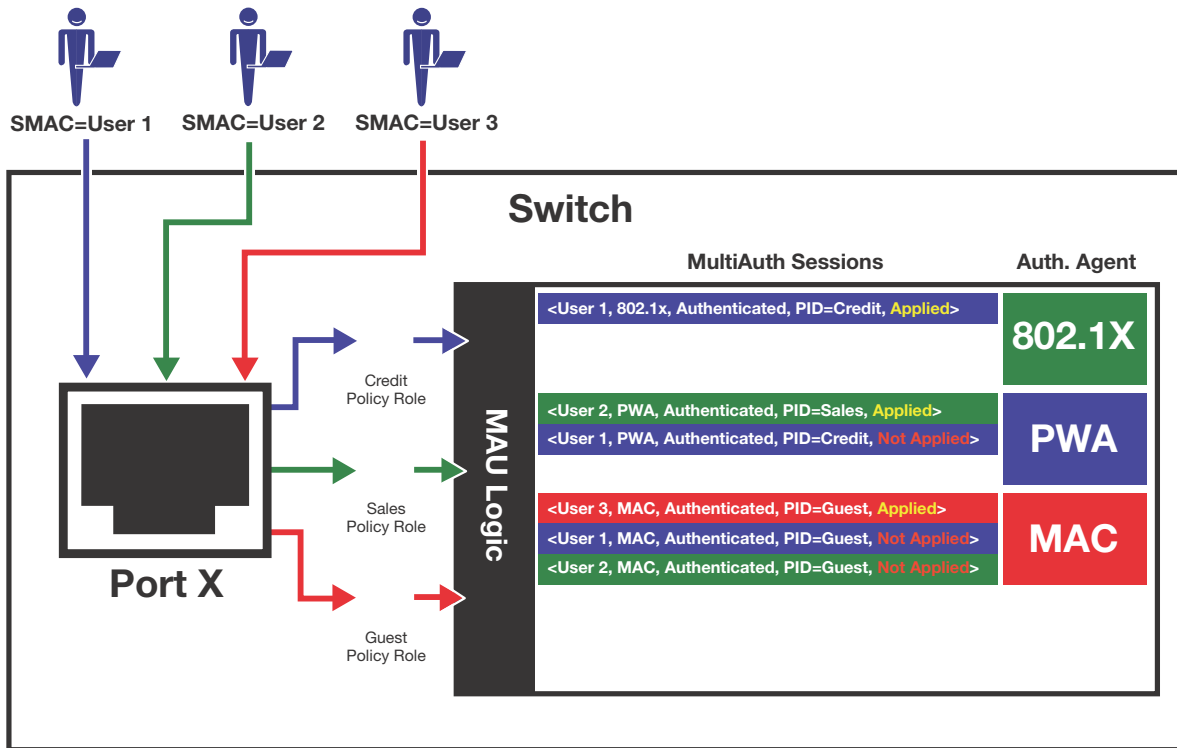
credentials sent to the RADIUS server. RADIUS looks up the user account for that user based upon the SMAC. The Filter-ID for that user is returned to the switch in the authentication response, and the authentication is validated for that user.

**Figure 10-2 Authenticating Multiple Users With Different Methods on a Single Port**



In Figure 10-3, full MultiAuth authentication takes place in that multiple users on a single port are validated for more than one authentication method. The applied authentication and policy are based upon the authentication method precedence level. On the far right column of the figure, the authentication methods are listed from top to bottom in order of precedence (the default order is displayed). User 1 is authenticating with both the 802.1x and PWA methods, with the Credit policy. Both the 802.1x and PWA authentication methods are validated, but only the 802.1x MultiAuth session is applied, because that has the highest precedence. User 2 is authenticating with both PWA and MAC methods, with the Sales policy. PWA, having a higher precedence than MAC, is the MultiAuth session applied for User 2. User 3 is a guest and is authenticating with the MAC method only. The MAC MultiAuth session, with the Guest policy is applied for User 3.

Figure 10-3 Selecting Authentication Method When Multiple Methods are Validated



## Remote Authentication Dial-In Service (RADIUS)

This section provides details for the configuration of RADIUS and RFC 3580 attributes.

| For information about...                      | Refer to page... |
|-----------------------------------------------|------------------|
| <a href="#">How RADIUS Data Is Used</a>       | 10-8             |
| <a href="#">The RADIUS Filter-ID</a>          | 10-8             |
| <a href="#">RFC 3580 — VLAN Authorization</a> | 10-8             |
| <a href="#">Policy Mappable Response</a>      | 10-10            |

The Remote Authentication Dial-In User Service (RADIUS) is an extensible protocol used to carry authentication and authorization information between the switch and the Authentication Server (AS). RADIUS is used by the switch for communicating supplicant supplied credentials to the authentication server and the authentication response from the authentication server back to the switch. This information exchange occurs over the link-layer protocol.

The switch acts as a client to RADIUS using UDP port 1812 by default (configurable in the **set radius** command). The authentication server contains a database of valid supplicant user accounts with their corresponding credentials. The authentication server checks that the information received from the switch is correct, using authentication schemes such as PAP, CHAP, or EAP. The authentication server returns an Accept or Reject message to the switch based on the credential validation performed by RADIUS. The implementation provides enhanced network security by using a shared secret and MD5 password encryption.

Required authentication credentials depend upon the authentication method being used. For 802.1x and PWA authentication, the switch sends username and password credentials to the authentication server. For MAC authentication, the switch sends the device MAC address and a

password configured on the switch to the authentication server. The authentication server verifies the credentials and returns an Accept or Reject message back to the switch.

## How RADIUS Data Is Used

The Enterasys switch bases its decision to open the port and apply a policy or close the port based on the RADIUS message, the port's default policy, and unauthenticated behavior configuration.

RADIUS provides accounting functionality by way of accounting packets from the switch to the RADIUS server, for such session statistics as start and end, total packets, and session end reason events. This data can be used for both billing and network monitoring purposes.

Additionally RADIUS is widely used by VoIP service providers. It is used to pass login credentials of a SIP end point (like a broadband phone) to a SIP Registrar using digest authentication, and then to the authentication server using RADIUS. Sometimes it is also used to collect call detail records (CDRs) later used, for instance, to bill customers for international long distance.

If you configure an authentication method that requires communication with an authentication server, you can use the RADIUS Filter-ID attribute to dynamically assign either a policy profile or management level to authenticating supplicants.

## The RADIUS Filter-ID

The RADIUS Filter-ID attribute consists of a string that is formatted in the RADIUS Access-Accept packet sent back from the authentication server to the switch during the authentication process.

Each user can be configured in the RADIUS server database with a RADIUS Filter-ID attribute that specifies the name of either a policy profile or management level the user should be assigned upon successful authentication. During the authentication process, when the authentication server returns a RADIUS Access-Accept packet that includes a Filter-ID matching a policy profile name configured on the switch, the switch then dynamically applies the policy profile to the physical port the supplicant is authenticating on.

The decorated Filter-ID supports a policy attribute, a management access attribute, or both in the following formats:

```
Enterasys:version=1:policy=polycyname
```

```
Enterasys:version=1:mgmt=access-mgmtType
```

```
Enterasys:version=1:mgmt=access-mgmtType:policy=polycyname
```

*polycyname* is the name of the policy to apply to this authentication.

*access-mgmtTypes* supported are: **ro** (read-only), **rw** (read-write), and **su** (super-user).

The undecorated Filter-ID supports the policy attribute only in the following format:

```
polycyname
```

The undecorated format is simply a string that specifies a policy profile name. The undecorated format cannot be used for management access authentication. Decorated Filter-IDs are processed first. If no decorated Filter-IDs are found, then undecorated Filter-IDs are processed. If multiple Filter-IDs are found that contain conflicting values, a Syslog message is generated.

## RFC 3580 — VLAN Authorization

Enterasys switches support the RFC 3580 RADIUS tunnel attribute for dynamic VLAN assignment. The VLAN-Tunnel-Attribute implements the provisioning of service in response to a successful authentication. On ports that do not support policy, the packet will be tagged with the VLAN-ID. The VLAN-Tunnel-Attribute defines the base VLAN-ID to be applied to the user.

## Dynamic VLAN Assignment

The RADIUS server may optionally include RADIUS tunnel attributes in a RADIUS Access-Accept message for dynamic VLAN assignment of the authenticated end system.

RFC 3580's RADIUS tunnel attributes are often configured on a RADIUS server to dynamically assign users belonging to the same organizational group within an enterprise to the same VLAN, or to place all offending users according to the organization's security policy in a Quarantine VLAN. Tunnel attributes are deployed for enterprises that have end system authentication configured on the network. For example, all engineers can be dynamically assigned to the same VLAN upon authentication, while sales are assigned to another VLAN upon authentication.

The name of the feature on Enterasys platforms that implements dynamic VLAN assignment through the receipt of RADIUS tunnel attributes is VLAN authorization. VLAN authorization depends upon receipt of the RFC 3580 RADIUS tunnel attributes in RADIUS Access-Accept messages. VLAN authorization must be enabled globally and on a per-port basis for the Tunnel attributes to be processed. When disabled per port or globally, the device will not process Tunnel attributes.

By default, all policy-capable Enterasys platforms will dynamically assign a policy profile to the port of an authenticating user based on the receipt of the Filter-ID RADIUS attribute. This is not the case for RADIUS tunnel attributes in that, by default, VLAN authorization is disabled.

### VLAN Authorization Attributes

Three Tunnel attributes are used for dynamic VLAN Authorization:

- Tunnel-Type attribute (Type=64, Length=6, Tag=0, Value=0x0D for VLAN)
- Tunnel-Medium-Type attribute (Type=65, Length=6, Tag=0, Value=0x06 for 802 media)
- Tunnel-Private-Group-ID attribute (Type=81, Length>=3, String=VID in ASCII)

The Tunnel-Type attribute indicates the tunneling protocol to be used when this attribute is formatted in RADIUS Access-Request messages, or the tunnel protocol in use when this attribute is formatted in RADIUS Access-Accept messages. Set Tunnel-Type attribute parameters as follows:

- Type: Set to 64 for Tunnel-Type RADIUS attribute
- Length: Set to 6 for six-byte length of this RADIUS attribute
- Tag: Provides a means of grouping attributes in the same packet which refer to the same tunnel. Valid values for this field are from 0x01 through 0x1F, inclusive. Set to 0 if unused. Unless alternative tunnel types are provided, it is only necessary for tunnel attributes to specify a single tunnel. As a result, where it is only desired to specify the VLAN-ID, the tag field should be set to zero (0x00) in all tunnel attributes.
- Value: Indicates the type of tunnel. A value of 0x0D (decimal 13) indicates that the tunneling protocol is a VLAN.

Tunnel-Medium-Type indicates the transport medium to use when creating a tunnel for the tunneling protocol, determined from Tunnel-Type attribute. Set Tunnel-Medium-Type attribute parameters as follows:

- Type: Set to 65 for Tunnel-Medium-Type RADIUS attribute
- Length: Set to 6 for six-byte length of this RADIUS attribute
- Tag: Provides a means of grouping attributes in the same packet which refer to the same tunnel. Valid value for this field are 0x01 through 0x1F, inclusive. Set to 0 if unused. Unless alternative tunnel types are provided, it is only necessary for tunnel attributes to specify a single tunnel. As a result, where it is only desired to specify the VLANID, the tag field should be set to zero (0x00) in all tunnel attributes.

- Value: Indicates the type of tunnel. A value of 0x06 indicates that the tunneling medium pertains to 802 media (including Ethernet)

Tunnel-Private-Group-ID attribute indicates the group ID for a particular tunneled session. Set the Tunnel-Private-Group-ID attribute parameters as follows:

- Type: Set to 81 for Tunnel-Private-Group-ID RADIUS attribute
- Length: Set to a value greater than or equal to 3.
- Tag: Provides a means of grouping attributes in the same packet which refer to the same tunnel. Valid values for this field are from 0x01 through 0x1F, inclusive. Set to 0 if unused. Unless alternative tunnel types are provided, it is only necessary for tunnel attributes to specify a single tunnel. As a result, where it is only desired to specify the VLANID, the tag field should be set to zero (0x00) in all tunnel attributes.
- String: Indicates the group. For the VLAN ID integer value, it is encoded as a string using ASCII. For example, the VLAN ID integer value 103 would be represented as 0x313033

### **VLAN Authorization Considerations**

VLAN Authorization poses some operational and management issues on the network.

- A VLAN is not a security container. It is a broadcast container and used to segment broadcast traffic on the network. ACLs implemented at the layer 3 routed interface for a VLAN only provide access control for traffic into and out of the VLAN. No access control mechanism for intra-VLAN communications exists, therefore users within the VLAN are not protected from each other. Malicious traffic allowed onto a VLAN can potentially infect all traffic on the VLAN. Such an infection can consume valuable hardware resources on the infrastructure, such as CPU cycles and memory. Infections can be transmitted to other hosts within the VLAN and to the layer 3 routed boundary. This leads to the direct competition of malicious traffic with business critical traffic on the network.
- End-To-End QoS cannot be truly guaranteed if QoS is implemented at the layer 3 routed interface for a network where business critical applications are classified and prioritized.
- If VLANs are implemented to group together users that are members of the same organizational group, then a VLAN must be configured everywhere in the network topology where a member of that organizational unit may connect to the network. For example, if an engineer may connect to the network from any location, then the Engineering VLAN must be configured on all access layer devices in the network. These VLAN configurations lead to over-extended broadcast domains as well as added configuration complexity in the network topology.
- A problem with moving an end system to a new VLAN is that the end system must be issued an IP address on the new VLAN's subnet to which it has become a member. If the end system does not yet have an IP address, this is not usually a problem. However, if the end system has an IP address, the lease of the address must time out before it attempts to obtain a new address, which may take some time. The IP address assignment process, implemented by DHCP, and the authentication process are not conjoined on the end system. Therefore, this leads to end systems possessing an invalid IP address after dynamic VLAN Authorization and lost IP connectivity until its current IP address times out. Furthermore, when a new IP address is eventually assigned to the end system, IP connectivity is disrupted for all applications on the end system.

### **Policy Mappable Response**

The policy mappable response, or conflict resolution, feature allows you to define how the system should handle allowing an authenticated user onto a port based on the contents of the RADIUS Accept message reply. There are three possible response settings: tunnel mode, policy mode, or both tunnel and policy, also known as hybrid authentication mode.



When the mactable response is set to **tunnel** mode, the system will use the tunnel attributes in the RADIUS reply to apply a VLAN to the authenticating user and will ignore any Filter-ID attributes in the RADIUS reply. When tunnel mode is configured, VLAN-to-policy mapping will not occur on a stackable fixed switch or standalone fixed switch platform.

When the mactable response is set to **policy** mode, the system will use the Filter-ID attributes in the RADIUS reply to apply a policy to the authenticating user and will ignore any tunnel attributes in the RADIUS reply. When policy mode is configured, no VLAN-to-policy mapping will occur.

When the mactable response is set to **both**, or hybrid authentication mode, both Filter-ID attributes (dynamic policy assignment) and tunnel attributes (dynamic VLAN assignment) sent in RADIUS Accept message replies are used to determine how the switch should handle authenticating users. When hybrid authentication mode is configured, VLAN-to-policy mapping can occur, as described below in [When Policy Mactable Response is “Both”](#).



**Note:** Hybrid authentication is supported on B-Series and C-Series stackable fixed switches and the G-Series standalone switches for Releases 6.3 and greater, and on A4 and I-Series for Release 6.61 and greater.

Using hybrid authentication mode eliminates the dependency on having to assign VLANs through policy roles — VLANs can be assigned by means of the tunnel attributes while policy roles can be assigned by means of the Filter-ID attributes. Alternatively, VLAN-to-policy mapping can be used to map policies to users using the VLAN specified by the tunnel attributes, without having to configure Filter-ID attributes on the RADIUS server. This separation gives administrators more flexibility in segmenting their networks beyond the platform’s policy role limits.

### When Policy Mactable Response is “Both”

Hybrid authentication mode uses both Filter-ID attributes and tunnel attributes. To enable hybrid authentication mode, use the **set policy mactable** command and set the **response** parameter to **both**. When configured to use both sets of attributes:

- If both the Filter-ID and tunnel attributes are present in the RADIUS reply, then the policy profile specified by the Filter-ID is applied to the authenticating user, and if VLAN authorization is enabled globally and on the authenticating user’s port, the VLAN specified by the tunnel attributes is applied to the authenticating user.

If VLAN authorization is not enabled, the VLAN specified by the policy profile is applied. See [“RFC 3580 — VLAN Authorization”](#) on page 10-8 for information about VLAN authorization.

- If the Filter-ID attributes are present but the tunnel attributes are not present, the policy profile specified by the Filter-ID is applied, along with the VLAN specified by the policy profile.
- If the tunnel attributes are present but the Filter-ID attributes are not present, and if VLAN authorization is enabled globally and on the authenticating user’s port, then the switch will check the VLAN-to-policy mapping table (configured with the **set policy mactable** command):
  - If an entry mapping the received VLAN ID to a policy profile is found, then that policy profile, along with the VLAN specified by the policy profile, will be applied to the authenticating user.
  - If no matching mapping table entry is found, the VLAN specified by the tunnel attributes will be applied to the authenticating user.
  - If the VLAN-to-policy mapping table is invalid, then the etsysPolicyRFC3580MapInvalidMapping MIB is incremented and the VLAN specified by the tunnel attributes will be applied to the authenticating user.

If VLAN authorization is not enabled, the tunnel attributes are ignored.

### When Policy Mappable Response is “Profile”

When the switch is configured to use only Filter-ID attributes, by setting the **set policy mappable** command **response** parameter to **policy**:

- If the Filter-ID attributes are present, the specified policy profile will be applied to the authenticating user. If no Filter-ID attributes are present, the default policy (if it exists) will be applied.
- If the tunnel attributes are present, they are ignored. No VLAN-to-policy mapping will occur.

### When Policy Mappable Response is “Tunnel”

When the switch is configured to use only tunnel attributes, by setting the **set policy mappable** command **response** parameter to **tunnel**, and if VLAN authorization is enabled both globally and on the authenticating user’s port:

- If the tunnel attributes are present, the specified VLAN will be applied to the authenticating user. VLAN-to-policy mapping will not occur on a stackable fixed switch or standalone fixed switch platform.
- If the tunnel attributes are not present, the default policy VLAN will be applied; if the default policy VLAN is not configured, the port VLAN will be applied.
- If the Filter-ID attributes are present, they are ignored.

If VLAN authorization is not enabled, the user will be allowed onto the port with the default policy, if it exists. If no default policy exists, the port VLAN will be applied.

## Configuring Authentication

This section provides details for the configuration of authentication methods, MultiAuth and RADIUS.

| For information about...                                   | Refer to page... |
|------------------------------------------------------------|------------------|
| <a href="#">Configuring IEEE 802.1x</a>                    | 10-14            |
| <a href="#">Configuring MAC-based Authentication</a>       | 10-15            |
| <a href="#">Configuring Port Web Authentication (PWA)</a>  | 10-16            |
| <a href="#">Configuring MultiAuth Authentication</a>       | 10-17            |
| <a href="#">Configuring VLAN Authorization</a>             | 10-20            |
| <a href="#">Configuring RADIUS</a>                         | 10-21            |
| <a href="#">Configuring User + IP Phone Authentication</a> | 10-22            |

Table 10-1 lists Authentication parameters and their default values.

**Table 10-1 Default Authentication Parameters**

| Parameter        | Description                                                            | Default Value                             |
|------------------|------------------------------------------------------------------------|-------------------------------------------|
| dot1x            | Enables and disables 802.1x authentication both globally and per port. | Globally: Disabled.<br>Per Port: Enabled. |
| dot1x authconfig | Configures 802.1x authentication.                                      | auto - auto authorization mode.           |



**Table 10-1 Default Authentication Parameters (continued)**

| Parameter                         | Description                                                                                                                           | Default Value                                                                   |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| macauthentication                 | Globally enables or disables MAC authentication on a device.                                                                          | Disabled.                                                                       |
| macauthentication port            | Enables or disables MAC authentication on a port                                                                                      | Disabled.                                                                       |
| MultiAuth idle-timeout            | Specifies the period length for which no traffic is received before a MultiAuth session is set to idle.                               | 300 seconds.                                                                    |
| MultiAuth mode                    | Globally sets MultiAuth for this device.                                                                                              | strict - authentication limited to 802.1x for a single user on a port.          |
| MultiAuth port mode               | Specifies the MultiAuth port mode to use for the specified port.                                                                      | auth-opt - Authentication is optional based upon global and port configuration. |
| MultiAuth precedence              | Specifies the authentication mode to use when multiple authentication types are successfully authenticated.                           | Precedence from high to low: 802.1x, PWA, MAC.                                  |
| MultiAuth session-timeout         | Specifies the maximum amount of time a session can live.                                                                              | 0 - no timeout in effect.                                                       |
| pwa                               | Globally enables or disables PWA authentication.                                                                                      | Disabled.                                                                       |
| pwa enhancedmode                  | Allows a user on an unauthenticated port to enter any URL in the browser to access the login page.                                    | Disabled.                                                                       |
| radius                            | Enable or disable RADIUS on this device.                                                                                              | Disabled.                                                                       |
| radius accounting                 | Enables or disables RADIUS accounting for this device.                                                                                | Disabled.                                                                       |
| radius accounting intervalminimum | Specifies the minimum interval before sending updates for RADIUS accounting.                                                          | 600 seconds.                                                                    |
| radius accounting retries         | Specifies the number of times a switch will attempt to contact an authentication server for RADIUS accounting that is not responding. | 2.                                                                              |
| radius accounting timeout         | Specifies the amount of time for a switch to make contact with a RADIUS server.                                                       | 5 seconds.                                                                      |
| radius accounting updateinterval  | Specifies the minimum interval between interim updates for RADIUS accounting.                                                         | 1800 seconds.                                                                   |
| radius retries                    | Specifies the number of times a switch will try to establish with the authentication server.                                          | 3.                                                                              |
| radius timeout                    | Specifies the amount of time a switch will wait to receive a response from the authentication server before sending another request.  | 20 seconds.                                                                     |

**Table 10-1 Default Authentication Parameters (continued)**

| Parameter                        | Description                                                                                             | Default Value                               |
|----------------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------|
| realm                            | Specifies authentication server configuration scope.                                                    | Both: management-access and network-access. |
| VLAN authorization status        | Enables or disables globally and per port VLAN authorization.                                           | Globally: Disabled.<br>Per Port: Enabled.   |
| VLAN authorization egress format | Determines whether dynamic VLAN tagging will be none, tagged, untagged, or dynamic for an egress frame. | Untagged.                                   |

## Configuring IEEE 802.1x

Configuring IEEE 802.1x on an authenticator switch port consists of:

- Setting the authentication mode globally and per port
- Configuring optional authentication port parameters globally and per port
- Globally enabling 802.1x authentication for the switch

[Procedure 10-1](#) describes how to configure IEEE 802.1x on an authenticator switch port. Unspecified parameters use their default values.

### Procedure 10-1 IEEE 802.1x Configuration

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Command(s)                                                                                                                                                                                                                                                               |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | <p>Set the IEEE 802.1x authentication mode both globally and per port:</p> <ul style="list-style-type: none"> <li>• <b>Auto</b> - The switch will only forward authenticated frames.</li> <li>• <b>Forced-auth</b> - 802.1x authentication is effectively disabled for this port. All received frames are forwarded.</li> <li>• <b>Forced-unauth</b> - 802.1x authentication is effectively disabled on the port. If 802.1x is the only authentication method on the port, all frames are dropped.</li> </ul> <p><b>Note:</b> Before enabling 802.1x authentication on the switch, you must set the authentication mode of ports that will not be participating in 802.1x authentication to forced-authorized to assure that frames will be forwarded on these ports. Examples of this kind of port are connections between switches and connections between a switch and a router.</p> <p>The setting of dot1x options other than <b>authcontrolled-portcontrol</b> are optional.</p> | <pre>set dot1x auth-config {[authcontrolled-portcontrol {auto   forced-auth   forced-unauth}] [maxreq value] [quietperiod value] [reauthenabled {false   true}] [reauthperiod value] [servertimeout timeout] [supptimeout timeout] [txperiod value]} [port-string]</pre> |

**Procedure 10-1 IEEE 802.1x Configuration (continued)**

| Step | Task                                                                                                                                                                                                                                                                                                                                        | Command(s)                                                                                       |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| 2.   | Display the access entity index values. Ports used to authenticate and authorize supplicants utilize access entities that maintain entity state, counters, and statistics for an individual supplicant. You need to know the index value associated with a single entity to enable, disable, initialize, or reauthenticate a single entity. | <b>show dot1x auth-session-stats</b>                                                             |
| 3.   | Enable EAP on the stackable fixed switch or standalone fixed switch.                                                                                                                                                                                                                                                                        | <b>set eapol {enable   disable} [auth-mode {auto   forced-auth   forced-unauth} port-string]</b> |
| 4.   | Enable IEEE 802.1x globally on the switch. Ports default to enabled.                                                                                                                                                                                                                                                                        | <b>set dot1x {enable   disable}</b>                                                              |
| 5.   | If an entity deactivates due to the supplicant logging off, inability to authenticate, or the supplicant or associated policy settings are no longer valid, you can re-initialize a deactivated access entity. If necessary, re-initialize the specified entity.                                                                            | <b>set dot1x init [port-string] [index index-list]</b>                                           |
| 6.   | If the authentication for a supplicant times out or is lost for any reason, you can reauthenticate that supplicant. If necessary, reauthenticate the specified entity.                                                                                                                                                                      | <b>set dot1x reauth [port-string] [index index-list]</b>                                         |
| 7.   | Display IEEE 802.1x configuration.                                                                                                                                                                                                                                                                                                          | <b>show dot1x auth-config</b>                                                                    |

## Configuring MAC-based Authentication

Configuring MAC-based authentication on a switch consists of:

- Setting the global MAC authentication password for the switch
- Enabling MAC authentication on a port
- Enabling MAC authentication globally
- Setting the authentication mode to multi
- Optionally re-initializing or re-authenticating existing sessions

[Procedure 10-2](#) describes how to configure MAC-based authentication. Unspecified parameters use their default values.

**Procedure 10-2 MAC-Based Authentication Configuration**

| Step | Task                                                                                                                                                                        | Command(s)                                                                                         |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| 1.   | Optionally set or clear a global password on the switch.                                                                                                                    | <b>set macauthentication password password</b><br><b>clear macauthentication password password</b> |
| 2.   | Enable or disable MAC authentication on a port. By default, MAC authentication is disabled for all ports. MAC authentication must be enabled on the ports that will use it. | <b>set macauthentication port {enable   disable} port-string</b>                                   |

**Procedure 10-2 MAC-Based Authentication Configuration (continued)**

| Step | Task                                                                                                                            | Command(s)                                                                                                                                    |
|------|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 3.   | Enable or disable MAC authentication globally on the device. By default, MAC authentication is globally disabled on the device. | <b>set macauthentication {enable   disable}</b>                                                                                               |
| 4.   | Set the MultiAuth mode.                                                                                                         | <b>set multiauth mode multi</b>                                                                                                               |
| 5.   | Display MAC authentication configuration or status of active sessions.                                                          | <b>show macauthentication</b><br><b>show macauthentication session</b>                                                                        |
| 6.   | If a session or port requires reinitialization, re-initialize a specific MAC session or port.                                   | <b>set macauthentication macinitialize</b><br><i>mac-address</i><br><b>set macauthentication portinitialize</b><br><i>port-string</i>         |
| 7.   | If a session or port requires reauthentication, re-authenticate a specific MAC session or port.                                 | <b>set macauthentication macreauthenticate</b><br><i>mac-address</i><br><b>set macauthentication portreauthenticate</b><br><i>port-string</i> |

## Configuring Port Web Authentication (PWA)

Configuring PWA on the switch consists of:

- Setting the IP address which the user will authenticate to on the switch
- Optionally enabling PWA enhanced mode and configure guest networking privileges
- Enabling PWA on the port
- Globally enabling PWA on the switch
- Setting the authentication mode to multi

[Procedure 10-3](#) describes how to configure PWA authentication. Unspecified parameters use their default values.

**Procedure 10-3 Port Web Authentication (PWA) Configuration**

| Step | Task                                                                        | Command(s)                                                                                                    |
|------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| 1.   | Set the IP address for the end-station the supplicant accesses.             | <b>set pwa ipaddress</b> <i>ip-address</i>                                                                    |
| 2.   | Optionally enable or disable PWA enhanced mode.                             | <b>set pwa enhancedmode enable</b><br><b>set pwa enhancedmode disabled</b>                                    |
| 3.   | Enable or disable PWA. PWA must be enabled on the port for PWA to function. | <b>set pwa portcontrol enable</b> <i>port-string</i><br><b>set pwa portcontrol disable</b> <i>port-string</i> |
| 4.   | Globally enable or disable PWA on the switch.                               | <b>set pwa enable</b><br><b>set pwa disabled</b>                                                              |
| 5.   | Set the MultiAuth mode.                                                     | <b>set multiauth mode multi</b>                                                                               |
| 6.   | Display PWA configuration.                                                  | <b>show pwa</b>                                                                                               |

## Optionally Enable Guest Network Privileges

With PWA enhanced mode enabled, you can optionally configure guest networking privileges. Guest networking allows an administrator to specify a set of credentials that will, by default, appear on the PWA login page of an end station when a user attempts to access the network. When enhanced mode is enabled, PWA will use a guest password and guest user name to grant network access with default policy privileges to users without established login names and passwords.

In order to configure guest networking privileges, you need to set the guest status, user name, and password. You can set guest status for no authentication, RADIUS authentication, or disabled. When you set guest status to no authentication, guest status is provided with its associated policy, but no authentication takes place. When you set guest status to RADIUS authentication, guest status is provided only after a successful authentication takes place. If guest networking status is disabled, all supplicants must be authenticated with a valid user name and password at the login page.

[Table 10-2](#) describes how to optionally enable guest networking privileges.

**Table 10-2 PWA Guest Networking Privileges Configuration**

| Task                                                                                                                                                                              | Command(s)                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
| Set a guest user name for PWA networking. PWA will use this name to grant network access to guests without established login names and passwords.                                 | <code>set pwa guestname name</code>         |
| Set a guest user password for PWA networking. PWA will use this password and the guest user name to grant network access to guests without established login names and passwords. | <code>set pwa guestpassword</code>          |
| Optionally enable guest status without authentication                                                                                                                             | <code>set pwa gueststatus authnone</code>   |
| Optionally enable guest status with authentication.                                                                                                                               | <code>set pwa gueststatus authradius</code> |
| Optionally disable guest status                                                                                                                                                   | <code>set pwa gueststatus disable</code>    |

## Configuring MultiAuth Authentication

Configuring MultiAuth authentication consists of:

- Setting MultiAuth authentication mode setting
- Setting MultiAuth authentication precedence settings
- Setting MultiAuth authentication port properties
- Setting MultiAuth authentication idle timeout values
- Setting MultiAuth authentication session timeout values

### Setting MultiAuth Authentication Mode

MultiAuth authentication mode can be set to MultiAuth or strict 802.1X single user mode. Set MultiAuth authentication to MultiAuth when multiple users need to be authenticated for 802.1X or in all cases for MAC and PWA authentication.

[Procedure 10-4](#) describes setting the MultiAuth authentication mode.

**Procedure 10-4 MultiAuth Authentication Configuration**

| Step | Task                                                                                                                                                        | Command(s)                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| 1.   | For a single user, single authentication 802.1x port configuration, set MultiAuth mode to strict.                                                           | <b>set multiauth mode strict</b> |
| 2.   | For multiple user 802.1x authentication or any non-802.1x authentication, set the system authentication mode to use multiple authenticators simultaneously. | <b>set multiauth mode multi</b>  |
| 3.   | To clear the MultiAuth authentication mode.                                                                                                                 | <b>clear multiauth mode</b>      |

**Setting MultiAuth Authentication Precedence**

MultiAuth authentication administrative precedence globally determines which authentication method will be selected when a user is successfully authenticated for multiple authentication methods on a single port. When a user successfully authenticates more than one method at the same time, the precedence of the authentication methods will determine which RADIUS-returned Filter-ID will be processed and result in an applied traffic policy profile.

MultiAuth authentication precedence defaults to the following order from high to low: 802.1x, PWA, and MAC on stackable fixed switch and standalone fixed switch devices. You may change the precedence for one or more methods by setting the authentication methods in the order of precedence from high to low. Any methods not entered are given a lower precedence than the methods entered in their pre-existing order. For instance, if you start with the default order and only set PWA and MAC, the new precedence order will be PWA, MAC, 802.1x.

Given the default order of precedence (802.1x, PWA, MAC), if a user was to successfully authenticate with PWA and MAC, the authentication method RADIUS Filter-ID applied would be PWA, because it has a higher position in the order. A MAC session would authenticate, but its associated RADIUS Filter-ID would not be applied.

[Procedure 10-5](#) describes setting the order for MultiAuth authentication precedence.

**Procedure 10-5 MultiAuth Authentication Precedence Configuration**

| Step | Task                                                                                                                                                                                     | Command(s)                                             |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| 1.   | Set a new order of precedence for the selection of the RADIUS Filter-ID that will be returned when multiple authentication methods are authenticated at the same time for a single user. | <b>set multiauth precedence {{dot1x} [mac] [pwa] }</b> |
| 2.   | Reset the order MultiAuth authentication precedence to the default values.                                                                                                               | <b>clear multiauth precedence</b>                      |

**Setting MultiAuth Authentication Port Properties**

MultiAuth authentication supports the configuration of MultiAuth port and maximum number of users per port properties. The MultiAuth port property can be configured as follows:

- **Authentication Optional** – Authentication methods are active on the port based upon the global and port authentication method. Before authentication succeeds, the current policy role applied to the port is assigned to the ingress traffic. This is the default role if no authenticated user or device exists on the port. After authentication succeeds, the user or device is allowed to access the network according to the policy information returned from the authentication server, in the form of the RADIUS Filter-ID attribute, or the static configuration on the switch. This is the default setting.

- **Authentication Required** – Authentication methods are active on the port, based on the global and per port authentication method configured. Before authentication succeeds, no traffic is forwarded onto the network. After authentication succeeds, the user or device gains access to the network based upon the policy information returned by the authentication server in the form of the RADIUS Filter-ID attribute, or the static configuration on the switch.
- **Force Authenticated** – The port is completely accessible by all users and devices connected to the port, all authentication methods are inactive on the port, and all frames are forwarded onto the network.
- **Force Unauthenticated** – The port is completely closed for access by all users and devices connected to the port. All authentication methods are inactive and all frames are discarded.

[Procedure 10-6](#) describes setting the MultiAuth authentication port and maximum user properties.

### Procedure 10-6 MultiAuth Authentication Port and Maximum User Properties Configuration

| Step | Task                                                                                                                                                                                                                                                                                                                                          | Command(s)                                                          |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| 1.   | Set the specified ports to the MultiAuth authentication optional port mode.                                                                                                                                                                                                                                                                   | <b>set multiauth port mode auth-opt</b> <i>port-string</i>          |
| 2.   | Set the specified ports to the MultiAuth authentication required port mode.                                                                                                                                                                                                                                                                   | <b>set multiauth port mode auth-reqd</b> <i>port-string</i>         |
| 3.   | Set the specified ports to the MultiAuth authentication force authenticated port mode.                                                                                                                                                                                                                                                        | <b>set multiauth port mode force-auth</b> <i>port-string</i>        |
| 4.   | Set the specified ports to the MultiAuth authentication force unauthenticated port mode.                                                                                                                                                                                                                                                      | <b>set multiauth port mode force-unauth</b> <i>port-string</i>      |
| 5.   | Optionally set the maximum number of authenticated users for the specified port.<br><b>Notes:</b> This value can be set to any value up to the maximum number of MultiAuth users supported for the device. See the firmware release notes that come with your device for the maximum number of supported MultiAuth users the device supports. | <b>set multiauth port mode numusers</b> <i>numusers port-string</i> |
| 6.   | Reset the ports MultiAuth authentication port mode to the default value for the specified ports.                                                                                                                                                                                                                                              | <b>clear multiauth port mode</b> <i>port-string</i>                 |
| 7.   | Reset the ports MultiAuth authentication port maximum number of users to the default value for the specified ports.                                                                                                                                                                                                                           | <b>clear multiauth port numusers</b> <i>port-string</i>             |

## Setting MultiAuth Authentication Timers

The idle timeout setting determines the amount of idle time in which no traffic transits the link for a user or device before the connection is removed from the connection table. The idle timeout can be set for any authentication method.

The session timeout setting determines the maximum amount of time a session can last before being terminated.

[Procedure 10-7](#) describes setting the MultiAuth authentication timers.

**Procedure 10-7 MultiAuth Authentication Timers Configuration**

| Step | Task                                                                                                                                 | Command(s)                                                             |
|------|--------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| 1.   | Optionally set the MultiAuth authentication idle timeout value for the specified authentication method.                              | <b>set multiauth idle-timeout</b> <i>auth-method</i> <i>timeout</i>    |
| 2.   | Reset the MultiAuth authentication idle timeout value to its default value for the specified authentication method.                  | <b>clear multiauth idle-timeout</b> <i>auth-method</i>                 |
| 3.   | Optionally set the maximum amount of time a session can last before termination for the specified authentication method.             | <b>set multiauth session-timeout</b> <i>auth-method</i> <i>timeout</i> |
| 4.   | Reset the maximum amount of time a session can last before termination to the default value for the specified authentication method. | <b>clear multiauth session-timeout</b> <i>auth-method</i>              |

**Displaying MultiAuth Configuration Information**

MultiAuth authentication supports the display of system-wide MultiAuth authentication values, MultiAuth authentication counters, port settings, end-user MAC addresses, session information, idle timeout settings, session timeout settings, and trap settings.

[Table 10-3](#) describes displaying of MultiAuth authentication settings and statistics.

**Table 10-3 Displaying MultiAuth Authentication Configuration**

| Task                                                                                                                      | Command(s)                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Display system-wide MultiAuth authentication values.                                                                      | <b>show multiauth</b>                                                                                           |
| Display MultiAuth authentication port settings for all or the specified ports.                                            | <b>show multiauth port</b> [ <i>port-string</i> ]                                                               |
| Display end-user MAC addresses per port for all MAC addresses and ports or for those specified.                           | <b>show multiauth station</b> [ <i>mac-address</i> ] [ <i>port-string</i> ]                                     |
| Display MultiAuth authentication sessions for all sessions or the specified authentication method, MAC address, or ports. | <b>show multiauth session</b> [ <i>agent</i> <i>auth-method</i> ] [ <i>mac-address</i> ] [ <i>port-string</i> ] |
| Display MultiAuth authentication idle timeout values.                                                                     | <b>show multiauth idle-timeout</b>                                                                              |
| Display MultiAuth authentication session timeout values.                                                                  | <b>show multiauth session-timeout</b>                                                                           |

**Configuring VLAN Authorization**

VLAN authorization allows for the dynamic assignment of users to the same VLAN. You configure VLAN authorization attributes within RADIUS. On the switch you enable VLAN authorization both globally and per-port. VLAN authorization is disabled globally by default. VLAN authorization is enabled per port by default. You can also set the VLAN egress format per-port. VLAN egress format defaults to untagged. VLAN egress format can be set as follows:

- **none** – No egress manipulation will be made.
- **tagged** – The authenticating port will be added to the current tagged egress for the VLAN-ID returned.
- **untagged** – The authenticating port will be added to the current untagged egress for the VLAN-ID returned.



- **dynamic** – Egress formatting will be based upon information contained in the authentication response.

The VLAN authorization table will always list any tunnel attribute's VIDs that have been received for authenticated end systems, but a VID will not actually be assigned unless VLAN authorization is enabled both globally and on the authenticating port. Dynamic VLAN authorization overrides the port PVID. Dynamic VLAN authorization is not reflected in the **show port vlan** display. The VLAN egress list may be statically configured, enabled based upon the **set vlanauthorization egress** command, or have dynamic egress enabled to allow full VLAN membership and connectivity.

[Procedure 10-8](#) describes setting VLAN authorization configuration.

### Procedure 10-8 VLAN Authorization Configuration

| Step | Task                                                                                             | Command(s)                                       |
|------|--------------------------------------------------------------------------------------------------|--------------------------------------------------|
| 1.   | Enable or disable VLAN authorization both globally and per port.                                 | <b>set vlanauthorization {enable   disable}</b>  |
| 2.   | Reset VLAN authorization configuration to default values for the specified port-list or for all. | <b>clear vlanauthorization {port-list   all}</b> |
| 3.   | Display VLAN authorization configuration settings for the specified port-list or for all.        | <b>show vlanauthorization {port-list   all}</b>  |

### Setting Dynamic Policy Profile Assignment

Dynamic policy profile assignment is implemented using the policy mapping table. When VLAN authorization is enabled, authenticated users are dynamically assigned to the received tunnel attribute's VID, unless preempted by a policy map-table configuration entry. Dynamic policy profile assignment is supported by mapping a VID to a policy role upon receipt of a RADIUS tunnel attribute.

[Procedure 10-9](#) describes configuring dynamic policy profile assignment

### Procedure 10-9 Policy Profile Assignment Configuration

| Step | Task                                                                | Command(s)                                                                               |
|------|---------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| 1.   | Identify the profile index to be used in the VID-to-policy mapping. | <b>show policy profile all</b>                                                           |
| 2.   | Map the VLAN ID to the profile index.                               | <b>set policy mactable {vlan-list profile-index   response {tunnel   policy   both}}</b> |
| 3.   | Display the current mactable configuration.                         | <b>show policy mactable.</b>                                                             |

## Configuring RADIUS

You can set, clear, and display RADIUS configuration for both authentication and accounting.

### Configuring the Authentication Server

There are four aspects to configuring the authentication server:

- **State** enables or disables the RADIUS client for this switch.
- **Establishment values** configure a timer setting the length of time before retries, as well as the number of retries, before the switch determines the authentication server is down and attempts to establish with the next server in its list.

- **Server identification** provides for the configuration of the server IP address and index value. The index determines the order in which the switch will attempt to establish a session with an authentication server. After setting the index and IP address you are prompted to enter a secret value for this authentication server. Any authentication requests to this authentication server must present the correct secret value to gain authentication.
- The **realm** provides for configuration scope for this server: management access, network access, or both.

Firmware supports the configuration of multiple authentication servers. The lowest index value associated with the server determines the primary server. If the primary server is down, the operational server with the next lowest index value is used. If the switch fails to establish contact with the authentication server before a configured timeout, the switch will retry for the configured number of times.

Servers can be restricted to management access or network access authentication by configuring the realm option.

[Procedure 10-10](#) describes authentication server configuration.

### Procedure 10-10 Authentication Server Configuration

| Step | Task                                                                                                                                                       | Command(s)                                                                                                                                               |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Configure the index value, IP address, and secret value for this authentication server.                                                                    | <b>set radius server</b> <i>index ip-address</i> [ <i>secret-value</i> ]                                                                                 |
| 2.   | Optionally set the number of seconds the switch will wait before retrying authentication server establishment.                                             | <b>set radius timeout</b> <i>timeout</i>                                                                                                                 |
| 3.   | Optionally set the number of retries that will occur before the switch declares an authentication server down.                                             | <b>set radius retries</b> <i>retries</i>                                                                                                                 |
| 4.   | Optionally set the authentication server configuration scope to management access, network access, or both for all or the specified authentication server. | <b>set radius realm</b> { <b>management-access</b>   <b>network-access</b>   <b>any</b> } { <i>as-index</i>   <b>all</b> }                               |
| 5.   | Globally enable or disable RADIUS on the switch.                                                                                                           | <b>set radius</b> { <b>enable</b>   <b>disable</b> }                                                                                                     |
| 6.   | Reset the specified RADIUS setting to its default value.                                                                                                   | <b>clear radius</b> { [ <b>retries</b> ] [ <b>timeout</b> ] [ <b>server</b> [ <i>index</i>   <b>all</b> ] [ <b>realm</b> { <i>index</i>   <b>all</b> }]} |
| 7.   | Display the current RADIUS authentication server settings.                                                                                                 | <b>show radius</b> [ <b>retries</b>   <b>authtype</b>   <b>timeout</b>   <b>server</b> [ <i>index</i>   <b>all</b> ]]                                    |

## Configuring User + IP Phone Authentication

User + IP phone authentication is a special application of multi-user authentication that allows a user and their IP phone to both use a single port on the switch but to have separate policy roles. The user's PC and their IP phone are daisy-chained together with a single connection to the network. The IP phone may authenticate using 802.1x or MAC authentication, while the user can use any supported authentication method.

This feature is the only version of multi-user authentication that is supported on the A4. It is not recommended to be used on the other fixed stackable and standalone platforms that can support multiple users per port unless you are integrating the switch into a legacy deployment.



**Note:** User + IP Phone authentication is not supported on the I-Series

With “User + IP Phone” authentication, the policy role for the IP phone is statically mapped using a policy admin rule which assigns any frames received with a VLAN tag set to a specific VID (for example, Voice VLAN) to a specified policy role (for example, IP Phone policy role). Therefore, it is required that the IP phone be configured to send VLAN-tagged frames tagged for the “Voice” VLAN. Refer to the command **set policy rule** for additional information about configuring a policy admin rule that maps a VLAN to a policy role.

Note that if the IP phone authenticates to the network, the RADIUS Access-Accept message must return null values for RFC 3580 tunnel attributes and the Filter-ID.

The second policy role, for the user, can either be statically configured with the default policy role on the port or dynamically assigned through authentication to the network (using a RADIUS Filter-ID). When the default policy role is assigned on a port, the VLAN set as the port's PVID is mapped to the default policy role unless the default policy has a defined VLAN, which will override the port's PVID. When a policy role is dynamically applied to a user as the result of a successfully authenticated session and the resulting policy has a configured VLAN, that VLAN will override the port PVID or the default policy's defined VLAN.

## Example

The following procedure and code example show the basic steps to configure User + IP phone authentication on several user ports.

### Procedure 10-11 User + IP Phone Configuration

| Step | Task                                                                                                                                               | Command(s)                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Configure the IP phones to send VLAN-tagged voice traffic frames, tagged for the phone VLAN.                                                       | N/A                                                                                                                                                 |
| 2.   | On the switch, create phone VLAN and user VLAN.<br>Optionally, give names to the VLANs.                                                            | <b>set vlan create</b> <i>vlan-list</i><br><br><b>set vlan name</b> <i>vid name</i>                                                                 |
| 3.   | Create a CoS setting for the phone VLAN.                                                                                                           | <b>set cos settings</b> <i>cos-index</i> <b>priority</b> <i>priority</i> [ <b>tos-value</b> <i>tos</i> ]<br>[ <b>irl-reference</b> <i>irl-ref</i> ] |
| 4.   | Set the number of users per port to 2 on the user ports                                                                                            | <b>set multiauth port numusers</b> 2<br><i>port-string</i>                                                                                          |
| 5.   | Create a policy profile for the users that uses the user VLAN.                                                                                     | <b>set policy profile</b> <i>index</i> <b>pvid-status</b> <b>enable</b> <b>pvid</b> <i>pvid</i>                                                     |
| 6.   | Create a policy profile for the phones that typically will have an associated CoS.                                                                 | <b>set policy profile</b> <i>index</i> <b>cos-status</b> <b>enable</b> <b>cos</b> <i>cos</i>                                                        |
| 7.   | Statically map the phone policy profile to frames received tagged with the phone VLAN and specify ports to egress the phone VLAN frames as tagged. | <b>set policy rule</b> <b>admin-profile</b> <b>vlantag</b> <i>vlanid</i> <b>admin-pid</b> <i>index</i> <b>port-string</b> <i>port-string</i>        |
| 8.   | Configure RADIUS                                                                                                                                   | See “ <a href="#">Configuring RADIUS</a> ” on page 10-21                                                                                            |
| 9.   | Configure authentication, either IEEE 802.1x or MAC-based authentication.                                                                          | See “ <a href="#">Configuring IEEE 802.1x</a> ” on page 10-14<br>See “ <a href="#">Configuring MAC-based Authentication</a> ” on page 10-15         |

The following code example:

- Creates and names two VLANS, one for the users and one for the phones.
- Creates a CoS setting of index 55.
- Sets the number of users to 2 on all the user ports.
- Creates a user policy profile that uses the user VLAN.
- Creates a policy profile for the phones and a policy rule that maps tagged frames on the user ports to that policy profile.
- Minimally configures RADIUS, 802.1x, and MAC authentication.

```
A4(su)->set vlan create 208
```

```
A4(su)->set vlan name 208 Sales
```

```
A4(su)->set vlan create 44
```

```
A4(su)->set vlan name 44 Phones
```

```
A4(su)->set cos settings 55 priority 6
```

```
A4(su)->set multiauth port numusers 2 fe.1.1-22
```

```
A4(su)->set policy profile 2 name "Sales Group" pvid-status enable pvid 208
untagged-vlans 208
```

```
A4(su)->set policy profile 144 name "Phone Group" cos-status enable cos 55
```

```
A4(su)->set policy rule admin-profile vlantag 44 admin-pid 144 port-string
fe.1.1-22
```

```
A4(su)->set radius enable
```

```
A4(su)->set radius server 1 192.168.10.10 1812 sharedsecret
```

```
A4(su)->set multiauth mode multi
```

```
A4(su)->set dot1x enable
```

```
A4(su)->set macauthentication enable
```

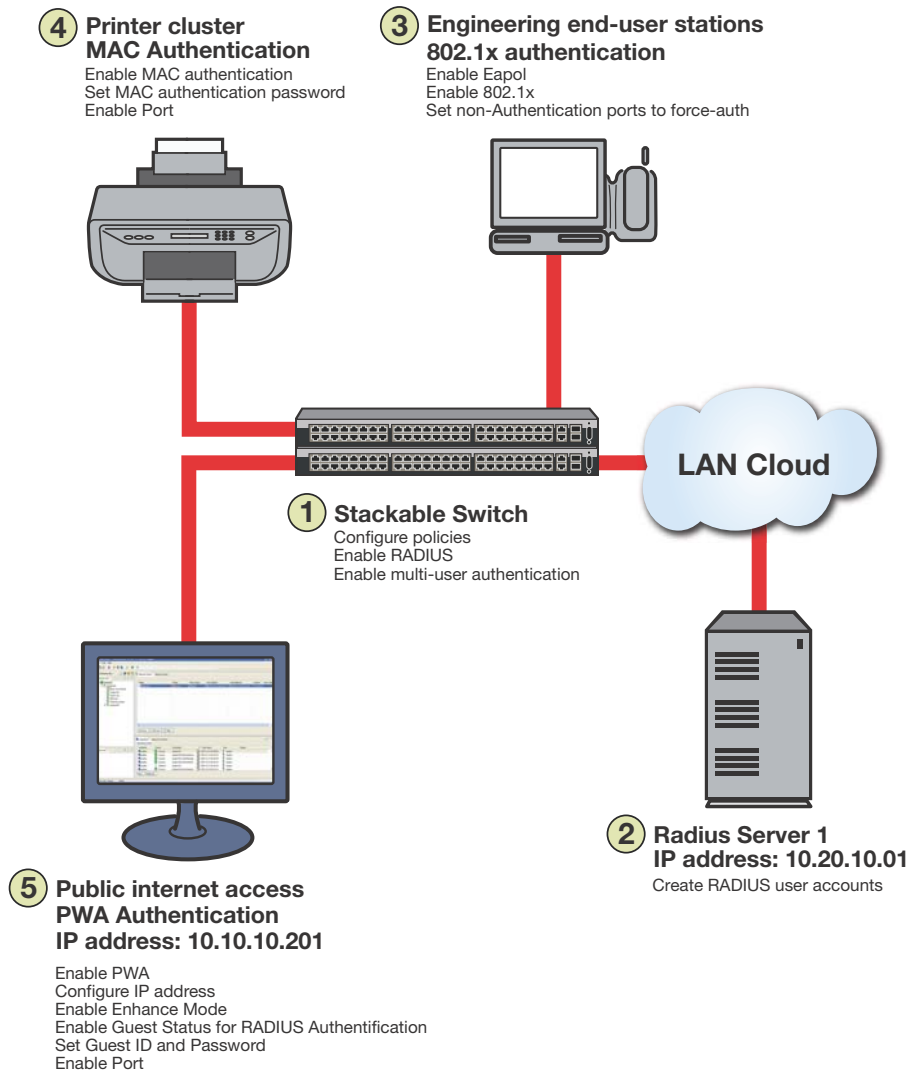
```
A4(su)->set macauthentication password mypass
```

```
A4(su)->set macauthentication port enable fe.1.1-22
```

## Authentication Configuration Example

Our example covers the three supported stackable and fixed switch authentication types being used in an engineering group: end-user stations, an IP phone, a printer cluster, and public internet access. [Figure 10-4](#) provides an overview of the fixed switch authentication configuration.

**Figure 10-4 Stackable Fixed Switch Authentication Configuration Example Overview**



Our configuration example consists of the following steps as shown in [Figure 10-4](#) and described in the sections that follow:

1. Configuring policies, RADIUS, and MultiAuth authentication on the switch.
2. Creating RADIUS user accounts on the authentication server.
3. Configuring for the engineering group 802.1x end-user stations, including the IP phone.
4. Configuring the printer cluster MAC authentication.
5. Configuring the public area internet access for PWA.

## Configuring MultiAuth Authentication

MultiAuth authentication must be set to **multi** whenever multiple users of 802.1x need to be authenticated or whenever any MAC-based or PWA authentication is present. For ports where no authentication is present, such as switch to switch, or switch to router connections, you should also set MultiAuth port mode to force authenticate to assure that traffic is not blocked by a failed authentication. For purposes of this example, we will limit authentication to a maximum of 6 users per port.

The following CLI input

- Sets MultiAuth authentication to **multi**.
- Sets ports with switch to switch and switch to router connections to force authenticate.
- Sets the maximum number of users that can authenticate on each port to 6.

```
System(rw)->set multiauth mode multi
System(rw)->set multiauth port mode force-auth ge.1.5-7
System(rw)->set multiauth port numusers 6 ge.1.5-7
System(rw)->set multiauth port mode force-auth ge.1.19-24
System(rw)->set multiauth port numusers 6 ge.1.19-24
```

This completes the MultiAuth authentication configuration piece for this example. Keep in mind that you would want to use the **set multiauth precedence** command to specify which authentication method should take precedence, should you have a single user configured for multiple authentications on the same port.

## Enabling RADIUS On the Switch

The switch needs to be informed about the authentication server. Use the following CLI input to:

- Configure the authentication server IP parameters on the switch.
- Enable the RADIUS server.

```
System(rw)->set radius server 1 10.20.10.01 1812 mysecret
System(rw)->set radius enable
```

## Creating RADIUS User Accounts on the Authentication Server

RADIUS account creation on the authentication server is specific to the RADIUS application you are using. Please see the documentation that comes with your RADIUS application. Create an account for all users to be authenticated.

## Configuring the Engineering Group 802.1x End-User Stations

There are three aspects to configuring 802.1x for the engineering group:

- Configure EAP on each end-user station.
- Set up an account in RADIUS on the authentication server for each end-user station.
- Configure 802.1x on the switch.

Configuring EAP on the end-user station and setting up the RADIUS account for each station is dependent upon your operating system and the RADIUS application being used, respectively. The important thing the network administrator should keep in mind is that these two configurations should be in place before moving on to the 802.1x configuration on the switch.

In an 802.1x configuration, policy is specified in the RADIUS account configuration on the authentication server using the RADIUS Filter-ID. See “[The RADIUS Filter-ID](#)” on page 8 for RADIUS Filter-ID information. If a RADIUS Filter-ID exists for the user account, the RADIUS protocol returns it in the RADIUS Accept message and the firmware applies the policy to the user.



**Note:** Globally enabling 802.1x on a switch sets the port-control type to **auto** for all ports. Be sure to set port-control to **forced-auth** on all ports that will not be authenticating using 802.1x and no other authentication method is configured. Otherwise these ports will fail authentication and traffic will be blocked.

The following CLI input:

- Enables EAP on the stackable fixed switch

```
System(rw)->set eapol enable
```

- Enables 802.1x on the switch
- Sets port-control to **forced-auth** for all connections between switches and routers, because they do not use authentication and would be blocked if not set to **forced-auth**.

```
System(rw)->set dot1x enable
```

```
System(rw)->set dot1x auth-config authcontrolled-portcontrol forced-auth ge.1.5
```

```
System(rw)->set dot1x auth-config authcontrolled-portcontrol forced-auth
ge.1.19
```

```
System(rw)->set dot1x auth-config authcontrolled-portcontrol forced-auth
ge.2.24
```

This completes the 802.1x end-user stations configuration.

## Configuring the Printer Cluster for MAC-Based Authentication

Perform the following tasks to configure MAC-based authentication for the printer cluster in our example:

- Set up an account for each printer on the authentication server that contains the printer MAC address, the MAC authentication password configured on the switch, and a RADIUS Filter-ID entry specifying the printer policy.
- Configure a policy using NetSight Policy Manager specifying the printer cluster VLAN and optionally configuring a CoS and rate limit.
- Enable MAC authentication globally on the switch.
- Enter the MAC authentication password as **enterasys** on the switch.
- Set the MAC authentication significant-bits to **24**.
- Enable MAC authentication on the ports used by the printer cluster: **ge.1.3-4**

With the authentication server configured with a RADIUS account for each printer, and the printer policy pre-configured, enter the following CLI input:

```
System(rw)->set macauthentication enable
```

```
System(rw)->set macauthentication password enterasys
```

```
System(rw)->set macauthentication significant-bits 24
```

```
System(rw)->set macauthentication port enable ge.1.3-4
```

This completes the printer cluster MAC authentication configuration.

## Configuring the Public Area PWA Station

The public area PWA station provides visitors to your business site with open access to the internet, while at the same time isolating the station from any access to your internal network. In order to provide a default set of network resources to communicate over HTTP, policy must be set to only allow DHCP, ARP, DNS, and HTTP. You may want to set a rate limit that would guard against excessive streaming. You will also need to set up RADIUS for the public station account on the authentication server. This configuration will include the guest name, password, and a RADIUS Filter-ID for the public policy.

Perform the following tasks to configure the public station for PWA authentication:

- Configure the policy appropriate to the public station.
- Setup the RADIUS user account for the public station on the authentication server.
- Enable PWA globally on the switch.
- Configure the IP address for the public station.
- Optionally set up a banner for the initial PWA screen.
- Enable PWA enhancedmode so that any URL input will cause the PWA sign in screen to appear.
- Set PWA gueststatus to RADIUS authentication mode.
- Set the PWA login guest name.
- Set the PWA login password.
- Enable PWA on the switch port where the public station is connected.

Once the policy and RADIUS account are configured, enter the following CLI input on the switch:

```
System(rw)->set pwa enable
System(rw)->set pwa ipaddress 10.10.10.101
System(rw)->set pwa banner "Enterasys Networks Public Internet Access Station"
System(rw)->set pwa enhancedmode enable
System(rw)->set pwa gueststatus authradius
System(rw)->set pwa guestname guest
System(rw)->set pwa guestpassword password
System(rw)->set pwa portcontrol enable ge.1.6
```

This completes the Authentication configuration example.

## Terms and Definitions

[Table 10-4](#) lists terms and definitions used in this Authentication configuration discussion.

**Table 10-4 Authentication Configuration Terms and Definitions**

| Term                       | Definition                                                                                                                          |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Authentication Server (AS) | An entity providing authorization services to an authenticator using RADIUS. The authentication server may be at a remote location. |
| Authenticator              | The switch seeking authentication from the authentication server for a supplicant.                                                  |
| Domain Name System (DNS)   | Serves as a means for the Internet to translate human-readable computer hostnames, e.g. www.example.com, into the IP addresses.     |



**Table 10-4 Authentication Configuration Terms and Definitions (continued)**

| Term                                       | Definition                                                                                                                                                                                                                              |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dynamic Host Configuration Protocol (DHCP) | A protocol used by networked clients to obtain various parameters necessary for the clients to operate in an Internet Protocol (IP) network.                                                                                            |
| Extensible Authentication Protocol (EAP)   | A protocol that provides the means for communicating the authentication information in an IEEE 802.1x context.                                                                                                                          |
| IEEE 802.1x                                | An IEEE standard for port-based Network Access Control that provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails.            |
| MAC-based Authentication                   | A means of authenticating a device attempting to gain access to the network based upon the device MAC address and a secret keyword known to the authenticator and the RADIUS application on the authentication server.                  |
| MultiAuth Authentication                   | The ability to authenticate multiple authentication modes for a user and apply the authentication mode with the highest precedence.                                                                                                     |
| Multi-user Authentication                  | The ability to appropriately authenticate multiple supplicants on a single link and provision network resources, based upon policy associated with each supplicant.                                                                     |
| Port Web Authentication (PWA)              | A means of authenticating a user by utilizing a web browser for the login process to authenticate to the network.                                                                                                                       |
| RADIUS Filter-ID                           | An Enterasys proprietary string formatted in the RADIUS Access-Accept packet sent back from the authentication server to the switch containing either the policy to apply to the supplicant, the management type for the port, or both. |
| RADIUS Protocol                            | An AAA (Authentication, Authorization, and Accounting) protocol for controlling access to network resources used by ISPs and corporations managing access to Internet or internal networks across an array of access technologies.      |
| Supplicant                                 | The user or device seeking access to network resources.                                                                                                                                                                                 |



## Configuring Link Aggregation

This chapter describes how to configure link aggregation on the fixed switch platforms.

| For information about...                               | Refer to page... |
|--------------------------------------------------------|------------------|
| <a href="#">Link Aggregation Overview</a>              | 11-1             |
| <a href="#">Configuring Link Aggregation</a>           | 11-9             |
| <a href="#">Link Aggregation Configuration Example</a> | 11-11            |
| <a href="#">Terms and Definitions</a>                  | 11-15            |

### Link Aggregation Overview

IEEE 802.3ad link aggregation provides a standardized means of grouping multiple parallel Ethernet interfaces into a single logical Layer 2 link. The formed group of Ethernet interfaces is referred to as a Link Aggregation Group (LAG). Dynamic LAG formation and activation is provided by the Link Aggregation Control Protocol (LACP).

Each pair of LAG physical ports is made up of a local port on the device responsible for LACP negotiation, referred to as the actor, and its directly linked remote port on the device participating in the LACP negotiation, referred to as the partner. LAGs form automatically based upon a set of criteria (see [“How a LAG Forms”](#) on page 11-3).

Only LAG members in the attached state carry user traffic. Once the LAG is formed, the system ID, made up of a system priority and the device MAC address, determines which device will be in charge of choosing the LAG port members that will be moved to the attached state. While port speed is not a criteria for joining a LAG, the port speed must match for all ports that are placed in the LACP attached state. Aggregatable ports not selected to carry traffic for this LAG are available to the next LAG as long as LAG resources are not depleted. Should LAG resources become depleted, aggregatable ports are placed in LACP standby state.

802.3ad LACP aggregations can be run between combinations of switches, routers, and edge devices, such as a server, that support LACP.



**Note:** Earlier (proprietary) implementations of port aggregation referred to groups of aggregated ports as “trunks”.

### Using Link Aggregation in a Network

The concept of grouping multiple ports into a single link is not a new idea. Cabletron's SmartTrunk, Cisco's Inter Switch Link trunking, and Adaptec's Duralink are previous examples. The problem with these older methods, from the network administrators point of view, is that they are proprietary. Administrators who wanted to implement faster logical links faced major

problems if they also wanted, or needed, to use a different brand of networking hardware. Link aggregation is standards based allowing for interoperability between multiple vendors in the network.

Older implementations required manual configuration. With LACP, if a set of links can aggregate, they will aggregate. LACP's ability to automatically aggregate links represents a timesaver for the network administrator who will not be required to manually configure the aggregates. However, manual overrides are provided for when the administrator needs to customize. Link aggregation also provides for rapid configuration and reconfiguration when there are changes in the physical connections. Link aggregation will automatically and quickly converge the new configuration. This convergence typically occurs in one second or less.

Link aggregation is a cost effective way to implement increased bandwidth. A major benefit of link aggregation is the ability to incrementally add bandwidth in a linear fashion. Without link aggregation, if there is a need to increase the bandwidth for a 100Mbps pipe, the only choice is an exponential upgrade to a 1000Mbps pipe. If there is a need for a 300Mbps pipe, aggregating three 100Mbps ports is both less expensive, because a forklift hardware upgrade is avoided, and makes for more efficient use of the system ports that are already available.

The physical links within the aggregate can serve as redundant backups to one another. Since only a single MAC address representing the entire aggregate is presented to the MAC client, the failure of any link within the aggregate is transparent. Failover is handled within the link aggregation sublayer.

## Implementing Link Aggregation

To implement link aggregation:

- Enable LACP on the network device
- Optionally set a non-default system priority for the device
- Optionally change the administratively assigned key for each port on the device
- Optionally enable single port LAGs on the device
- Enable LACP port state on B5 and C5 platforms
- Optionally change LAG parameters on each port
- Optionally assign static ports to a LAG when the partner device only supports a non-LACP method of aggregation

## LACP Operation

In order to allow LACP to determine whether a set of links connect to the same device, and to determine whether those links are compatible from the point of view of aggregation, it is necessary to be able to establish:

- A globally unique identifier for each device that participates in link aggregation.
- A means of identifying the set of capabilities associated with each port and with each aggregator, as understood by a given device.
- A means of identifying a LAG and its associated aggregator.

For each aggregatable port in the device, LACP:

- Maintains configuration information (reflecting the inherent properties of the individual links as well as those established by network administration) to control aggregation.
- Exchanges configuration information with other devices to allocate the link to a LAG.



**Note:** A given link is allocated to, at most, one LAG at a time. The allocation mechanism attempts to maximize aggregation, subject to management controls.

- Attaches the port to the aggregator used by the LAG, and detaches the port from the aggregator when it is no longer used by the LAG.
- Uses information from the partner device's link aggregation control entity to decide whether to aggregate ports.

The operation of LACP involves the following activities:

- Checking that candidate links can actually be aggregated.
- Controlling the addition of a link to a LAG and the creation of the group if necessary.
- Monitoring the status of aggregated links to ensure that the aggregation is still valid.
- Removing a link from a LAG if its membership is no longer valid, and removing the group if it no longer has any member links.

Multi-port LAGs will continue to operate as long as there is at least one active port in the LAG. Therefore, there is no need to create backup single port LAGs or to specifically assign the LAG and all its physical ports to the egress list of the LAG's VLAN.

## How a LAG Forms

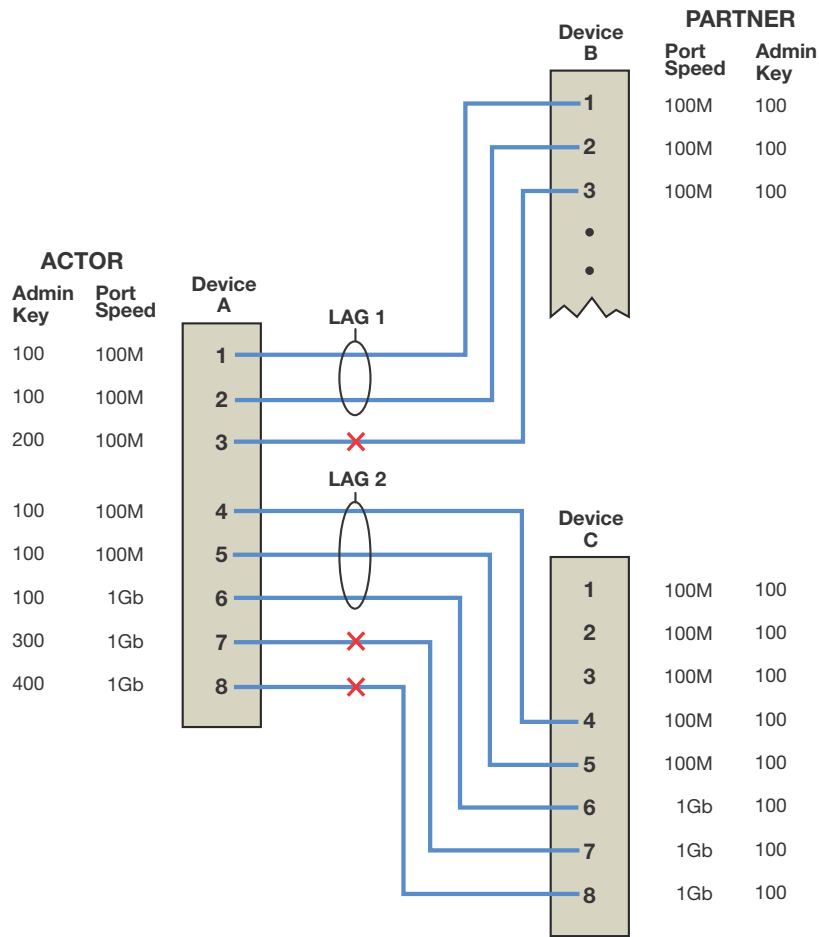
LAGs form automatically with LACP enabled on the device. There are four criteria for forming a LAG. Both actor and partner ports must:

1. Operate in full duplex mode.
2. Have matching local LAG and physical port admin keys for the device controlling LAG formation.
3. Operate in parallel in that a LAG can have only two devices associated with it.
4. Consist of two or more physical actor to partner port pairings unless the single port LAG feature is enabled.

[Figure 11-1](#) on page 11-4 displays a LAG formation example containing three devices with five 100Mbps ports and three 1Gb ports configured. For this example, all ports are operating in full-duplex mode, and the admin key for all LAG ports has been set to 100. Device A is the actor and therefore determines which ports will join a LAG. Devices B and C are the partners.

In our example two LAGs have formed because the actor ports are shared between two partner devices. Attempting to form a single LAG using all the actor ports would have broken the rule that actor and partner ports must operate in parallel.

Figure 11-1 LAG Formation



Actor ports 1 - 3 on device A directly connect to partner ports 1 - 3 on device B:

- We have already stated that all ports are operating in full-duplex mode, so rule 1 is satisfied for all three ports.
- Investigating the port admin keys, we see that ports 1 and 2 on device A are set to 100 (the same setting as all LAG ports on the device), while port 3 on device A is set to 200. Because the port admin keys are the same for both the LAG port and these physical ports, ports 1 and 2 satisfy rule 2. Because the admin key for physical port 3 is different from any possible LAG for this device, port 3 can not be part of any LAG.
- Because ports 1 and 2 for both the actor and partner operate in parallel with each other, rule 3 is satisfied for these ports.
- Rule 4 is satisfied, regardless of whether single port LAGs are enabled, because there are two aggregatable port pairings between devices A and B.

For these reasons, LAG 1 (lag.0.1) is formed using actor and partner ports 1 and 2.

Actor ports 4 - 8 on device A directly connect to partner ports 4 - 8 on device C:

- Because all ports are operating in full-duplex mode, rule one is satisfied for all five ports.

- Investigating port admin keys, we see that ports 4 - 6 on device A are set to 100 (the same setting as all LAG ports on the device), while ports 7 and 8 on device A are set to 300 and 400, respectively. Because port admin keys for all LAGs and the physical ports 4 - 6 are the same, physical ports 4 - 6 satisfy rule 2. Because the admin key settings for physical ports 7 and 8 do not agree with any LAG admin key setting on the device, ports 7 and 8 can not be part of any LAG.
- Because ports 4 - 6 for both the actor and partner operate in parallel with each other, rule 3 is satisfied for these ports.
- Rule 4 is satisfied, regardless of whether single port LAG is enabled, because there are three aggregatable port pairings between devices A and C.

For these reasons, LAG 2 (lag.0.2) is formed using actor and partner ports 4 - 6.



**Note:** Port speed is not a consideration in the forming phase for LAGs. LAG 2 contains 100Mbps and 1Gb port members.

There are a few cases in which ports will not aggregate:

- An underlying physical port is attached to another port on this same switch (loopback).
- There is no available aggregator for two or more ports with the same LAG ID. This can happen if there are simply no available aggregators, or if none of the aggregators have a matching admin key and system priority.
- 802.1x authentication is enabled using the **set eapol** command and ports that would otherwise aggregate are not 802.1X authorized.

## Attached Ports

Once a LAG is formed, two steps must take place before traffic can pass over the LAG:

- The device that will choose which ports to move to the attached state must be identified
- The process of moving the chosen ports to the LACP attached state must take place

A system ID, made up of the device MAC address and the system priority, is associated with each device. The device with the lower system priority is in charge of selecting the LAG members to move to the attached state. If a system priority tie occurs, the system with the lower MAC address value breaks the tie.

Only LAG members with the same port speed can be moved to the attached state. In a case where multiple speeds are present in a LAG, the LAG member with the lowest port priority on the device in charge, as well as all other members with the same port speed as the member with the lowest port priority, are selected and moved to the attached state. Using LAG2 in [Figure 11-1](#) on page 11-4 as an example, if the LAG2 member port priorities are set as shown in [Table 11-1](#) on page 11-5, ports 4 and 5 are moved to the attached state.

**Table 11-1 LAG2 Port Priority Assignments**

| Port Number | Port Speed | Port Priority |
|-------------|------------|---------------|
| 4           | 100Mbps    | 200           |
| 5           | 100Mbps    | 300           |
| 6           | 1Gb        | 300           |

This is true because port 4 has the lowest priority of the three ports currently in the LAG, and port 5 has the same speed as the port with the lowest priority in the LAG, regardless of its priority.

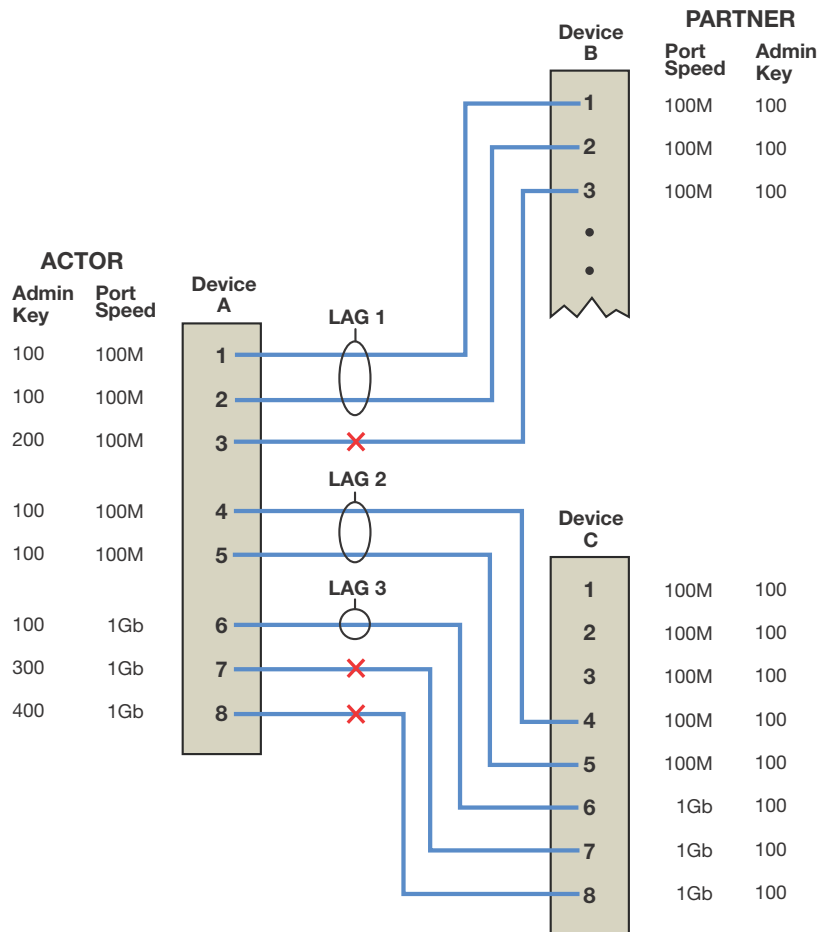
Because port 6 has both a different speed and a higher priority than the port with the lowest priority in the LAG, it is not moved to the attached state.

If LAG members with different port speeds should tie for the lowest port priority, the LAG member with the lowest port number breaks the tie. In our example, should all three ports have the same port priority, ports 4 and 5 would still be the ports moved to the attached state because port 4 has the lowest port number and port 5 has the same port speed as port 4.

If in our example you wanted the reverse outcome of port 6 moved to the attached state instead of ports 4 and 5, setting port 6 to a lower priority than ports 4 and 5, as well as enabling the single port LAG feature on this device, would accomplish that goal.

Aggregatable ports not moved to the attached state are made available to form another LAG providing a LAG resource is available for this system. Port 6 in [Figure 11-1](#) on page 11-4, was not moved to the attached state. The only criteria port 6 does not meet to form its own LAG is rule 4: being a single aggregatable port. The single port LAG feature must be enabled for port 6 to form a LAG. If single port LAG is enabled on this system, port 6 would form and attach to LAG 3. [Figure 11-2](#) illustrates the three LAGs described in this example.

**Figure 11-2 LAGs Moved to Attached State**



Should an aggregatable port be available with all LAG resources depleted for this system, the port is placed in LACP standby state. Ports in standby state do not forward traffic. If all ports initially moved to the attach state for a given LAG become unavailable, a LAG resource will then be available. LACP will initiate a new selection process using the ports in standby state, using the same rules as the initial process of forming LAGs and moving ports to the attached state.



## Single Port Attached State Rules

By default, a LAG must contain two or more actor and partner port pairs for the LAG to be initiated by this device. A feature exists to allow the creation of a single port LAG that is disabled by default. If single port LAG is enabled, a single port LAG can be created on this device. If single port LAG is disabled, a single port LAG will not be initiated by this device. If a peer device is able to form a single port LAG and advertises its willingness to do so, a single port LAG can form. There are three conditions under which a single port LAG can exist and the LAG member can be moved to the attached state:

- The single port LAG feature is enabled.  
or,
- The single port LAG feature is disabled, but the peer device is able and willing to form a single port LAG.  
or,
- An already existing LAG configuration persists through a device or module reset. If upon reset there is only a single port active for an already existing LAG, that single port will move to the attached state regardless of the single port LAG setting.

## LAG Port Parameters

LAG port parameters can be changed per port.

[Table 11-2](#) specifies the LACP port parameters that can be changed.

**Table 11-2 LAG Port Parameters**

| Term           | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port Admin Key | The port admin key can be set for both the actor and partner side of the link. The admin key only affects the local device. LACP uses this value to determine which underlying physical ports are capable of aggregating. Aggregator ports allow only underlying ports with physical port and LAG admin keys that match to join a LAG. Setting the physical port admin key to a different value than any LAG resource on the device will ensure that this link does not join a LAG. Valid values are <b>1 - 65535</b> . Default value is <b>32768</b> .                                                                                                                                                                                                                                                                                        |
| Port Priority  | Port priority can be set for both the actor and partner side of the link. The port priority plays a role in determining which set of ports will move to the attached state and pass traffic. The lower port priority, for the port on the system in charge of selecting ports to move to the attached state, determines which ports will actually move to the attached state. If a LAG is made up of ports with different speeds, setting a lower port priority to ports with the desired speed for the LAG will ensure that those ports move to the attached state. Port priority is also used to determine which ports join a LAG if the number of ports available exceeds the number of ports supported for that device. Valid values are <b>0 - 65535</b> , with lower values designating higher priority. Default value is <b>32768</b> . |

**Table 11-2 LAG Port Parameters (continued)**

| Term                      | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrative State      | <p>A number of port level administrative states can be set for both the actor and partner ports. The following port administrative states are set by default:</p> <ul style="list-style-type: none"> <li>• <b>lacpactive</b> - Transmitting LACP PDUs is enabled.</li> <li>• <b>lacptimeout</b> - Transmitting LACP PDUs every 30 seconds. If this state is disabled, LACP PDUs are transmitted every 1 second. Note that the actor and partner LACP timeout values must agree.</li> <li>• <b>lacpagg</b> - Aggregation on this port is enabled.</li> <li>• <b>lacpsync</b> - Transition to synchronization state is allowed.</li> <li>• <b>lacpcollect</b> - Transition to collection state is allowed.</li> <li>• <b>lacpdist</b> - Transition to distribution state is allowed.</li> <li>• <b>lacpdef</b> - Transition to defaulted state is allowed.</li> <li>• <b>lacpexpire</b> - Transition to expired state is allowed.</li> </ul> <p>It is recommended that these default states not be changed unless you know what you are doing. Contact Enterasys customer support should you need assistance modifying port level administrative states.</p> |
| Partner Default System ID | A default partner system ID can be set. This is a default MAC address for the system partner.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| LACP PDU processing       | (Optional) LACP PDU processing can be enabled or disabled for this port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## Static Port Assignment

Static port assignment allows you to assign ports to a LAG when the partner device does not support LACP, but does support another proprietary form of link aggregation. To assign a static port, specify the LAG port ID, the admin key value for this LAG, and the ports to be assigned. If you do not specify an admin key value, a key will be assigned according to the specified aggregator. For example, a key of 4 would be assigned to lag.0.4.

## Flexible Link Aggregation Groups



**Note:** Flexible link aggregation groups are not supported on the I-Series platforms. Up to 6 LAGs, with a maximum of 8 associated physical ports per LAG, can be configured.

Starting with firmware v6.61, you can define the maximum number of Link Aggregation Groups (LAGs) that can be supported on the switch, although the maximum number of physical ports on the switch that can be aggregated remains at 48 ports. Use the command **set lacp groups** to set the maximum number of LAGs to 6, 12, or 24. Since the maximum number of physical aggregatable ports remains 48, if you set the maximum number of LAGs to:

- 6, each LAG can have up to 8 associated physical ports. This is the system default.
- 12, each LAG can have up to 4 associated physical ports.
- 24, each LAG can have up to 2 associated physical ports.

Changing the maximum number of LAGs requires a system reset and the LACP configuration will be returned to default values. You are prompted to confirm the change before the system executes the command.

The virtual link aggregation ports continue to be designated as lag.0.x, where x can range from 1 to 24, depending on the maximum number of LAGs configured.

## Configuring Link Aggregation

This section provides details for the configuration of link aggregation on the N-Series, S-Series, stackable, and standalone switch products.

[Table 11-3](#) lists link aggregation parameters and their default values.

**Table 11-3 Default Link Aggregation Parameters**

| Parameter                         | Description                                                                                                                                                                                                    | Default Value                                                                                              |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| LACP State                        | Current state of LACP on the device.                                                                                                                                                                           | Enabled                                                                                                    |
| System Priority                   | LACP system priority for this device.                                                                                                                                                                          | 32768                                                                                                      |
| Port Key                          | The Port Administrative Key (also referred to as operational key).                                                                                                                                             | 32768                                                                                                      |
| Port Priority                     | Determines which ports move to the attached state when ports of different speeds form a LAG. Also determines which ports join a LAG if the ports available exceed the number of ports supported by the device. | 32768                                                                                                      |
| Single Port State                 | Allows or disallows a LAG to be created with a single port.                                                                                                                                                    | Disabled (disallows creation of a single port LAG)                                                         |
| LACP Port Active State            | Port state providing for transmission of LACP PDUs.                                                                                                                                                            | B3, C3, G-Series, I-Series: Enabled<br>B5, C5: Disabled                                                    |
| LACP Port Timeout State           | Port state determining the frequency of LACP PDU transmission and period before declaring the partner LACP port down if no response is received.                                                               | 30 second: frequency of LACP PDU transmission<br>90 seconds: period before declaring the partner port down |
| Number of link aggregation groups | The maximum number of link aggregation groups (LAGs) that can be supported. Number can be 6, 12, or 24.                                                                                                        | 6 LAGs, each with a maximum of 8 physical ports attached.                                                  |

[Procedure 11-1](#) describes how to configure link aggregation.

### Procedure 11-1 Configuring Link Aggregation

| Step | Task                                                                                                                                                                                                                                                  | Command(s)                             |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| 1.   | Optionally, change the number of LAGs supported from the default of 6.<br><br>Changing the group limit will result in a system reset and LACP configuration settings will be returned to their default values, with the exception of the group limit. | <code>set lacp groups {6 12 24}</code> |
| 2.   | Enable LACP on the device. LACP global state is enabled by default for all devices.                                                                                                                                                                   | <code>set lacp {disable enable}</code> |
| 3.   | Optionally, change the system priority for the device.                                                                                                                                                                                                | <code>set lacp asyspri value</code>    |

**Procedure 11-1 Configuring Link Aggregation (continued)**

| Step | Task                                                                                                                                                                                                                                                                          | Command(s)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.   | Optionally, change the administratively assigned key for each aggregation on the device.                                                                                                                                                                                      | <b>set lacp aadminkey</b> <i>port-string value</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 5.   | Optionally, enable single port LAGs on the device.                                                                                                                                                                                                                            | <b>set lacp singleportlag</b> {enable   disable}                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 6.   | Optionally, modify the LAG port parameters. See <a href="#">Table 11-2</a> on page 11-7 for a description of port parameters.<br>If necessary, enable LACP on the port. See <a href="#">Table 11-3</a> on page 11-9 for the default LACP port active state for your platform. | <b>set port lacp port</b> <i>port-string</i><br>{<br>[aadminkey <i>aadminkey</i> ] [aportpri <i>aportpri</i> ]<br>[padminsyspri <i>padminsyspri</i> ] [padminsysid <i>padminsysid</i> ] [padminkey <i>padminkey</i> ]<br>[padminportpri <i>padminportpri</i> ] [padminport <i>padminport</i> ]<br><br>[aadminstate {lacpactive   lacptimeout   lacpagg   lacpsync   lacpcollect   lacpdist   lacpdef   lacpexpire}]<br><br>[padminstate {lacpactive   lacptimeout   lacpagg   lacpsync   lacpcollect   lacpdist   lacpdef   lacpexpire}]<br><br>[enable   [disable]]<br>} |
| 7.   | Optionally, assign static ports to a LAG when the partner device only supports a non-LACP method of aggregation.                                                                                                                                                              | <b>set lacp static</b> <i>lagportstring</i> [ <i>key</i> ] <i>port-string</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

[Table 11-4](#) describes how to manage link aggregation.

**Table 11-4 Managing Link Aggregation**

| Task                                                                                                                                                                | Command                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reset LACP system priority or admin key settings to the default values.                                                                                             | <b>clear lacp</b> {[asyspri] [aadminkey <i>port-string</i> ]}                                                                                                                                                                                                                                                                                                                                                         |
| Remove specific static ports from an aggregation.                                                                                                                   | <b>clear lacp static</b> <i>lagportstring port-string</i>                                                                                                                                                                                                                                                                                                                                                             |
| Reset the single port LAG feature to the default value of disabled.                                                                                                 | <b>clear lacp singleportlag</b>                                                                                                                                                                                                                                                                                                                                                                                       |
| Reset a link aggregation port setting to the default value for one or more ports. See <a href="#">Table 11-2</a> on page 11-7 for a description of port parameters. | <b>clear port lacp port</b> <i>port-string</i><br>{<br>[aadminkey] [aportpri] [padminsyspri] [padminsysid]<br>[padminkey] [padminportpri] [padminport]<br><br>[aadminstate {lacpactive   lacptimeout   lacpagg   lacpsync   lacpcollect   lacpdist   lacpdef   lacpexpire   all}]<br><br>[padminstate {lacpactive   lacptimeout   lacpagg   lacpsync   lacpcollect   lacpdist   lacpdef   lacpexpire   all}]<br><br>} |

**Table 11-4 Managing Link Aggregation (continued)**

| Task                                                                                                                                                                                                                                                                                          | Command                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| Reset the maximum number of LACP groups to the default of 6.<br><br>If the number of LACP groups has been changed from the default, executing this command will result in a system reset and LACP configuration settings will be returned to their default values, including the group limit. | <code>clear lacp groups</code> |

[Table 11-5](#) describes how to display link aggregation information and statistics.

**Table 11-5 Displaying Link Aggregation Information and Statistics**

| Task                                                                                             | Command                                                                                 |
|--------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Display the global LACP enable state, or display information about one or more aggregator ports. | <code>show lacp [state   port-string]</code>                                            |
| Display the status of the single port LAG function.                                              | <code>show lacp singleportlag</code>                                                    |
| Display link aggregation information for one or more underlying physical ports.                  | <code>show port lacp port port-string {[status {detail   summary}]   [counters]}</code> |
| Display the maximum number of LACP groups configured on the switch.                              | <code>show lacp groups</code>                                                           |

## Link Aggregation Configuration Example

This example provides a link aggregation configuration example that includes a fixed switch stack as an edge switch, an S8 distribution switch, and a second fixed switch stack that will aggregate both end-users at the edge and the data from a local server.

See [Figure 11-3](#) on page 11-12 for an illustration of this example, including port, key, and system priority assignments.

Three LAGs are created for the example:

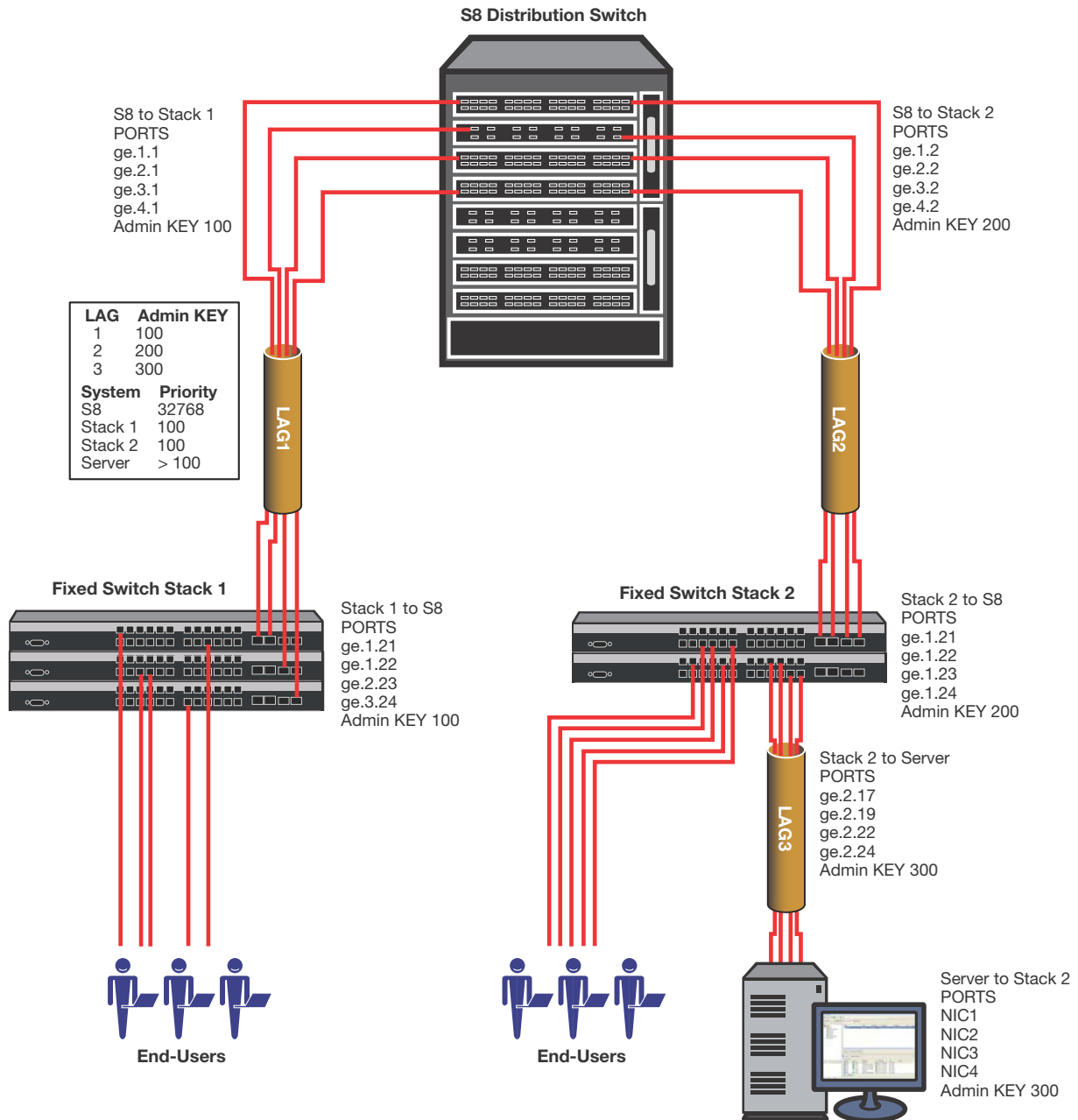
- LAG 1 provides an uplink aggregate of four 1Gb ports for the fixed switch stack of three C5 switches (Stack 1) to the S8 distribution switch.
- LAG2 provides an uplink aggregate of four 1Gb ports for the fixed switch stack of two C5 switches (Stack 2) to the S8 distribution switch for both the end-user and server data flows.
- LAG3 provides an aggregate of four 1Gb ports between the fixed switch stack of two C5 switches (Stack 2) and the server.

Each LAG consists of four ports. The primary goal of the aggregates in this example is to provide link and slot redundancy for the affected data streams. With that in mind, LAG members are spread between available system slots. Four out of the five S8 available slots are used providing complete redundancy at the S8. All three switches are used in the Stack 1. The four ports from the server to the Stack 2 switches and the Stack 2 switches to the S8 are evenly split between the two stackable switches.

For this example we will manually configure the LAGs that will form and prevent any other LAGs from forming. Because we have specific port to LAG goals in mind, the first thing we want to do

on each device is to ensure that LAGs form only where we configure them. Since the admin key for the LAG and its associated ports must agree for the LAG to form, an easy way to ensure that LAGs do not automatically form is to set the admin key for all LAGs on all devices to a non-default value. The physical ports will initially retain admin key defaults. In our example, the admin keys for all LAGs are set to the highest configurable value of 65535.

Figure 11-3 Link Aggregation Example



Both physical port and LAG admin keys will be set as shown in Table 11-6 to ensure that the LAGs form only for the desired ports.

**Table 11-6 LAG and Physical Port Admin Key Assignments**

| Device                        | LAG      | LAG Admin Key | Physical Port | Physical Port Admin Key |
|-------------------------------|----------|---------------|---------------|-------------------------|
| <b>S8 Distribution Switch</b> | <b>1</b> | 100           | ge.1.1        | 100                     |
|                               |          |               | ge.2.1        | 100                     |
|                               |          |               | ge.3.1        | 100                     |
|                               |          |               | ge.4.1        | 100                     |
|                               | <b>2</b> | 200           | ge.1.2        | 200                     |
|                               |          |               | ge.2.2        | 200                     |
|                               |          |               | ge.3.2        | 200                     |
|                               |          |               | ge.4.2        | 200                     |
| <b>Fixed Switch Stack 1</b>   | <b>1</b> | 100           | ge.1.21       | 100                     |
|                               |          |               | ge.1.22       | 100                     |
|                               |          |               | ge.2.23       | 100                     |
|                               |          |               | ge.3.24       | 100                     |
| <b>Fixed Switch Stack 2</b>   | <b>2</b> | 200           | ge.1.21       | 200                     |
|                               |          |               | ge.1.22       | 200                     |
|                               |          |               | ge.1.23       | 200                     |
|                               |          |               | ge.1.24       | 200                     |
|                               | <b>3</b> | 300           | ge.2.17       | 300                     |
|                               |          |               | ge.2.19       | 300                     |
|                               |          |               | ge.2.22       | 300                     |
|                               |          |               | ge.2.24       | 300                     |
| <b>Server</b>                 | <b>3</b> | 300           | NIC1 ETH      | 300                     |
|                               |          |               | NIC2 ETH      | 300                     |
|                               |          |               | NIC3 ETH      | 300                     |
|                               |          |               | NIC4 ETH      | 300                     |

Which device determines port selection for the LAG is an optional consideration. If system priorities remain at the default value, the lowest MAC address device determines port selection for the LAG. For purposes of this example, we will set the system priority of the fixed switch Stack 1 to 100 to ensure it will control port selection for LAG1, instead of the S8. The fixed switch Stack 2 system priority will be set to 100 to ensure it will control port selection for LAG2, instead of the S8. For the stackable switch to control port selection for LAG3 requires that you ensure that the server has a system priority higher than 100.

Each LAG in our example is made up of physical ports of the same speed, so there is no need to set the port priority to a non-default value. The only port value to be changed is the admin key for each physical port and each LAG. These modifications are detailed in [Table 11-6](#) on page 11-13.

Given that the intent of the example is to have three LAGs of 4 ports each, there is no need to enable the single port LAG feature. Once the LAGs initiate, they will persist across resets. Should only a single port be active after a reset, the LAG will form regardless of the single port LAG feature setting.

The output algorithm defaults to selecting the output port based upon the destination and source IP address. This setting will not be changed in our example. In any case, note that the stackable switch does not support the output algorithm feature.

## Configuring the S8 Distribution Switch

The first thing we want to do is set the admin key for all LAGs to the non-default value of 65535 so that no LAGs will automatically form:

```
S8(rw)->set lacp aadminkey lag.0.* 65535
```

LAGs 1 and 2 will form on the S8 so we need to set the admin keys for these LAGs:

```
S8(rw)->set lacp aadminkey lag.0.1 100
S8(rw)->set lacp aadminkey lag.0.2 200
```

LACP port state is disabled by default on the S8, so we will enable LACP port state here. We next want to set the admin keys and port enable LACP for the S8 physical ports:

```
S8(rw)->set port lacp port ge.1.1 aadminkey 100 enable
S8(rw)->set port lacp port ge.2.1 aadminkey 100 enable
S8(rw)->set port lacp port ge.3.1 aadminkey 100 enable
S8(rw)->set port lacp port ge.4.1 aadminkey 100 enable
S8(rw)->set port lacp port ge.1.2 aadminkey 200 enable
S8(rw)->set port lacp port ge.2.2 aadminkey 200 enable
S8(rw)->set port lacp port ge.3.2 aadminkey 200 enable
S8(rw)->set port lacp port ge.4.2 aadminkey 200 enable
```

Because we want the two fixed switch stacks to be in charge of port selection, the system priority for the S8 will be left at the default value of 32768.

## Configuring the Fixed Switch Stack 1

The first thing we want to do is set the admin key for all LAGs to the non-default value of 65535 so that no LAGs will automatically form:

```
Stack1(rw)->set lacp aadminkey lag.0.* 65535
```

LAG 1 will form on the fixed switch Stack 1 so we need to set the admin key for this LAG:

```
Stack1(rw)->set lacp aadminkey lag.0.1 100
```

LACP port state is disabled by default on the B5s and C5s, so we will enable LACP port state here. We next want to set the admin keys and port enable LACP for the physical ports:

```
Stack1(rw)->set port lacp port ge.1.21 aadminkey 100 enable
Stack1(rw)->set port lacp port ge.1.22 aadminkey 100 enable
Stack1(rw)->set port lacp port ge.2.23 aadminkey 100 enable
Stack1(rw)->set port lacp port ge.3.24 aadminkey 100 enable
```

Next we want to change the system priority for the Stack 1 so that it will be in charge of port selection on LAG1:

```
Stack1(rw)->set lacp asyspri 100
```

## Configuring the Fixed Switch Stack 2

The first thing we want to do is set the admin key for all LAGs to the non-default value of 65535 so that no LAGs will automatically form:

```
Stack2(rw)->set lacp aadminkey lag.0.* 65535
```

LAGs 2 and 3 will form on Stack 2 so we need to set the admin key for this LAG:

```
Stack2(rw)->set lacp aadminkey lag.0.2 200
Stack2(rw)->set lacp aadminkey lag.0.3 300
```



LACP port state is disabled by default on the B5s and C5s, so we will enable LACP port state here. We next want to set the admin keys for the stackable switch physical ports:

```
Stack2(rw)->set port lacp port ge.1.21 aadminkey 200 enable
Stack2(rw)->set port lacp port ge.1.22 aadminkey 200 enable
Stack2(rw)->set port lacp port ge.1.23 aadminkey 200 enable
Stack2(rw)->set port lacp port ge.1.24 aadminkey 200 enable
Stack2(rw)->set port lacp port ge.2.17 aadminkey 300 enable
Stack2(rw)->set port lacp port ge.2.19 aadminkey 300 enable
Stack2(rw)->set port lacp port ge.2.22 aadminkey 300 enable
Stack2(rw)->set port lacp port ge.2.24 aadminkey 300 enable
```

Next we want to change the system priority for Stack 2 so that it will be in charge of port selection on LAGs 2 and 3:

```
Stack2(rw)->set lacp asyspri 100
```

## Configuring the Server

Configuring link aggregation on the server is dependent upon the installed LACP application. There are three aspects to link aggregation on the server you must ensure for this example:

- The admin key for LAG3 must be set to 300
- The admin keys for each NIC port must be set to 300
- The system priority for the server must be set greater than 100 to ensure that the fixed switch stack will control port selection

This completes the example configuration.

## Terms and Definitions

[Table 11-7](#) lists terms and definitions used in this link aggregation configuration discussion.

**Table 11-7 Link Aggregation Configuration Terms and Definitions**

| Term              | Definition                                                                                                                                                                                                                                                                                                                                     |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Aggregator        | Virtual port that controls link aggregation for underlying physical ports. Each device provides aggregator ports, which are designated in the CLI as <b>lag.0.1</b> through <b>lag.0.x</b> . (See <a href="#">“Flexible Link Aggregation Groups”</a> on page 11-8.)                                                                            |
| LAG               | Link Aggregation Group. Once underlying physical ports (i.e.; <b>fe.x.x</b> , or <b>ge.x.x</b> ) are associated with an aggregator port, the resulting aggregation will be represented as one LAG with a <b>lag.x.x</b> port designation.                                                                                                      |
| LACPDU            | Link Aggregation Control Protocol Data Unit. The protocol exchanges aggregation state/mode information by way of a port’s actor and partner operational states. LACPDU’s sent by the first party (the actor) convey to the second party (the actor’s protocol partner) what the actor knows, both about its own state and that of its partner. |
| Actor and Partner | An actor is the local device sending LACPDU’s. Its protocol partner is the device on the other end of the link aggregation. Each maintains current status of the other via LACPDU’s containing information about their ports’ LACP status and operational state.                                                                               |
| Admin Key         | Value assigned to aggregator ports and physical ports that are candidates for joining a LAG. The LACP implementation uses this value to determine which underlying physical ports are capable of aggregating by comparing keys. Aggregator ports allow only underlying ports with admin keys that match the aggregator to join their LAG.      |

**Table 11-7 Link Aggregation Configuration Terms and Definitions (continued)**

| <b>Term</b>     | <b>Definition</b>                                                                                                                                                                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port Priority   | Port priority determines which physical ports are moved to the attached state when physical ports of differing speeds form a LAG. Port priority also determines which ports will join a LAG when the number of supported ports for a LAG is exceeded.                                         |
| System Priority | Value used to build a LAG ID, which determines aggregation precedence. If there are two partner devices competing for the same aggregator, LACP compares the LAG IDs for each grouping of ports. The LAG with the lower LAG ID is given precedence and will be allowed to use the aggregator. |

---

## Configuring SNMP

This chapter describes basic SNMP concepts, the SNMP support provided on Enterasys fixed stackable and standalone switches, and how to configure SNMP on the switches using CLI commands.

| For information about...                           | Refer to page... |
|----------------------------------------------------|------------------|
| <a href="#">SNMP Overview</a>                      | 12-1             |
| <a href="#">SNMP Concepts</a>                      | 12-2             |
| <a href="#">SNMP Support on Enterasys Switches</a> | 12-3             |
| <a href="#">Configuring SNMP</a>                   | 12-7             |
| <a href="#">Reviewing SNMP Settings</a>            | 12-18            |

### SNMP Overview

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. The most widely used management protocol on Internet Protocol (IP) networks, it helps you monitor network performance, troubleshoot problems, and plan for network growth.

SNMP's simplicity lies in the fact that it uses a basic set of command messages to relay notifications of events and error conditions over a connectionless communication link.

Most network devices support the three versions of the protocol: SNMPv1, SNMPv2c, and SNMPv3. The latest version, SNMPv3, provides enhanced security and administrative features as described in this document.

SNMP is a simple, cost-effective tool for monitoring your network devices for conditions that warrant administrative attention. It is widely used because it is:

- Easily integrated into your existing LAN topology
- Based on an open standard, making it non-proprietary and well documented
- Flexible enough to communicate the specific conditions you need monitored in your network
- A common management platform supported by many network devices

### Implementing SNMP

You can implement SNMP on Enterasys switching devices using simple CLI commands as described in this document. The configuration process involves the following tasks:

1. Creating users and groups allowed to manage the network through SNMP

2. Setting security access rights
3. Setting SNMP Management Information Base (MIB) view attributes
4. Setting target parameters to control the formatting of SNMP notification messages
5. Setting target addresses to control where SNMP notifications are sent
6. Setting SNMP notification parameters (filters)
7. Reviewing SNMP statistics

## SNMP Concepts

### Manager/Agent Model Components

SNMP provides a message format for communication between managers and agents, which use a MIB and a relatively small set of commands to exchange information. The SNMP manager can be part of a network management system, such as Enterasys NetSight<sup>®</sup>, while the agent and MIB reside on the switch.

The SNMP agent acts upon requests from the manager to either collect data from the MIB or set data into the MIB. A repository for information about device parameters and network data, the MIB is organized in a tree structure in which individual variables are represented as leaves on the branches. A unique object identifier (OID) distinguishes each variable in the MIB and is the means by which the manager and agent specify which managed elements are changed.

An agent can send unsolicited notification messages (also known as traps or informs) alerting the SNMP manager to a condition on the network. These conditions include such things as improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events.

### Message Functions

SNMP uses five basic message types (Get, Get Next, Get Response, Set, and Trap) to communicate between the manager and the agent. The Get and Get Next messages allow the manager to request information for a specific variable. The agent, upon receiving a Get or Get Next message, will issue a Get Response message to the manager with either the information requested or an error indication about why the request cannot be processed.

A Set message allows the manager to request a change to a specific variable. The agent then responds with a Get Response message indicating the change has been made or an error indication about why the change cannot be made.

A trap or inform message allows the agent to spontaneously inform the manager of an “important” event in the network.

The SNMP manager and agent use information in the MIB to perform the operations described in [Table 12-1](#).

**Table 12-1 SNMP Message Functions**

| Operation                     | Function                                                                                                                                      |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| get-request                   | Retrieves a value from a specific variable.                                                                                                   |
| get-next-request              | Retrieves a value from a variable within a table. <sup>1</sup>                                                                                |
| get-bulk-request <sup>2</sup> | Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data. |

**Table 12-1 SNMP Message Functions (continued)**

| Operation                  | Function                                                                                  |
|----------------------------|-------------------------------------------------------------------------------------------|
| get-response               | Replies to a get-request, get-next-request, and set-request sent by a management station. |
| set-request                | Stores a value in a specific variable.                                                    |
| trap   inform <sup>3</sup> | Unsolicited message sent by an SNMP agent to an SNMP manager when an event has occurred.  |

1. With this operation, an SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
2. The get-bulk operation is only supported in SNMPv2c or later.
3. Inform notifications are only supported in SNMPv3.

## Trap Versus Inform Messages

As compared to earlier versions, SNMPv3 provides a higher degree of reliability for notifying management stations when critical events occur. Traditionally, SNMP agents communicated events to SNMP managers via “traps.” However, if a temporary network problem prevented the manager from receiving the trap, then the trap would be lost. SNMPv3 provides “informs”, which are a more reliable form of traps. The SNMP agent initiates the inform process by sending an inform request to the manager. The manager responds to the inform request to acknowledge receipt of the message. If the inform is not received by the manager, the inform request will timeout and a new inform request will be sent. Subsequent inform requests will be sent as previous requests time-out until either an acknowledgement is received from the manager, or until a pre-specified retry-count is reached.

## Access to MIB Objects

SNMP uses the following authentication methods to grant user access to MIB objects and functions.

### Community Name Strings

Earlier SNMP versions (v1 and v2c) rely on community name strings for authentication. In order for the network management station (NMS) to access the switch, the community string definitions on the NMS must match at least one of the three community string definitions on the switch. A community string can have one of these attributes:

- Read-only (**ro**)—Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access.
- Read-write (**rw**)—Gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community strings.

### User-Based

SNMPv3 provides a User-Based Security Model (USM) which relies on a user name match for authenticated access to network management components.

Refer to “[Security Models and Levels](#)” on page 12-6 for more information.

## SNMP Support on Enterasys Switches

By default, SNMP Version 1 (SNMPv1) is configured on Enterasys switches. The default configuration includes a single community name - **public** - which grants read-write access to the whole MIB tree for both SNMPv1 and SNMPv2c.

## Versions Supported

Enterasys devices support three versions of SNMP:

- Version 1 (SNMPv1) — This is the initial implementation of SNMP. Refer to RFC 1157 for a full description of functionality.
- Version 2 (SNMPv2c) — The second release of SNMP, described in RFC 1907, has additions and enhancements to data types, counter size, and protocol operations.
- Version 3 (SNMPv3) — This is the most recent version of SNMP, and includes significant enhancements to administration and security. The major difference between SNMPv3 and earlier versions is that v3 provides a User-Based Security Model (USM) to associate users with managed access to security information. In addition to better security and better access control, SNMPv3 also provides a higher degree of reliability for notifying management stations when critical events occur.

SNMPv3 is fully described in RFC 2571, RFC 2572, RFC 2573, RFC 2574, and RFC 2575.

## SNMPv1 and v2c Network Management Components

The Enterasys implementation of SNMPv1 and v2c network management components fall into the following three categories:

- Managed devices (such as a switch).
- SNMP agents and MIBs, including SNMP traps, community strings, and Remote Monitoring (RMON) MIBs, which run on managed devices.
- SNMP network management applications, such as the Enterasys NetSight application, which communicate with agents to get statistics and alerts from the managed devices.

## SNMPv3 User-Based Security Model (USM) Enhancements

SNMPv3 adds to v1 and v2c components by providing secure access to devices by authenticating and encrypting frames over the network. The Enterasys supported advanced security features provided in SNMPv3's User-Based Security Model are as follows:

- Message integrity — Collects data securely without being tampered with or corrupted.
- Authentication — Determines the message is from a valid source.
- Encryption — Scrambles the contents of a frame to prevent it from being seen by an unauthorized source.

Unlike SNMPv1 and SNMPv2c, in SNMPv3, the concept of SNMP agents and SNMP managers no longer apply. These concepts have been combined into an SNMP entity. An SNMP entity consists of an SNMP engine and SNMP applications. An SNMP engine consists of the following four components:

- Dispatcher — Sends and receives messages.
- Message processing subsystem — Accepts outgoing PDUs from the dispatcher and prepares them for transmission by wrapping them in a message header and returning them to the dispatcher. Also accepts incoming messages from the dispatcher, processes each message header, and returns the enclosed PDU to the dispatcher.
- Security subsystem — Authenticates and encrypts messages.
- Access control subsystem — This component determines which users and which operations are allowed access to managed objects.

## Terms and Definitions

Table 12-2 lists common SNMP terms and defines their use on Enterasys devices.

**Table 12-2 SNMP Terms and Definitions**

| Term             | Definition                                                                                                                                                                                                                                                                                    |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| community        | A name string used to authenticate SNMPv1 and v2c users.                                                                                                                                                                                                                                      |
| context          | A subset of MIB information to which associated users have access rights.                                                                                                                                                                                                                     |
| engine ID        | A value used by both the SNMPv3 sender and receiver to propagate inform notifications.                                                                                                                                                                                                        |
| group            | A collection of SNMP users who share the same access privileges.                                                                                                                                                                                                                              |
| inform           | A notification message sent by an SNMPv3 agent to a network management station, a console, or a terminal to indicate the occurrence of a significant event, such as when a port or device goes up or down, when there are authentication failures, and when power supply errors occur.        |
| MIB              | Management Information Base, a repository for information about device parameters and network data organized in a tree structure.                                                                                                                                                             |
| notify profile   | Associates target parameters to an SNMP notify filter to determine who should not receive SNMP notifications. This is useful for fine-tuning the amount of SNMP traffic generated.                                                                                                            |
| OID              | Object Identifier, a unique ID distinguishing each variable in the MIB and is the means by which the SNMP manager and agent specify which managed elements are changed.                                                                                                                       |
| security level   | The permitted level of security within a security model. The three levels of SNMP security are: <ul style="list-style-type: none"> <li>no authentication required (NoAuthNoPriv)</li> <li>authentication required (AuthNoPriv)</li> <li>privacy (authPriv)</li> </ul>                         |
| security model   | An authentication strategy that is set up for an SNMP user and the group in which the user resides. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP frame.                                                       |
| storage type     | Specifies whether an SNMP user entry will be stored in volatile or nonvolatile memory.                                                                                                                                                                                                        |
| taglist          | A list of SNMP notify values that link a target (management station IP) address to specific SNMP notifications.                                                                                                                                                                               |
| target address   | A unique identifier and a specific IP address that will receive SNMP notification messages.                                                                                                                                                                                                   |
| target parameter | Controls where and under what circumstances SNMP notifications will be sent. This entry can be bound to a target IP address allowed to receive SNMP notification messages.                                                                                                                    |
| trap             | A notification message sent by an SNMPv1 or v2c agent to a network management station, a console, or a terminal to indicate the occurrence of a significant event, such as when a port or device goes up or down, when there are authentication failures, and when power supply errors occur. |
| user             | A person registered in SNMPv3 to access management information. In v1 and v2c, a user is set with the community name string.                                                                                                                                                                  |

**Table 12-2 SNMP Terms and Definitions (continued)**

| Term | Definition                                                                                                                                                                                                                                                                                                              |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| USM  | User-Based Security Model, the SNMPv3 authentication model which relies on a user name match for access to network management components.                                                                                                                                                                               |
| VACM | View-based Access Control Model, which determines remote access to SNMP managed objects, allowing subsets of management information to be organized into user views.                                                                                                                                                    |
| view | Specifies permission for accessing SNMP MIB objects granted to a particular SNMP user group. View types and associated access rights are: <ul style="list-style-type: none"> <li>• read - view-only access</li> <li>• write - allowed to configure MIB agent contents</li> <li>• notify - send trap messages</li> </ul> |

## Security Models and Levels

An SNMP security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. The three levels of SNMP security on Enterasys devices are: No authentication required (NoAuthNoPriv); authentication required (AuthNoPriv); and privacy (authPriv). A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP frame. [Table 12-3](#) identifies the levels of SNMP security available on Enterasys devices and authentication required within each model.

**Table 12-3 SNMP Security Models and Levels**

| Model    | Security Level | Authentication   | Encryption | How It Works                                                                                                                                                               |
|----------|----------------|------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| v1       | NoAuthNoPriv   | Community string | None       | Uses a community string match for authentication.                                                                                                                          |
| v2c      | NoAuthNoPriv   | Community string | None       | Uses a community string match for authentication.                                                                                                                          |
| v3 / USM | NoAuthNoPriv   | User name        | None       | Uses a user name match for authentication.                                                                                                                                 |
|          | AuthNoPriv     | MD5 or SHA       | None       | Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.                                                                                                      |
|          | authPriv       | MD5 or SHA       | DES        | Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard. |

## Access Control

In addition to the [Security Models and Levels](#) described above, the Enterasys implementation of SNMP also provides a View-based Access Control Model (VACM), which determines remote access to managed objects. VACM allows you to organize subsets of management information into “views.” Management information that is in a user’s view gives the user the corresponding access level to that management information: either read, write, or notify. Individual users can be organized into groups for whom you can pre-define what views are available based on the



security model and security level used to request access. In this way, VACM allows you to permit or deny access to any individual item of management information depending on a user's group membership and the level of security provided by the communications channel.

## Configuring SNMP

This section provides the following information about configuring SNMP on Enterasys devices:

| For information about...                                        | Refer to page... |
|-----------------------------------------------------------------|------------------|
| <a href="#">Configuration Basics</a>                            | 12-7             |
| <a href="#">How SNMP Processes a Notification Configuration</a> | 12-7             |
| <a href="#">SNMP Defaults</a>                                   | 12-8             |
| <a href="#">Configuring SNMPv1/SNMPv2c</a>                      | 12-9             |
| <a href="#">Configuring SNMPv3</a>                              | 12-10            |
| <a href="#">Configuring Secure SNMP Community Names</a>         | 12-15            |

### Configuration Basics

Completing an SNMP configuration on an Enterasys device involves defining users who will be authorized to receive SNMP notifications about network events, associating security (target) parameters, access rights and MIB views to those users, and specifying an IP address where they will receive notifications. The basic steps in this process are:

1. Creating a name that will act as an SNMP user password:
  - This will be a **community** name for an SNMPv1 or v2c configuration, or.
  - A **user** name for an SNMPv3 configuration.
2. Creating a group for the user named in [Step 1](#).
3. Creating access rights for the user group named in [Step 2](#).
4. Defining MIB view(s) for the user group.
5. Creating a target parameters entry to associate security and authorization criteria to the users created in [Step 1](#).
6. Verifying if any applicable SNMP notification entries exist, or creating a new one. You will use this entry to send SNMP notification messages to the appropriate targets configured in [Step 5](#).
7. Creating a target address entry to bind a management IP address to:
  - The notification entry and tag name created in [Step 6](#), and
  - The target parameters entry created in [Step 5](#).



**Note:** Commands for configuring SNMP on Enterasys devices are independent during the SNMP setup process. For instance, target parameters can be specified when setting up optional notification filters — even though these parameters have not yet been created with the `set snmp targetparams` command. The steps in this section are a guideline to configuring SNMP and do not necessarily need to be executed in this order.

### How SNMP Processes a Notification Configuration

In order to send a trap or inform notification requested by a MIB code, the SNMP agent requires the equivalent of a trap “door”, a “key” to unlock the door, and a “procedure” for crossing the

doorstep. To determine if all these elements are in place, the SNMP agent processes a device configuration as follows:

1. Determines if the “keys” for trap “doors” do exist. The key that SNMP is looking for is the notification entry created with the **set snmp notify** command.
2. Searches for the doors matching such a key and verifies that the door is available. If so, this door is tagged or bound to the notification entry. It was built using the **set snmp targetaddr** command, which specifies the management station IP address to which this door leads, and the “procedure” (**targetparams**) to cross the doorstep
3. Verifies that the description of how to step through the door is, in fact, there. The agent checks **targetparams** entries and determines this description was made with the **set snmp targetparams** command, which tells exactly which SNMP protocol to use and what community or user name to provide.
4. Verifies that the specified name, configured using either the **set snmp community** or **set snmp user** command is available.
5. Sends the notification message to the target address.

## SNMP Defaults

### Device Start Up Configuration

By default, SNMPv1 is configured on Enterasys switches. [Table 12-4](#) lists the default configuration parameters, which include a single community name - **public** - granting read-write access to the whole MIB tree for both SNMPv1 and SNMPv2c.

**Table 12-4 Default Enterasys SNMP Configuration**

| Parameter               | Default Value                            |
|-------------------------|------------------------------------------|
| Community name          | public                                   |
| Group access privileges | rw (read-write)                          |
| Group user name         | public                                   |
| Security model          | v1                                       |
| Security access rights  | all (for read, write, and notify access) |
| MIB view                | all (entire MIB tree)                    |

You can revise this default configuration by following the steps described in [“Adding to or Modifying the Default Configuration”](#) on page 12-10.

To take advantage of the advanced security and other features available in SNMPv3, it is recommended that you add to the Enterasys default configuration by configuring SNMPv3 as described in [“Configuring SNMPv3”](#) on page 12-10.

Refer also to [“Configuring Secure SNMP Community Names”](#) on page 12-15 for a description of a recommended configuration that will prevent unsecured access to SNMP information.

## Configuring SNMPv1/SNMPv2c

### Creating a New Configuration

[Procedure 12-1](#) shows how to create a new SNMPv1 or SNMPv2c configuration. This example assumes that you haven't any preconfigured community names or access rights.



**Note:** The **v1** parameter in this example can be replaced with **v2** for SNMPv2c configuration.

#### Procedure 12-1 New SNMPv1/v2c Configuration

| Step | Task                                                                                                                         | Command(s)                                                                                                  |
|------|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| 1.   | Create a community name.                                                                                                     | <code>set snmp community community_name</code>                                                              |
| 2.   | Create a security model (VACM) group using the <i>community name</i> you assigned in step 1.                                 | <code>set snmp group group_name user community_name security-model v1</code>                                |
| 3.   | Set security access rights for the VACM group.                                                                               | <code>set snmp access group_name security model v1 read viewname write viewname notify viewname</code>      |
| 4.   | Set MIB view attributes.                                                                                                     | <code>set snmp view viewname viewname subtree subtree</code>                                                |
| 5.   | Specify the target parameters for SNMP notification message generation.                                                      | <code>set snmp targetparams targetparams user community_name security-model v1 message processing v1</code> |
| 6.   | Specify the target address to which SNMP notification messages generated using the specified target parameters will be sent. | <code>set snmp targetaddr targetaddr ipaddr param targetparams taglist taglist</code>                       |
| 7.   | Specify a name for this notification entry and bind it to the target address.                                                | <code>set snmp notify notify tag taglist</code>                                                             |

#### Example

The following example is an SNMPv1 or v2 configuration using the steps in [Procedure 12-1](#). It shows how to:

- Create the community name **public**.
- Assign the **public** user to the group named **groupRW** and the SNMPv1 security model.
- Specify that, if SNMP messages are received with the **public** name string, the view **RW** for read requests, write requests, and notify requests will be applied to this user.
- For the view **RW**, include the MIB subtree denoted with OID **1** and **0.0**, and exclude view access to subtree denoted with OID **1.3.6.1.6.3.13.1** (which is the notification MIB).
- Assign a target parameters entry, **TVv1public**, for security level processing to the **public** community name.
- Create a target address entry named **TVTrap** at IP address **10.42.1.10**, which will use security and authorization criteria contained in the target parameters entry called **TVv1public**, and bind these parameters together with a tag entry called **TVTrapTag**.

```
enterasys(su)->set snmp community public
enterasys(su)->set snmp group groupRW user public security model v1
enterasys(su)->set snmp access groupRW security-model v1 read RW write RW
notify RW
enterasys(su)->set snmp view viewname RW subtree 1
```

```

enterasys(su)->set snmp view viewname RW subtree 0.0
enterasys(su)->set snmp view viewname RW subtree 1.3.6.1.6.3.13.1 excluded
enterasys(su)->set snmp targetparams TVv1public user public security-model v1
message processing v1
enterasys(su)->set snmp targetaddr TVTrap 10.42.1.10 param TVv1public taglist
TVTrapTag
enterasys(su)->set snmp notify TVTrap tag TVTrapTag

```

## Adding to or Modifying the Default Configuration

By default, SNMPv1 is configured on Enterasys switches. A single community name - **public** - is configured, which grants read-write access to the whole MIB tree for both SNMPv1 and SNMPv2c.

The beginning command sequence in the default configuration is similar to the first part of the previous example. It looks like this:

```

enterasys(su)->set snmp community public
enterasys(su)->set snmp group groupRW user public security-model v1
enterasys(su)->set snmp access groupRW security-model v1 read All write All notify
All
enterasys(su)->set snmp view viewname All subtree 1

```



**Note:** Any use of the parameter 'All' must be exactly as shown in this example. Any other variation (including, but not limited to, values such as 'all' or 'ALL') will not be valid.

You can modify this default configuration as shown in the following examples.

### Adding a New Community Name

Use these commands to add a new SNMPv1 community name called **newname** with the same permissions as the default configuration:

```

enterasys(su)->set snmp community newname
enterasys(su)->set snmp group groupRW user newname security-model v1

```

Use this command to remove the **public** community name from the default configuration:

```

enterasys(su)->clear snmp community public

```



**Note:** You can leave the **set snmp group groupRW user public security-model v1** statement in the default configuration in case you want to re-activate the **public** community name at some point, or can clear it as well.

Refer to “[Configuring Secure SNMP Community Names](#)” on page 12-15 for a description of a recommended configuration that will prevent unsecured access to SNMP information.

## Configuring SNMPv3

[Procedure 12-2](#) shows how to complete a basic SNMPv3 configuration. For additional configuration information, refer to:

- “[Configuring an SNMPv3 Inform or Trap Engine ID](#)” on page 12-13
- “[Configuring an SNMP View](#)” on page 12-14
- “[Configuring Secure SNMP Community Names](#)” on page 12-15

## Procedure 12-2 SNMPv3 Configuration

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Command(s)                                                                                                                                                                                                                                                                        |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | <p>Create an SNMPv3 user and specify authentication, encryption, and security credentials.</p> <ul style="list-style-type: none"> <li>If <b>remote</b> is not specified, the user will be registered for the local SNMP engine.</li> <li>If <b>authentication</b> is not specified, no authentication will be applied.</li> <li>If <b>privacy</b> is not specified, no encryption will be applied.</li> </ul>                                                                                                                                                                                                                                   | <pre>set snmp user user [<b>remote</b> remoteid] [<b>privacy</b> privpassword] [<b>authentication</b> {md5   sha}] [authpassword]</pre>                                                                                                                                           |
| 2.   | <p>Create a user group and add the user created in Step 1.</p> <ul style="list-style-type: none"> <li>If storage type is not specified, <b>nonvolatile</b> will be applied.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <pre>set snmp group groupname user user security-model usm [<b>volatile</b>   nonvolatile]</pre>                                                                                                                                                                                  |
| 3.   | <p>Set security access rights for the group.</p> <ul style="list-style-type: none"> <li>If security level is not specified, no authentication will be applied.</li> <li>Only one context, the “default context”, is supported in this release. There is no need to configure this parameter.</li> <li>If <b>read</b> view is not specified none will be applied.</li> <li>If <b>write</b> view is not specified, none will be applied.</li> <li>If <b>notify</b> view is not specified, none will be applied.</li> <li>If storage type is not specified, entries will be stored as permanent and will be held through device reboot.</li> </ul> | <pre>set snmp access groupname security- model usm [<b>noauthentication</b>   <b>authentication</b>   <b>privacy</b>] [<b>exact</b>   <b>prefix</b>] [<b>read</b> readviewname] [<b>write</b> writeviewname] [<b>notify</b> notifyviewname] [<b>volatile</b>   nonvolatile]</pre> |
| 4.   | <p>Define views created in Step 3.</p> <ul style="list-style-type: none"> <li>If not specified, <b>mask</b> will be set to <b>ff:ff:ff:ff</b>.</li> <li>If not specified, subtree use will be <b>included</b>.</li> <li>If storage type is not specified, <b>nonvolatile</b> (permanent) will be applied.</li> </ul>                                                                                                                                                                                                                                                                                                                            | <pre>set snmp view viewname viewname subtree subtree [<b>mask</b> mask] [<b>included</b>   <b>excluded</b>] [<b>volatile</b>   nonvolatile]</pre>                                                                                                                                 |
| 5.   | <p>Set SNMP target parameters.</p> <ul style="list-style-type: none"> <li>If not specified, security level will be set to <b>noauthentication</b>.</li> <li>If not specified, storage type will be set to <b>nonvolatile</b>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                        | <pre>set snmp targetparams targetparams user user security-model usm message-processing v3 [<b>noauthentication</b>   <b>authentication</b>   <b>privacy</b>] [<b>volatile</b>   <b>nonvolatile</b>]</pre>                                                                        |

**Procedure 12-2 SNMPv3 Configuration (continued)**

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Command(s)                                                                                                                                                                |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.   | Set the SNMP target address for notification message generation. <ul style="list-style-type: none"> <li>If not specified, <i>udpport</i> will be set to <b>162</b>.</li> <li>If not specified, <i>mask</i> will be set to <b>255.255.255.255</b>.</li> <li>If not specified, <i>timeout</i> will be set to <b>1500</b> (15 seconds).</li> <li>If not specified, number of <i>retries</i> will be set to <b>3</b>.</li> <li>If <b>taglist</b> is not specified, none will be set.</li> <li>If not specified, storage type will be <b>nonvolatile</b>.</li> </ul> | <pre>set snmp targetaddr targetaddr ipaddr param param [udpport udpport] [mask mask] [timeout timeout] [retries retries] [taglist taglist] [volatile   nonvolatile]</pre> |
| 7.   | Set SNMP notification parameters. <ul style="list-style-type: none"> <li>If not specified, message type will be set to <b>trap</b>.</li> <li>If not specified, storage type will be set to <b>nonvolatile</b>.</li> </ul>                                                                                                                                                                                                                                                                                                                                       | <pre>set snmp notify notify tag tag [trap   inform] [volatile   nonvolatile]</pre>                                                                                        |

The following example is an SNMPv3 configuration using the steps in [Procedure 12-2](#). It shows how to

- Create the user **Enterasys\_user**, specifying authentication, encryption, and security credentials.
- Assign **Enterasys\_user** to the **Enterasys** group and associate it to the SNMPv3 security model, **usm**.
- Specify that, if SNMP messages are received with authentication and encryption, the view, **readView** for read requests, and the view **writeView** for write requests will be applied to this user group based on the USM security model.
- For the view **writeView**, include the MIB subtree denoted with OID **1**, and exclude the subtree denoted by OID **1.3.6.1.4.1.5624.1.2.16** (which is the Configuration Management MIB).
- Assign an SNMPv3 target parameters entry named **enterasysn** to the **Enterasys\_user** using the USM security model.
- Create a target address entry named **Enterasys\_Networks** at IP address **172.29.10.1** which will use security and authorization criteria contained in a target parameters entry called **enterasysn**, and bind these parameters together with a tag entry called **v3TrapTag**.

```
enterasys(su)-> set snmp user Enterasys_user privacy my_privacy authentication md5
my_authentication
enterasys(su)-> set snmp group Enterasys user Enterasys_user security-model usm
enterasys(su)-> set snmp access Enterasys security-model usm privacy read readView
write writeView
enterasys(su)-> set snmp view viewname readView subtree 1
enterasys(su)-> set snmp view viewname writeView subtree 1
enterasys(su)-> set snmp view viewname writeView subtree 1.3.6.1.4.1.5624.1.2.16
excluded
enterasys(su)-> set snmp targetparams enterasysn user Enterasys_user
security-model usm message-processing v3
enterasys(su)-> set snmp targetaddr Enterasys_Networks 172.29.10.1 param
enterasysn taglist v3TrapTag
```

```
enterasys(su)-> set snmp notify SNMPv3TrapGen tag v3TrapTag inform
```

## How SNMP Will Process This Configuration

As described in “[How SNMP Processes a Notification Configuration](#)” on page 12-7, if the SNMP agent on the device needs to send an inform message, it looks to see if there is a notification entry that says what to do with inform messages. Then, it looks to see if the tag list (**v3TrapTag**) specified in the notification entry exists. If it exists, then the inform message is sent to the target addresses specified by the tag list, (**Enterasys\_Networks**) using the parameters specified for each address (**enterasysn**).

## Configuring an SNMPv3 Inform or Trap Engine ID

This section provides additional information for configuring SNMPv3 inform or trap notifications. The steps in [Procedure 12-3](#) on page 12-13 add to the following configuration example:

```
enterasys(su)->set snmp view viewname All subtree 1
enterasys(su)->set snmp user v3user privacy despasswd authentication md5 md5passwd
enterasys(su)->set snmp group v3group user v3user security-model usm
enterasys(su)->set snmp access v3group security-model usm privacy exact read All
write All notify All
enterasys(su)->set snmp notify v3notify tag v3tag inform
enterasys(su)->set snmp targetaddr v3TA 134.141.209.73 param v3TP taglist v3tag
enterasys(su)->set snmp targetparams v3TP user v3user security-model usm
message-processing v3 privacy
```

### Inform EngineIDs

In the Enterasys SNMP implementation, the receiver's EngineID value is used by both the sender and receiver to propagate inform notifications. In order to send and receive SNMP v3 informs in their most secure form (with authentication and privacy enabled), you must configure a user ID and corresponding receiver EngineID on the sender as shown in the example in [Procedure 12-3](#). This example assumes that NetSight Console is the receiver, and an Enterasys switch is the sender.



**Note:** The following file location and EngineID are provided as examples. Your settings will vary.

[Procedure 12-3](#) adds to the configuration example shown in “[Configuring an SNMPv3 Inform or Trap Engine ID](#)” on page 12-13.

### Procedure 12-3 Configuring an EngineID

| Step | Task                                                                                                  | Command(s)                                                                                 |
|------|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 1.   | If necessary, create an SNMP3 configuration.                                                          | Refer to “ <a href="#">Configuring an SNMPv3 Inform or Trap Engine ID</a> ” on page 12-13. |
| 2.   | On the management station, navigate to and display the Netsight Console SNMP trap configuration file. | <b>C:\Program Files\Enterasys Networks\NetSight Shared\snmptrapd.conf</b>                  |
| 3.   | Determine the EngineID from this line in the configuration file.                                      | <b>oldEngineID<br/>0x800007e5804f19000d232aa40</b>                                         |

**Procedure 12-3 Configuring an EngineID (continued)**

| Step | Task                                                                                                                                                                                                                               | Command(s)                                                                                                                                                                                                                                                               |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.   | On the Enterasys switch, define the same user as in the above example ( <b>v3user</b> ) with this EngineID and with the same Auth/Priv passwords you used previously.                                                              | <pre>set snmp user v3user remote 800007e5804f190000d232aa40 privacy despasswd authentication md5 md5passwd</pre> <p><b>Note:</b> You can omit the <b>0x</b> from the EngineID. You can also use the colon notation like this: 80:00:07:e5:80:4f:19:00:00:d2:32:aa:40</p> |
| 5.   | Navigate to and display the user configuration on the management station. (This assumes that you have already created the user in Netsight Console, so you will only need to add it to the configuration file of the trap daemon.) | <pre>C:\Program Files\Enterasys Networks\NetSight Console\Bin\snmptrapd.conf</pre>                                                                                                                                                                                       |
| 6.   | Using any plain text editor, add this line to the configuration file.                                                                                                                                                              | <pre>createuser v3user MD5 md5passwd DES despasswd</pre>                                                                                                                                                                                                                 |

**Trap EngineID**

To use traps instead of inform notifications, you would change the preceding configuration as follows:

- Use this command to specify trap notifications:

```
set snmp notify v3notify tag v3tag trap
```

- Verify that the “createuser” entry in the NetSight Console SNMP trap configuration looks like this:

```
createuser -e 0x800015f80300e06314d79c v3user MD5 md5passwd DES despasswd
```

When you are finished modifying the configuration, save the file and restart the SNMP Trap Service using NetSight Services Manager.



**Note:** When installed on a Unix platform, the NetSight server must be manually restarted.

**Configuring an SNMP View**

It is possible to include certain OIDs and exclude certain other OIDs within one SNMP MIB view. You do this by stacking different **set snmp view** includes and excludes which specify a single view name. This allows the user to view all of the “included” OID strings for their associated view name, minus all of the “excluded” OID strings for their view name. If no such parameter is specified, “included” is assumed.

Though it is possible to create and use multiple view names as desired, for demonstration purposes it is simplest to modify the default view, since it is already being referenced by the remainder of the SNMP command set.

The following example removes the default view specifications, and inserts one which permits access to branch MIB **1.3.6.1.2.1** with the exception of branch interfaces **1.3.6.1.2.1.2.:**

```
enterasys(su)->clear snmp view All 1
enterasys(su)->clear snmp view All 0.0
enterasys(su)->set snmp view viewname All subtree 1.3.6.1.2.1
enterasys(su)->set snmp view viewname All subtree 1.3.6.1.2.1.2 excluded
enterasys(su)->show snmp view
View Name = All
```



```
Subtree OID = 1.3.6.1.2.1
Subtree mask =
View Type = included
Storage type = nonVolatile
Row status = active

View Name = All
Subtree OID = 1.3.6.1.2.1.2
Subtree mask =
View Type = excluded
Storage type = nonVolatile
Row status = active
```

You can test this configuration using any MIB browser directed to the IP of the configured device and using the default community name **public** associated with the view **All**. If configured correctly, only your specified sections of the MIBs will be visible.

## Configuring Secure SNMP Community Names

[Procedure 12-4](#) on page 12-16 provides an example of a recommended configuration that will prevent unsecured SNMPv1/v2c access of potentially security compromising information.

As discussed previously in this document, SNMP v1 and v2c are inherently insecure device management protocols. Community names used to define access levels are passed in clear text in all protocol frames sent to the managed entity and may be visible by read-only SNMP users when querying certain SNMP configuration-related objects. In addition, you may be further exposing your network due to configuration conventions which reuse the community names in other aspects of entity management, such as CLI login passwords, and SNMP security names.

Enterasys recommends that you “secure” all SNMP community names. You do this by creating a configuration that hides, through the use of “views” sensitive information from SNMP v1/v2c users as follows:

**Procedure 12-4 Configuring Secure Community Names**

| Step | Task                                                                                                                                                                                                                                                                                                                   | Command(s)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | <p>Create the following SNMP view group configurations.</p> <ul style="list-style-type: none"> <li>An admin (v3) view group with secure read, write, and notify access</li> <li>A read-only view group with unsecure (v1 and v2c) access</li> <li>A read-write view group with unsecure (v1 and v2c) access</li> </ul> | <pre> <b>set snmp access</b> admin-groupname <b>security-model</b> usm <b>privacy exact</b> <b>read</b> secured-viewname <b>write</b> secure- viewname <b>notify</b> secured-viewname  <b>set snmp access</b> read-only-groupname <b>security-model</b> v1 <b>exact read</b> unsecured-viewname  <b>set snmp access</b> read-only-groupname <b>security-model</b> v2c <b>exact read</b> unsecured-viewname  <b>set snmp access</b> read-write-groupname <b>security-model</b> v1 <b>exact read</b> unsecure-viewname <b>write</b> unsecured- viewname  <b>set snmp access</b> read-write-groupname <b>security-model</b> v2c <b>exact read</b> unsecured-viewname <b>write</b> unsecured- viewname </pre> |
| 2.   | Create v1/v2c “public” and “private” community names and security names.                                                                                                                                                                                                                                               | <pre> <b>set snmp community</b> private- communityname <b>securityname</b> read- write-securityname  <b>set snmp community</b> public- communityname <b>securityname</b> read- only-securityname </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 3.   | Create user groups and bind them to the security names created in Step 2.                                                                                                                                                                                                                                              | <pre> <b>set snmp group</b> admin-groupname <b>user</b> admin-username  <b>set snmp group</b> read-only-groupname <b>user</b> read-only-securityname <b>security-model</b> v1  <b>set snmp group</b> read-write-groupname <b>user</b> read-write-securityname <b>security-model</b> v1  <b>set snmp group</b> read-only-groupname <b>user</b> read-only-securityname <b>security-model</b> v2c  <b>set snmp group</b> read-write-groupname <b>user</b> read-write-securityname <b>security-model</b> v2c </pre>                                                                                                                                                                                           |
| 4.   | Using the <i>admin-username</i> assigned in Step 3, create the v3 user and define authentication keys.                                                                                                                                                                                                                 | <pre> <b>set snmp user</b> admin-username <b>privacy</b> priv-key <b>authentication sha</b> auth-key </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Procedure 12-4 Configuring Secure Community Names (continued)**

| Step | Task                                                                                                                                                                                                                                                                                           | Command(s)                                                                                                                                                                                                                                      |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.   | Using the viewnames assigned in Step 1, create restricted views for v1/v2c users, and unrestricted views for v3 users.                                                                                                                                                                         | <pre>set snmp view viewname secured- viewname subtree 1 set snmp view viewname secured- viewname subtree 0.0 set snmp view viewname unsecured- viewname subtree 1 set snmp view viewname unsecured- viewname subtree 0.0</pre>                  |
| 6.   | Exclude the following from the restricted view <ul style="list-style-type: none"> <li>• snmpUsmMIB (which contains v3 user names, but no passwords)</li> <li>• snmpVacmMIB (which contains SNMP view configurations)</li> <li>• snmpCommunityTable (which contains community names)</li> </ul> | <pre>set snmp view viewname unsecured- viewname subtree 1.3.6.1.6.3.15 excluded set snmp view viewname unsecured- viewname subtree 1.3.6.1.6.3.16 excluded set snmp view viewname unsecured- viewname subtree 1.3.6.1.6.3.18.1.1 excluded</pre> |

**Example**

The following example shows an SNMP community names configuration using the steps in [Procedure 12-4](#) on page 12-16.

```
enterasys(su)->set snmp access gAdmin security-model usm privacy exact read
vSecured write vSecured notify vSecured
enterasys(su)->set snmp access gReadOnlyV1V2C security-model v1 exact read
vUnsecured
enterasys(su)->set snmp access gReadOnlyV1V2C security-model v2c exact read
vUnsecured
enterasys(su)->set snmp access gReadWriteV1V2C security-model v1 exact read
vUnsecured write vUnsecured
enterasys(su)->set snmp access gReadWriteV1V2C security-model v2c exact read
vUnsecured write vUnsecured
enterasys(su)->set snmp community cnPrivate securityname sn_v1v2c_rw
enterasys(su)->set snmp community cnPublic securityname sn_v1v2c_ro
enterasys(su)->set snmp group gReadOnlyV1V2C user sn_v1v2c_ro security-model v1
enterasys(su)->set snmp group gReadWriteV1V2C user sn_v1v2c_rw security-model v1
enterasys(su)->set snmp group gReadOnlyV1V2C user sn_v1v2c_ro security-model v2c
enterasys(su)->set snmp group gReadWriteV1V2C user sn_v1v2c_rw security-model v2c
enterasys(su)->set snmp group gAdmin user it-admin security-model usm
enterasys(su)->set snmp user it-admin privacy priv_key authentication sha auth_key
enterasys(su)->set snmp view viewname vSecured subtree 1
enterasys(su)->set snmp view viewname vSecured subtree 0.0
enterasys(su)->set snmp view viewname vUnsecured subtree 1
enterasys(su)->set snmp view viewname vUnsecured subtree 0.0
enterasys(su)->set snmp view viewname vUnsecured subtree 1.3.6.1.6.3.15 excluded
enterasys(su)->set snmp view viewname vUnsecured subtree 1.3.6.1.6.3.16 excluded
enterasys(su)->set snmp view viewname vUnsecured subtree 1.3.6.1.6.3.18.1.1
excluded
```

## Reviewing SNMP Settings

**Table 12-5 Commands to Review SNMP Settings**

| Task                                                                                                    | Command                                                                                           |
|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Display SNMPv1/SNMPv2c community names and status.                                                      | <code>show snmp community name</code>                                                             |
| Display the context list configuration for SNMP view-based access control.                              | <code>show snmp context</code>                                                                    |
| Display SNMP traffic counter values.                                                                    | <code>show snmp counters</code>                                                                   |
| Display SNMP engine properties.                                                                         | <code>show snmp engineid</code>                                                                   |
| Display SNMP group information.                                                                         | <code>show snmp group groupname grpname</code>                                                    |
| Display an SNMP group's access rights.                                                                  | <code>show snmp access grpname</code>                                                             |
| Display SNMP target parameter profiles.                                                                 | <code>show snmp targetparams paramname</code>                                                     |
| Display SNMP target address information.                                                                | <code>show snmp targetaddr</code>                                                                 |
| Display SNMP notify configuration.                                                                      | <code>show snmp notify</code>                                                                     |
| Display SNMP notify filter information, identifying which profiles will not receive SNMP notifications: | <code>show snmp notifyfilter [profile] [subtree oid-or-mibobject] [volatile   nonvolatile]</code> |
| Display SNMP notify profile information.                                                                | <code>show snmp notifyprofile [profile] [targetparam targetparam] [volatile   nonvolatile]</code> |
| Display SNMPv3 users.                                                                                   | <code>show snmp user user</code>                                                                  |
| Display SNMP views.                                                                                     | <code>show snmp view viewname</code>                                                              |

## Configuring Neighbor Discovery

This chapter describes how to configure the Link Layer Discovery Protocol (LLDP), the Enterasys Discovery Protocol, and the Cisco Discovery Protocol on Enterasys fixed stackable and standalone switches.

| For information about...                                 | Refer to page... |
|----------------------------------------------------------|------------------|
| <a href="#">Neighbor Discovery Overview</a>              | 13-1             |
| <a href="#">Configuring LLDP</a>                         | 13-7             |
| <a href="#">Configuring Enterasys Discovery Protocol</a> | 13-10            |
| <a href="#">Configuring Cisco Discovery Protocol</a>     | 13-11            |

### Neighbor Discovery Overview

Neighbor discovery is the Layer 2 process in which a device identifies and advertises itself to its directly connected neighbors. Enterasys devices support the following neighbor discovery protocols:

- Link Layer Discovery Protocol (LLDP) and its extension, LLDP-MED, which is the IEEE 802.1AB standard for neighbor discovery
- Enterasys Discovery Protocol, for discovering Enterasys devices
- Cisco Discovery Protocol, for discovering Cisco devices

Neighbor discovery is useful for:

- Determining an accurate physical network topology
- Creating an inventory of network devices
- Troubleshooting the network

LLDP, Enterasys Discovery Protocol, and Cisco Discovery Protocol are enabled on Enterasys devices by default. Though all three discovery protocols can run simultaneously, LLDP is the preferred protocol.

If a device, attached to a port that has been enabled for neighbor discovery, does not support LLDP but supports Enterasys Discovery Protocol or Cisco Discovery Protocol, then one of those protocols is used instead.

### Neighbor Discovery Operation

The neighbor discovery protocols support the Layer 2 process of network devices advertising their identities and capabilities on a LAN and discovering that information about their directly

connected neighbors. While Enterasys Discovery Protocol and Cisco Discovery Protocol are vendor-specific protocols, LLDP is an industry standard (IEEE 802.1AB), vendor-neutral protocol.

The LLDP-enabled device periodically advertises information about itself (such as management address, capabilities, media-specific configuration information) in an LLDPDU (Link Layer Discovery Protocol Data Unit), which is sent in a single 802.3 Ethernet frame (see [Figure 13-3](#) on page 13-6). An LLDPDU consists of a set of TLV (type, length, and value) attributes. The information, which is extracted and tabulated by an LLDP-enabled device's peers, is recorded in IEEE-defined management information base (MIB) modules, making it possible for the information to be accessed by a network management system using a management protocol such as SNMP. The information is aged to ensure that it is kept up to date. Ports can be configured to send this information, receive this information, or both.

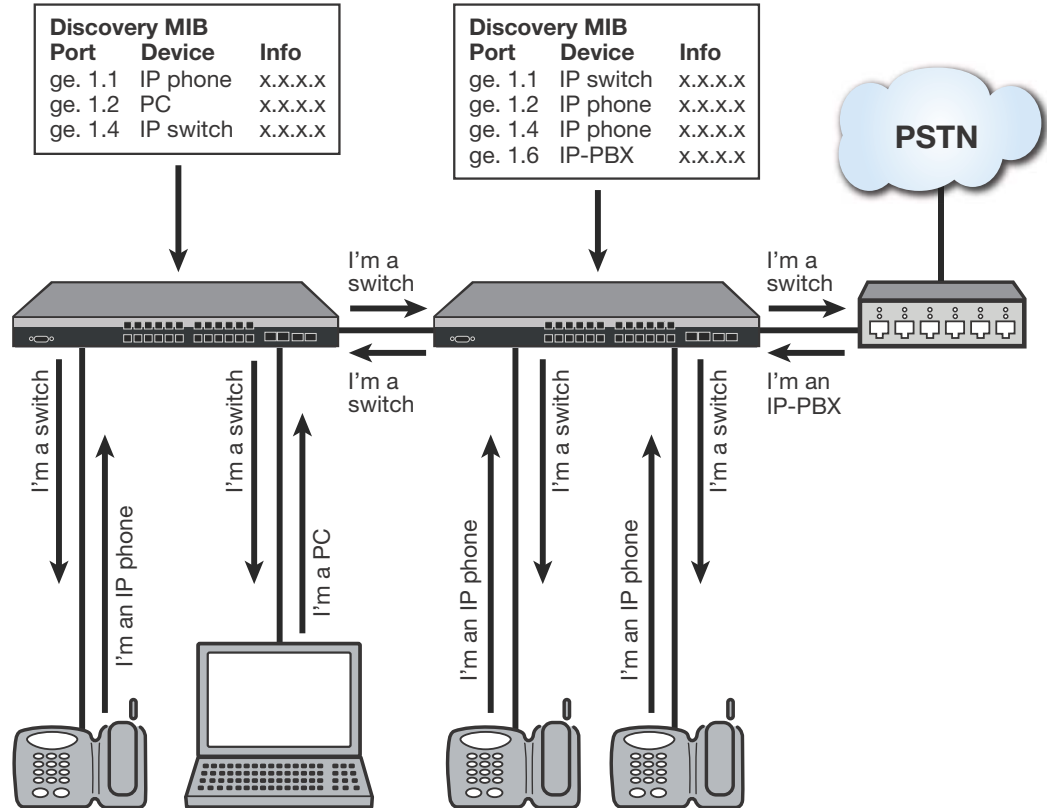
The LLDP agent operates only in an advertising mode, and hence does not support any means for soliciting information or keeping state between two LLDP entities.

LLDP can be used for many advanced features in a VoIP network environment. These features include basic configuration, network policy configuration, location identification (including for Emergency Call Service/E911), Power over Ethernet management, and inventory management.

To fulfill these needs, the standard provides extensions to IEEE 802.1AB that are specific to the requirements of media endpoint devices in an IEEE 802 LAN. Interaction behavior between the media endpoint devices and the LAN infrastructure elements are also described where they are relevant to correct operation or multi-vendor interoperability. Media endpoint devices addressed include, but are not limited to, IP phones, IP voice/media gateways, IP media servers, and IP communication controllers.

[Figure 13-1](#) on page 13-3 shows an example of LLDP communication between devices, done via Layer 2 with LLDPDU packets. The communication is only between LLDP-enabled devices — the information is not forwarded to other devices.

Figure 13-1 Communication between LLDP-enabled Devices



## LLDP-MED

The LLDP-Media Endpoint Discovery (LLDP-MED) extension of LLDP is defined to share information between media endpoint devices such as IP telephones, media gateways, media servers, and network connectivity devices.

Either LLDP or LLDP-MED, but not both, can be used on an interface between two devices. A switch port uses LLDP-MED when it detects that an LLDP-MED device is connected to it.

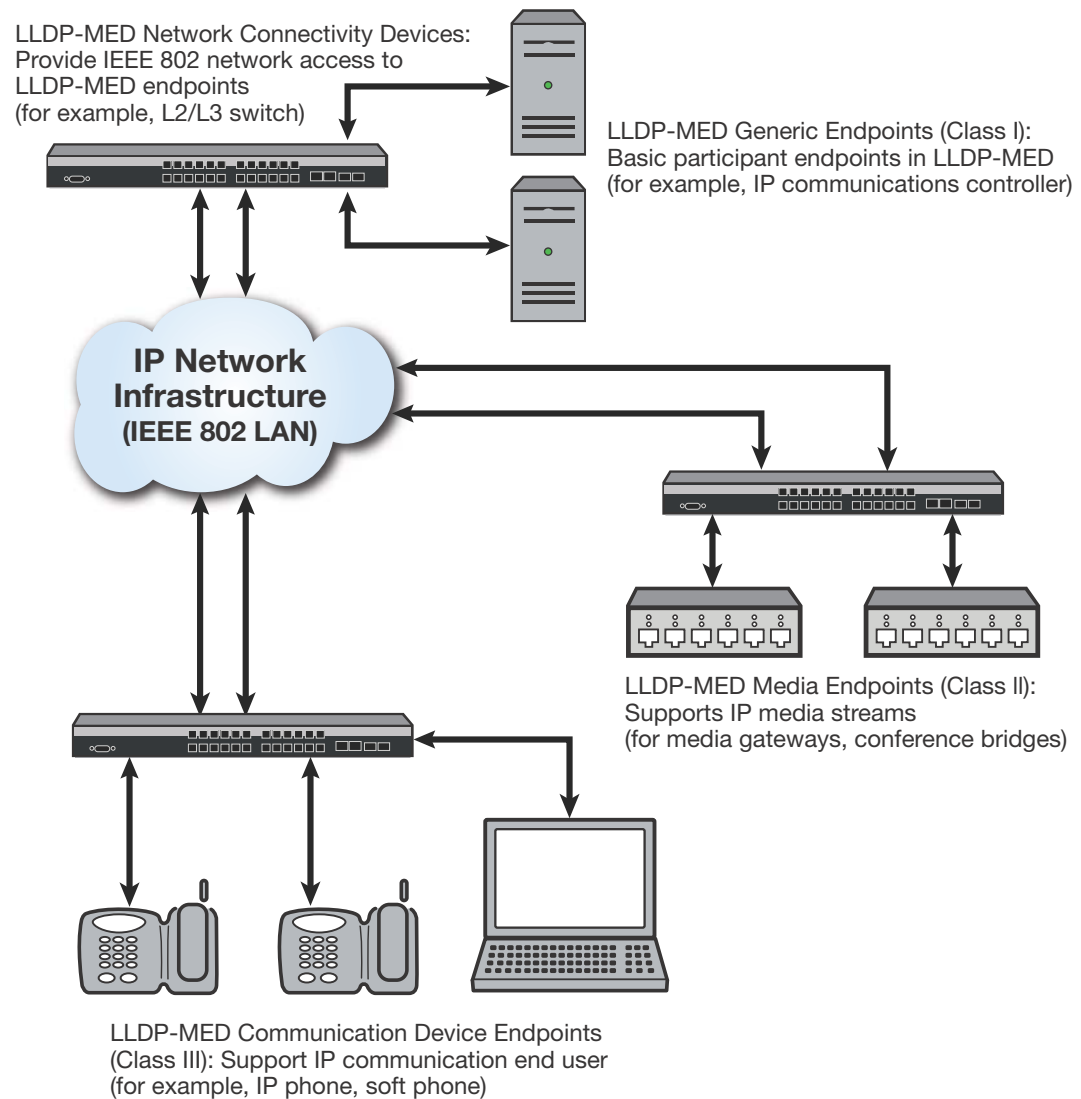
LLDP-MED provides the following benefits:

- Auto discovery of LAN policies, such as VLAN ID, 802.1p priority, and Diffserv codepoint settings, leading to plug-and-play networking.
- Device location and topology discovery, allowing creation of location databases and, in the case of VoIP, provision of E911 services.
- Extended and automated power management of Power over Ethernet endpoints
- Inventory management, allowing network administrators to track their network devices and to determine their characteristics, such as manufacturer, software and hardware versions, and serial or asset numbers.

There are two primary LLDP-MED device types (as shown in [Figure 13-2](#) on page 13-5):

- Network connectivity devices, which are LAN access devices such as LAN switch/routers, bridges, repeaters, wireless access points, or any device that supports the IEEE 802.1AB and MED extensions defined by the standard and can relay IEEE 802 frames via any method.
- Endpoint devices, which have three defined sub-types or classes:
  - LLDP-MED Generic Endpoint (Class I) — All endpoint products that, while requiring the base LLDP discovery services defined in the standard, do not support IP media or act as an end-user communication device, such as IP communications controllers, other communication-related servers, or any device requiring basic services. Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.
  - LLDP-MED Media Endpoint (Class II) — All endpoint products that have IP media capabilities but that may not be associated with a particular end user, such as voice/media gateways, conference bridges, and media servers. Capabilities include all of the capabilities defined for Generic Endpoint (Class I) and are extended to include aspects related to media streaming. Discovery services defined in this class include media type specific network layer policy discovery.
  - LLDP-MED Communication Endpoint (Class III) — All endpoint products that act as an endpoint user communication device supporting IP media. Capabilities include all of the capabilities defined for the Generic Endpoint (Class I) and Media Endpoint (Class II) devices and are extended to include aspects related to end user devices, such as IP phones, PC-based soft phones, and other communication devices that directly support the end user.

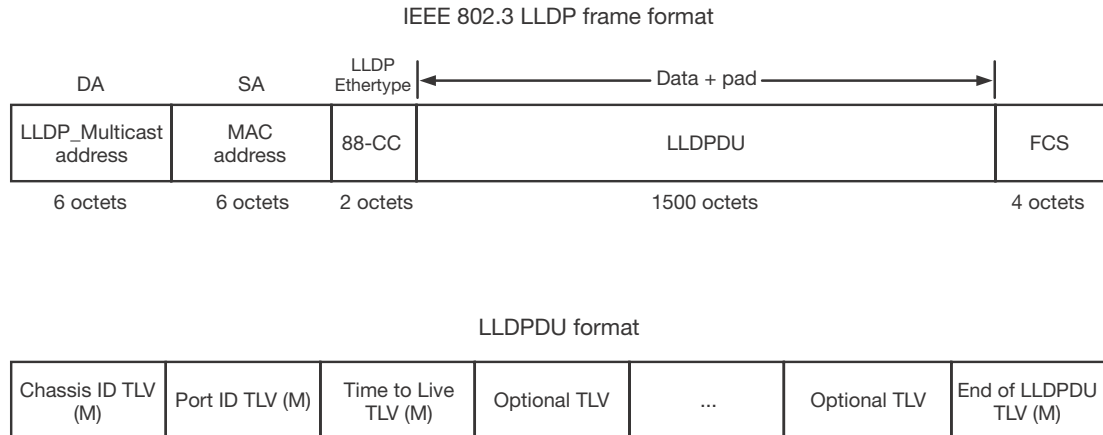


**Figure 13-2 LLDP-MED**

## LLDPDU Frames

As shown in [Figure 13-3](#) on page 13-6, each LLDPDU frame contains the following mandatory TLVs:

- **Chassis ID** — The chassis identification for the device that transmitted the LLDP packet.
- **Port ID** — The identification of the specific port that transmitted the LLDP packet. The receiving LLDP agent joins the chassis ID and the port ID to correspond to the entity connected to the port where the packet was received.
- **Time to Live** — The length of time that information contained in the receive LLDP packet will be valid.
- **End of LLDPDU** — Indicates the final TLV of the LLDPDU frame.

**Figure 13-3 Frame Format**

M = Mandatory TLV (required for all LLDPDUs)

Each LLDPDU frame can also contain the following optional TLVs:

- Port Description — The port from which the LLDP agent transmitted the frame.
- System Name — The system's administratively assigned name.
- System Description — Includes the system's name, hardware version, OS level, and networking software version.
- System Capabilities — A bitmap that defines the primary functions of the system. The currently defined capabilities include, among other things, WLAN access point, router, and telephone.
- Management Address — The IP or MAC address associated with the local LLDP agent that may be used to reach higher layer entities.

An LLDPDU frame can also contain the following extension TLVs:

- 802.1 VLAN extension TLVs describe attributes associated with VLANs:
  - Port VLAN ID — Allows a bridge port to advertise the port's VLAN identifier (PVID) that will be associated with untagged or priority tagged frames it receives.
  - Port & Protocol VLAN ID — Allows a bridge to advertise whether it supports protocol VLANs and, if so, what VLAN IDs these protocols will be associated with.
  - VLAN Name — Allows a bridge to advertise the textual name of any VLAN with which it is configured.
  - Protocol Identity — Allows a bridge to advertise the particular protocols that are accessible through its port.
- 802.3 LAN interface extensions TLVs describe attributes associated with the operation of an 802.3 LAN interface:
  - MAC/PHY Configuration/Status — Advertises the bit-rate and duplex capability of the sending 802.3 node, the current duplex and bit-rating of the sending 802.3 node, and whether these settings were the result of auto-negotiation during link initiation or manual override.
  - Power-Via-MDI — Advertises the power-via-MDI capabilities of the sending 802.3 node.
  - Link-Aggregation — Advertises whether the link is capable of being aggregated, whether it is currently in an aggregation, and, if it is in an aggregation, the port of the aggregation.

- Maximum Frame Size — Advertises the maximum supported 802.3 frame size of the sending station.
- LLDP-MED extension TLVs:
  - Capabilities — Indicates the network connectivity device’s capabilities.
  - Network Policy — Used to configure tagged/untagged VLAN ID/L2 priority/DSCP on LLDP-MED endpoints (for example, IP phones).
  - Location Identification — Provides the location identifier information to communication endpoint devices, based on the configuration of the network connectivity device it is connected to.
  - Extended Power via MDI — Enables advanced power management between LLDP-MED endpoints and network connectivity devices.
  - Inventory Management — Includes hardware revision, firmware revision, software revision, serial number, manufacturer name, model name, and asset ID.

Some TLVs support multiple subtypes. For example, Port ID is sent as an ifName (for example, ge.1.1) between Enterasys devices, but when an LLDP-MED endpoint is detected on a port, that TLV subtype changes to a network address (MAC address), and other MED TLVs are sent, as defined by the MED spec.

## Configuring LLDP

### LLDP Configuration Commands

[Table 13-1](#) lists LLDP configuration commands. The table indicates which commands are device specific.

**Table 13-1 LLDP Configuration Commands**

| Task                                                                                                                                                                                                                                                                                                                                                                             | Command                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| Set the time, in seconds, between successive LLDP frame transmissions initiated by changes in the LLDP local system information. Default value is 30 seconds.                                                                                                                                                                                                                    | <code>set lldp tx-interval frequency</code>          |
| Set the time-to-live value used in LLDP frames sent by this device. The time-to-live for LLDPDU data is calculated by multiplying the transmit interval by the hold multiplier. The default value is 4.                                                                                                                                                                          | <code>set lldp hold-multiplier multiplier-val</code> |
| Set the minimum interval between LLDP notifications sent by this device. LLDP notifications are sent when a remote system change has been detected. The default value is 5 seconds.                                                                                                                                                                                              | <code>set lldp trap-interval frequency</code>        |
| Set the number of fast start LLDPDUs to be sent when an LLDP-MED endpoint device is detected. Network connectivity devices transmit only LLDP TLVs in LLDPDUs until they detect that an LLDP-MED endpoint device has connected to a port. At that point, the network connectivity device starts sending LLDP-MED TLVs at a fast start rate on that port. The default value is 3. | <code>set lldp med-fast-repeat count</code>          |

**Table 13-1 LLDP Configuration Commands (continued)**

| Task                                                                                                                                                                                                                                                                                                                                                                                                          | Command                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable or disable transmitting and processing received LLDPDUs on a port or range of ports.                                                                                                                                                                                                                                                                                                                   | <code>set lldp port status {tx-enable   rx-enable   both   disable} port-string</code>                                                                                                                                                                                                                                 |
| Enable or disable sending LLDP traps when a remote system change is detected.                                                                                                                                                                                                                                                                                                                                 | <code>set lldp port trap {enable   disable} port-string</code>                                                                                                                                                                                                                                                         |
| Enable or disable sending an LLDP-MED trap when a change in the topology has been sensed on the port (that is, a remote endpoint device has been attached or removed from the port).                                                                                                                                                                                                                          | <code>set lldp port med-trap {enable   disable} port-string</code>                                                                                                                                                                                                                                                     |
| Configure LLDP-MED location information on a port or range of ports. Currently, only Emergency Call Services (ECS) Emergency Location Identification Number (ELIN) is supported. ELIN is a special phone number used to indicate location, and is assigned and associated with small geographies in the organization. It is one of the forms of identification that the location identification TLV provides. | <code>set lldp port location-info elin elin-string port-string</code>                                                                                                                                                                                                                                                  |
| Select the optional LLDP and LLDP-MED TLVs to be transmitted in LLDPDUs by the specified port or ports.                                                                                                                                                                                                                                                                                                       | <code>set lldp port tx-tlv {[all]   [port-desc] [sys-name] [sys-desc] [sys-cap] [mgmtaddr] [vlan-id] [stp] [lacp] [gvrp] [mac-phy] [poe] [link-aggr] [max-frame] [medcap] [med-pol] [med-loc] [med-poe]} port-string</code>                                                                                            |
| Configure network policy for a set of applications on a port or range of ports. The policies configured with this command are sent in LLDPDUs as LLDP-MED Network Policy TLVs. Multiple Network Policy TLVs can be sent in a single LLDPDU.                                                                                                                                                                   | <code>set lldp port network-policy {all   voice   voice-signaling   guest-voice   guest-voice-signaling   softphone-voice   video-conferencing   streaming-video   video-signaling} [state {enable   disable}] [ tag {tagged   untagged}] [vid {vlan-id   dot1p}] [cos cos-value] [dscp dscp-value] port-string</code> |
| Return LLDP parameters to their default values.                                                                                                                                                                                                                                                                                                                                                               | <code>clear lldp {all   tx-interval   hold-multiplier   trap-interval   med-fast-repeat}</code>                                                                                                                                                                                                                        |
| Return the port status to the default value of both (both transmitting and processing received LLDPDUs are enabled).                                                                                                                                                                                                                                                                                          | <code>clear lldp port status port-string</code>                                                                                                                                                                                                                                                                        |
| Return the port LLDP trap setting to the default value of disabled.                                                                                                                                                                                                                                                                                                                                           | <code>clear lldp port trap port-string</code>                                                                                                                                                                                                                                                                          |
| Return the port LLDP-MED trap setting to the default value of disabled.                                                                                                                                                                                                                                                                                                                                       | <code>clear lldp port med-trap port-string</code>                                                                                                                                                                                                                                                                      |
| Return the port ECS ELIN location setting to the default value of null.                                                                                                                                                                                                                                                                                                                                       | <code>clear lldp port location-info elin port-string</code>                                                                                                                                                                                                                                                            |
| Return network policy for a set of applications on a port or range of ports to default values.                                                                                                                                                                                                                                                                                                                | <code>clear lldp port network-policy {all   voice   voice-signaling   guest-voice   guest-voice-signaling   softphone-voice   video-conferencing   streaming-video   video-signaling} {[state ] [ tag ] [vid ] [cos ] [dscp ] } port-string</code>                                                                     |

**Table 13-1 LLDP Configuration Commands (continued)**

| Task                                                                                                                                    | Command                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Clear the optional LLDP and LLDP-MED TLVs to be transmitted in LLDPDUs by the specified port or ports to the default value of disabled. | <code>clear lldp port tx-tlv {[all]   [port-desc] [sys-name] [sys-desc] [sys-cap] [mgmtaddr] [vlan-id] [stp] [lacp] [gvrp] [mac-phy] [poe] [link-aggr] [max-frame] [medcap] [med-pol] [med-loc] [med-poe]} port-string</code> |

Refer to your device's *CLI Reference Guide* for more information about each command.

## Basic LLDP Configuration

[Procedure 13-1](#) describes the basic steps to configure LLDP on all Enterasys switch devices.

### Procedure 13-1 Configuring LLDP

| Step | Task                                                                                                                                                                                                                | Command(s)                                                                                                                                                                                  |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Configure global system LLDP parameters.                                                                                                                                                                            | <code>set lldp tx-interval</code><br><code>set lldp hold-multiplier</code><br><code>set lldp trap-interval</code><br><code>set lldp med-fast-repeat</code><br><code>clear lldp</code>       |
| 2.   | Enable/disable specific ports to: <ul style="list-style-type: none"> <li>Transmit and process received LLDPDUs</li> <li>Send LLDP traps</li> <li>Send LLDP-MED traps</li> </ul>                                     | <ul style="list-style-type: none"> <li><code>set/clear lldp port status</code></li> <li><code>set/clear lldp port trap</code></li> <li><code>set/clear lldp port med-trap</code></li> </ul> |
| 3.   | Configure an ECS ELIN value for specific ports.                                                                                                                                                                     | <code>set/clear lldp port location-info</code>                                                                                                                                              |
| 4.   | Configure Network Policy TLVs for specific ports.                                                                                                                                                                   | <code>set/clear lldp port network-policy</code>                                                                                                                                             |
| 5.   | Configure which optional TLVs should be sent by specific ports. For example, if you configured an ECS ELIN and/or Network Policy TLVs, you must enable those optional TLVs to be transmitted on the specific ports. | <code>set/clear lldp tx-tlv</code>                                                                                                                                                          |

### Example LLDP Configuration: Time to Live

This example sets the transmit interval to 20 seconds and the hold multiplier to 5, which will configure a time-to-live of 100 to be used in the TTL field in the LLDPDU header.

```
System(rw)->set lldp tx-interval 20
System(rw)->set lldp hold-multiplier 5
```

### Example LLDP Configuration: Location Information

After you configure a location information value, you must also configure the port to send the Location Information TLV with the `set lldp port tx-tlv` command. This example configures the ELIN identifier 5551234567 on ports ge.1.1 through ge.1.6 and then configures the ports to send the Location Information TLV.

```
System(rw)->set lldp port location-info 5551234567 ge.1.1-6
```

```
System(rw)->set lldp port tx-tlv med-loc ge.1.1-6
```

## LLDP Display Commands

Table 13-2 lists LLDP show commands.

**Table 13-2 LLDP Show Commands**

| Task                                                                                                                                                                                     | Command                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display LLDP configuration information.                                                                                                                                                  | <code>show lldp</code>                                                                                                                                                                                 |
| Display the LLDP status of one or more ports.                                                                                                                                            | <code>show lldp port status [port-string]</code>                                                                                                                                                       |
| Display the ports that are enabled to send an LLDP notification when a remote system change has been detected or an LLDP-MED notification when a change in the topology has been sensed. | <code>show lldp port trap [port-string]</code>                                                                                                                                                         |
| Display information about which optional TLVs have been configured to be transmitted on ports.                                                                                           | <code>show lldp port tx-tlv [port-string]</code>                                                                                                                                                       |
| Display configured location information for one or more ports.                                                                                                                           | <code>show lldp port location-info [port-string]</code>                                                                                                                                                |
| Display the local system information stored for one or more ports.                                                                                                                       | <code>show lldp port local-info [port-string]</code>                                                                                                                                                   |
| Display the remote system information stored for a remote device connected to a local port.                                                                                              | <code>show lldp port remote-info [port-string]</code>                                                                                                                                                  |
| Display LLDP port network policy configuration information.                                                                                                                              | <code>show lldp port network policy {all   voice   voice-signaling   guest-voice   guestvoice-signaling   software-voice   video-conferencing   streaming-video   videosignaling} [port-string]</code> |

Refer to your device's *CLI Reference Guide* for a description of the output of each command.

## Configuring Enterasys Discovery Protocol

### Enterasys Discovery Protocol Configuration Commands

Table 13-3 lists Enterasys Discovery Protocol configuration commands.

**Table 13-3 Enterasys Discovery Protocol Configuration Commands**

| Task                                                                                 | Command                                                            |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Enable or disable the Enterasys Discovery Protocol on one or more ports.             | <code>set cdp state {auto   disable   enable} [port-string]</code> |
| Set a global Enterasys Discovery Protocol authentication code.                       | <code>set cdp auth auth-code</code>                                |
| Set the message interval frequency (in seconds) of the Enterasys Discovery Protocol. | <code>set cdp interval frequency</code>                            |
| Set the hold time value for Enterasys Discovery Protocol configuration messages.     | <code>set cdp hold-time hold-time</code>                           |

**Table 13-3 Enterasys Discovery Protocol Configuration Commands (continued)**

| Task                                                     | Command                                                                                      |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Reset Enterasys Discovery Protocol settings to defaults. | <code>clear cdp {[state] [port-state port-string] [interval] [hold-time] [auth-code]}</code> |

Refer to your device's *CLI Reference Guide* for more information about each command.

## Example Enterasys Discovery Protocol Configuration

This example shows how to globally enable CDP:

```
System(rw)->set cdp state enable
```

This example shows how to enable the CDP for port ge.1.2:

```
System(rw)->set cdp state enable ge.1.2
```

This example shows how to disable the CDP for port ge.1.2:

```
System(rw)->set cdp state disable ge.1.2
```

## Enterasys Discovery Protocol Show Commands

[Table 13-4](#) lists Enterasys Discovery Protocol show commands.

**Table 13-4 Enterasys Discovery Protocol Show Commands**

| Task                                                                                        | Command                                   |
|---------------------------------------------------------------------------------------------|-------------------------------------------|
| Display the status of the CDP discovery protocol and message interval on one or more ports. | <code>show cdp [port-string]</code>       |
| Display Network Neighbor Discovery information from all supported discovery protocols.      | <code>show neighbors [port-string]</code> |

Refer to your device's *CLI Reference Guide* for a description of the output of each command.

## Configuring Cisco Discovery Protocol

The following points describe how the Cisco DP extended trust settings work on the switch.

- A Cisco DP port trust status of trusted or untrusted is only meaningful when a Cisco IP phone is connected to a switch port and a PC or other device is connected to the back of the Cisco IP phone.
- A Cisco DP port state of trusted or untrusted only affects tagged traffic transmitted by the device connected to the Cisco IP phone. Untagged traffic transmitted by the device connected to the Cisco IP phone is unaffected by this setting.
- If the switch port is configured to a Cisco DP trust state of **trusted** (with the **trusted yes** parameter of this command), this setting is communicated to the Cisco IP phone instructing it to allow the device connected to it to transmit traffic containing any CoS or Layer 2 802.1p marking.
- If the switch port is configured to a Cisco DP trust state of **untrusted (trusted no)**, this setting is communicated to the Cisco IP phone instructing it to overwrite the 802.1p tag of traffic transmitted by the device connected to it to 0, by default, or to the value specified by the **cos** parameter of this command.

- There is a one-to-one correlation between the value set with the **cos** parameter and the 802.1p value assigned to ingress traffic by the Cisco IP phone. A value of 0 equates to an 802.1p priority of 0. Therefore, a value of 7 is given the highest priority.



**Note:** The Cisco Discovery Protocol must be globally enabled using the **set cisdnp status** command before operational status can be set on individual ports.

## Cisco Discovery Protocol Configuration Commands

Table 13-5 lists Cisco Discovery Protocol configuration commands.

**Table 13-5 Cisco Discovery Protocol Configuration Commands**

| Task                                                                                                                                                                           | Command                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable or disable Cisco Discovery Protocol globally on the device.                                                                                                             | <code>set cisdnp status {auto   enable   disable}</code>                                                                                                                               |
| Set the number of seconds between Cisco Discovery Protocol PDU transmissions.                                                                                                  | <code>set cisdnp timer time</code>                                                                                                                                                     |
| Set the time to live (TTL) for Cisco Discovery Protocol PDUs. This is the amount of time (in seconds) neighboring devices will hold PDU transmissions from the sending device. | <code>set cisdnp holdtime time</code>                                                                                                                                                  |
| Set the status, voice VLAN, extended trust mode, and CoS priority for untrusted traffic for the Cisco Discovery Protocol on one or more ports.                                 | <code>set cisdnp port { [status {disable   enable}] [ vvid {&lt;vlan-id&gt; / none / dot1p / untagged}] [trust-ext {trusted   untrusted}] [cos-ext value] } &lt;port-string&gt;</code> |
| Clear the Cisco Discovery Protocol back to the default values.                                                                                                                 | <code>clear cisdnp { [status   timer   holdtime   port {status   vvid   trust-ext   cos-ext}] } &lt;port-string&gt;</code>                                                             |

Refer to your device's *CLI Reference Guide* for more information about each command.

## Example Cisco Discovery Protocol Configuration

This example shows how to enable Cisco Discovery Protocol on the device:

```
System(rw)->set cisdnp status enable
```

## Cisco Discovery Protocol Configuration Commands

Table 13-6 lists Cisco Discovery Protocol show commands.

**Table 13-6 Cisco Discovery Protocol Show Commands**

| Task                                                                                   | Command                                          |
|----------------------------------------------------------------------------------------|--------------------------------------------------|
| Display global Cisco Discovery Protocol information.                                   | <code>show cisdnp</code>                         |
| Display summary information about the Cisco Discovery Protocol on one or more ports.   | <code>show cisdnp port info [port-string]</code> |
| Display Network Neighbor Discovery information from all supported discovery protocols. | <code>show neighbors [port-string]</code>        |



Refer to your device's *CLI Reference Guide* for a description of the output of each command.



## Configuring Syslog

This chapter describes how System Logging, or Syslog, operates on Enterasys fixed stackable and standalone switches, and how to configure Syslog.

| For information about...                        | Refer to page... |
|-------------------------------------------------|------------------|
| <a href="#">System Logging Overview</a>         | 14-1             |
| <a href="#">Syslog Operation</a>                | 14-2             |
| <a href="#">Syslog Components and Their Use</a> | 14-3             |
| <a href="#">Interpreting Messages</a>           | 14-6             |
| <a href="#">About Security Audit Logging</a>    | 14-6             |
| <a href="#">Configuring Syslog</a>              | 14-8             |

### System Logging Overview

Syslog, short for System Logging, is a standard for forwarding log messages in an IP network that is typically used for network system management and security auditing. The term often applies to both the actual Syslog protocol, as well as the application sending Syslog messages.

As defined in RFC 3164, the Syslog protocol is a client/server-type protocol which enables a station or device to generate and send a small textual message (less than 1024 bytes) to a remote receiver called the Syslog server. Messages are transmitted using User Datagram Protocol (UDP) packets and are received on UDP port 514. These messages inform about simple changes in operational status or warn of more severe issues that may affect system operations.

When managed properly, logs are the eyes and ears of your network. They capture events and show you when problems arise, giving you information you need to make critical decisions, whether you are building a policy rule set, fine tuning an Intrusion Detection System, or validating which ports should be open on a server. However, since it is practically impossible to wade through the volumes of log data produced by all your servers and network devices, Syslog's ability to place all events into a single format so they can be analyzed and correlated makes it a vital management tool. Because Syslog is supported by a wide variety of devices and receivers across multiple platforms, you can use it to integrate log data from many different types of systems into a central repository.

Efficient Syslog monitoring and analysis reduces system downtime, increases network performance, and helps tighten security policies. It can help you:

- Troubleshoot switches, fire walls and other devices during installation and problem situations.
- Perform intrusion detection.
- Track user activity.

By default, Syslog is operational on Enterasys switch devices at startup. All generated messages are eligible for logging to local destinations and to remote servers configured as Syslog servers. Using simple CLI commands, you can adjust device defaults to configure the following:

- Message sources – which system applications on which modules should log messages?
- Message destinations – will messages be sent to the local console, the local file system, or to remote Syslog servers? Which facility (functional process) will be allowed to send to each destination?

## Syslog Operation

Developers of various operating systems, processes, and applications determine the circumstances that will generate system messages and write those specifications into their programs. Messages can be generated to give status, either at a certain period of time, or at some other interval, such as the invocation or exit of a program. Messages can also be generated due to a set of conditions being met. Typically, developers quantify these messages into one of several broad categories, generally consisting of the facility that generated them, along with an indication of the severity of the message. This allows system administrators to selectively filter the messages and be presented with the more important and time sensitive notifications quickly, while also having the ability to place status or informative messages in a file for later review.

Switches must be configured with rules for displaying and/or forwarding event messages generated by their applications. In addition, Syslog servers need to be configured with appropriate rules to collect messages so they can be stored for future reference.

### Syslog Operation on Enterasys Devices

The Syslog implementation on Enterasys devices uses a series of system logging messages to track device activity and status. These messages inform users about simple changes in operational status or warn of more severe issues that may affect system operations. Logging can be configured to display messages at a variety of different severity levels about application-related error conditions occurring on the device.

You can decide to have all messages stored locally, as well as to have all messages of a high severity forwarded to another device. You can also have messages from a particular facility sent to some or all of the users of the device, and displayed on the system console. For example, you may want all messages that are generated by the mail facility to be forwarded to one particular Syslog server. However you decide to configure the disposition of the event messages, the process of having them sent to a Syslog collector generally consists of:

- Determining which messages at which severity levels will be forwarded.
- Defining one or more remote receivers (Syslog servers/console displays).

### Filtering by Severity and Facility

Syslog daemons determine message priority by filtering them based on a combined facility and severity code. Severity indicates the seriousness of the error condition generating the Syslog message. This is a value from 1 to 8, with 1 indicating highest severity. Facility categorizes which functional process is generating an error message. The Enterasys implementation uses the eight facility designations reserved for local use: **local0** – **local7** defined in RFC 3164. You can modify these default facility and severity values to control message receipt and aid in message sorting on target servers.

For example, you can configure all router messages to go to Server 1 using facility local1, while all SNMP messages go to Server 1 using facility local2.

The following sections provide greater detail on modifying key Syslog components to suit your enterprise.

## Syslog Components and Their Use

Table 14-1 describes the Enterasys implementation of key Syslog components.

**Table 14-1 Syslog Terms and Definitions**

| Term     | Definition                                                                                                                                                                        | Enterays Usage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Facility | Categorizes which functional process is generating an error message. Syslog combines this value and the severity value to determine message priority.                             | Enterays uses the eight facility designations reserved for local use: <b>local0</b> – <b>local7</b> . Default is <b>local4</b> , which allows the message severity portion of the priority code to be visible in clear text, making message interpretation easiest. For more information about facility designations, refer to RFC 3164.                                                                                                                                                                                                                                                                                                                              |
| Severity | Indicates the severity of the error condition generating the Syslog message. The lower the number value, the higher will be the severity of the condition generating the message. | <p>Enterays devices provide the following eight levels:</p> <ul style="list-style-type: none"> <li>1 - emergencies (system is unusable)</li> <li>2 - alerts (immediate action required)</li> <li>3 - critical conditions</li> <li>4 - error conditions</li> <li>5 - warning conditions</li> <li>6 - notifications (significant conditions)</li> <li>7 - informational messages</li> <li>8 - debugging messages</li> </ul> <p>The default Syslog configuration allows applications (log message sources) to forward messages at a severity level of 6, and destinations (console, file system, or remote Syslog servers) to log messages at a severity level of 8.</p> |



**Note:** Numerical values used in Enterasys syslog CLI and the feature's configuration MIB range from 1-8. These map to the RFC 3164 levels of 0-7 respectively. Syslog messages generated report the RFC 3164 specified level values.

|             |                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application | Client software applications running on devices that can generate Syslog messages. | <p>Enterays supported applications and their associated CLI mnemonic values include:</p> <ul style="list-style-type: none"> <li><b>CLIWEB</b> - Command Line Interface and Webview management</li> <li><b>SNMP</b> - Simple Network Management Protocol</li> <li><b>STP</b> - Spanning Tree Protocol</li> <li><b>Driver</b> – Hardware drivers</li> <li><b>System</b> - Non-application items such as general chassis management</li> <li><b>Stacking</b> - Stacking management (if applicable)</li> <li><b>UPN</b> - User Personalized Networks</li> <li><b>Router</b> - Router</li> <li><b>Security</b> – Security audit logging</li> <li><b>RtrOspf</b> – OSPF</li> <li><b>RtrMcast</b> – Multicast</li> <li><b>RtrVrrp</b> – VRRP</li> </ul> <p>Use the <b>show logging application all</b> command to list supported applications and the corresponding CLI numeric or mnemonic values you can use to configure application logging on your devices.</p> |
|-------------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

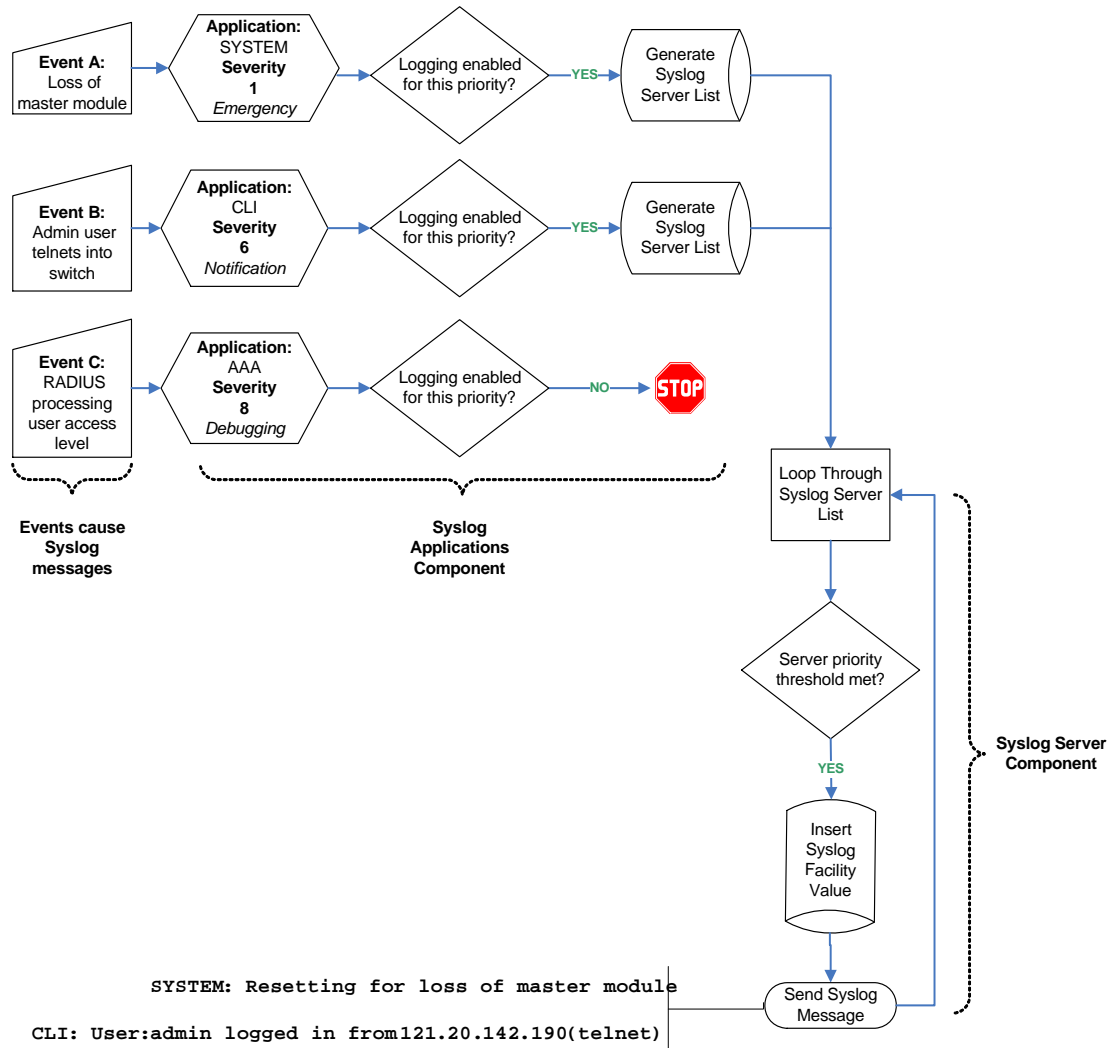
**Table 14-1 Syslog Terms and Definitions (continued)**

| Term          | Definition                                                       | Enterays Usage                                                                                                                                                                                                      |
|---------------|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syslog server | A remote server configured to collect and store Syslog messages. | Enterasys devices allow up to 8 server IP addresses to be configured as destinations for Syslog messages. By default, Syslog server is globally enabled, with no IP addresses configured, at a severity level of 8. |

## Basic Syslog Scenario

Figure 14-1 shows a basic scenario of how Syslog components operate on an Enterasys switch. By default, all applications running on the Enterasys switch are allowed to forward Syslog messages generated at severity levels 6 through 1. In the configuration shown, these default settings have not been changed.

Figure 14-1 Basic System Scenario



Default application settings in the example in Figure 14-1 have not been modified. Therefore, an emergency message triggered by a system reset due to loss of the master module is forwarded to Syslog destinations. The CLI-related message notifying that a user has logged in remotely is also forwarded. Configured Syslog server(s) will receive all forwarded messages since their default severity threshold is at 8 (accepting messages at all severity levels).

Any messages generated by applications at severity levels 7 and 8 are not forwarded in this example. For instance, forwarding does not occur for an AAA authentication-related debugging message with information about RADIUS access level processing for a particular user. If at some point in time it becomes necessary, for example, to log all AAA authentication-related message activity and to save it to a file so authentication details can be tracked, the administrator can allow that specific application to forward debugging messages to a Syslog server, as well as to the console and persistent file storage.

For more information on how to configure these basic settings, refer to “[Syslog Command Precedence](#)” on page 14-8, and the “[Configuration Examples](#)” on page 14-12.

## Interpreting Messages

Every system message generated by the Enterasys switch platforms follows the same basic format:

```
<facility/severity> time stamp address application [unit] message text
```

### Example

This example shows Syslog informational messages, displayed with the **show logging buffer** command. It indicates that messages were generated by facility code 16 (local4) at severity level 5 from the CLI application on IP address 10.42.71.13.

```
Switch1(rw)->show logging buffer
<165>Sep 4 07:43:09 10.42.71.13 CLI[5]User:rw logged in from 10.2.1.122 (telnet)
<165>Sep 4 07:43:24 10.42.71.13 CLI[5]User: debug failed login from 10.4.1.100
(telnet)
```

[Table 14-2](#) describes the components of these messages.

**Table 14-2 Syslog Message Components**

| Component         | Description                                                                                                                                                                                                                                                                                               | Example Code                                                                    |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Facility/Severity | Combined code indicating the facility generating the message and the severity level used to determine message priority. Facility codes 16 - 23 are Syslog designations for local0 - local7, the Enterasys supported designations for local use. For a complete list of facility codes, refer to RFC 3164. | <165> = Numerical code indicating a message from facility local4 at severity 5. |
| Time stamp        | Month, date, and time the Syslog message appeared.                                                                                                                                                                                                                                                        | Sep  4 07:43:09                                                                 |
| Address           | IP address of the client originating the Syslog message.                                                                                                                                                                                                                                                  | 10.42.71.13                                                                     |
| Application       | Client process generating the Syslog message.                                                                                                                                                                                                                                                             | CLI                                                                             |
| Unit              | Location of the device generating the Syslog message.                                                                                                                                                                                                                                                     | [5] = unit 5 in stack                                                           |
| Message text      | Brief description of error condition.                                                                                                                                                                                                                                                                     | User: debug failed login from 10.4.1.100 (telnet)                               |

## About Security Audit Logging

Security audit logging provides a mechanism to generate a separate and secure log file, in addition to the previously existing unsecured log file (“current.log”).

The secure permanent log file, named “secure.log,” records security related events occurring on the switch. The secure log file contains 1000 256-byte log entries and is managed as a circular list. Up to 10 files are allowed in the secure directory, with a total size of 512 KB.

The “secure.log” file is stored in the **secure/logs** directory, which is only visible to and accessible by super user accounts. Super-users can create, edit, and delete files in the secure directory, and can copy files to and from the secure directory.



The `secure.log` file stored in the `secure/logs` directory cannot be deleted, edited, or renamed. Super-users can copy the `secure.log` file using SCP, SFTP, or TFTP.

By default, security audit logging is disabled. Only a system administrator (super-user) may enable the security audit logging function, and only a system administrator has the ability to retrieve, copy, or upload the `secure.log` file. Security audit logging is enabled or disabled with the command `set logging local`.

## Security Events Logged

A new logging application identifier, "Security," has been defined to specify the level of logging desired. When "Security" is set to level 5, the following security audit logs will be generated:

- Logins and logouts
- Login failures

When "Security" is set to level 6, the following security audit logs will additionally be generated:

- Login banner acceptance
- Excessive logon attempts
- Remote system access
- Changes in privileges or security attributes
- Changes of security levels or categories of information
- Failed attempts to access restricted privilege level or data files
- Audit file access
- Password changes (actual passwords will not recorded)

When "Security" is set to level 7, the following security audit logs will additionally be generated:

- All CLI commands that are executed. The following information is logged for each command:
  - Date and time
  - Local IP address
  - User
  - Source (console, web, SSH or telnet)
  - Remote IP address (if SSH, telnet or web)
  - The action (command line text)
  - Status of command (OK or FAILED)
- Any hidden debug commands entered by the user will be logged.

## Trap Generation

When approximately 80% of the maximum security audit logs have been written to the log file, an SNMP trap will be generated to indicate a high percentage of utilization. Recording to the log file will continue and wrap back to the beginning when the maximum number of entries has been recorded. All successive occurrences of reaching 80% of the log file will generate an additional trap.

The trap generation is done using the Enterasys Syslog Client MIB notification `etsysSyslogSecureLogArchiveNotification`.

If, for any reason, an event that is to be sent to the secure log gets dropped, resulting in the failure to record the event, an SNMP trap will be generated. The trap generation will be done using the Enterasys Syslog Client MIB notification `etsysSyslogSecureLogDroppedMsgNotification`.

## Format Examples

The following examples illustrate secure log entry formats for different types of events.

- User logs in via console

```
<164>Apr 21 08:44:13 10.27.12.70-1 USER_MGR[1] User:admin:su logged in from console
```

- User logs in via Telnet

```
<164>Apr 21 08:42:57 10.27.12.70-1 USER_MGR[1] User:admin:su logged in from 10.27.6.118(telnet)
```

- User sets port speed via console

```
<167>Apr 21 10:39:19 10.27.12.70-1 CLI_WEB[1] User:admin:su; Source:console; Action:"set port speed *.*.1 10 "; Status:OK
```

- User sets port speed via telnet

```
<167>Apr 21 10:39:39 10.27.12.70-1 CLI_WEB[1] User:admin:su; Source:10.27.6.118(telnet); Action:"set port speed *.*.2 100"; Status:OK
```

## Configuring Syslog

Use the procedures in this section to perform the following logging configuration tasks:

- [“Syslog Command Precedence”](#) (page 14-8)
- [“Configuring Syslog Server\(s\)”](#) (page 14-9)
- [“Modifying Syslog Server Defaults”](#) (page 14-10)
- [“Reviewing and Configuring Logging for Applications”](#) (page 14-10)
- [“Enabling Console Logging and File Storage”](#) (page 14-11)
- [“Configuration Examples”](#) (page 14-12)

## Syslog Command Precedence

[Table 14-3](#) lists basic Syslog commands and their order of precedence on Enterasys switches.

**Table 14-3 Syslog Command Precedence**

| Syslog Component | Command                                                                                                                                   | Function                                                                                                                                                                                                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Logging defaults | <code>set logging default</code><br>{ <code>[[facility facility]</code><br><code>[severity severity]</code><br><code>[port port]</code> } | Sets default parameters for facility code, severity level and/or UDP port for all Syslog servers and local destinations.<br><br>Settings will be applied when Syslog servers are configured without specifying values with the <b>set logging server</b> command. This command overrides factory defaults. |

**Table 14-3 Syslog Command Precedence (continued)**

| Syslog Component     | Command                                                                                                                                        | Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server settings      | <code>set logging server index ip-addr ip-addr [facility facility] [severity severity] [descr descr] [port port] state enable   disable</code> | During or after new server setup, specifies a server index, IP address, and operational state for a Syslog server. Optionally, this command specifies a facility code, severity level at which messages will be accepted, text string description, and/or UDP port for the specified server.<br><br>This command overrides system defaults for the specified server. If not specified with this or the <b>set logging default</b> command, optional server parameters will be set to the system defaults listed in <a href="#">Table 14-4</a> on page 14-10. |
| Application settings | <code>set logging application { [mnemonic   all] } [level level] [servers servers]</code>                                                      | Sets the severity level at which one or all applications will send messages to Syslog servers. If not specified, settings will apply to all configured servers and severity level will not be changed from system defaults.                                                                                                                                                                                                                                                                                                                                  |

## About Server and Application Severity Levels

By default, client applications will forward Syslog messages at severity levels 6 through 1, and servers will log messages at all severity levels (8 through 1). You can use the procedures described in this chapter to change these parameters, fine tuning the scope of message logging and modifying the Syslog behavior between one or more client applications and one or more servers.

## Configuring Syslog Server(s)

Use the following commands to configure one or more servers as destinations for Syslog messages and verify the configuration:

1. Add a Syslog server to the device's server list:

```
set logging server index ip-addr ip-addr state enable
```

*Index* is a value from 1 to 8 that specifies the server table index number for this server.

2. (Optional) Verify the server configuration:

```
show logging server [index]
```

If *index* is not specified, information for all configured Syslog servers will be displayed.

### Example

This sample output from the **show logging server** command shows that two servers have been added to the device's Syslog server list. These servers are using the default UDP port 514 to receive messages from clients and are configured to log messages from the local1 and local2 facilities, respectively. Logging severity on both servers is set at 5 (accepting messages at severity levels 5 through 1). Using the commands described in the next section, these settings can be changed on a per-server basis, or for all servers.

```
Switch1(rw)->show logging server
```

|   | IP Address     | Facility | Severity   | Description | Port | Status  |
|---|----------------|----------|------------|-------------|------|---------|
| 1 | 132.140.82.111 | local1   | warning(5) | default     | 514  | enabled |
| 2 | 132.140.90.84  | local2   | warning(5) | default     | 514  | enabled |

## Modifying Syslog Server Defaults

Unless otherwise specified, the switch will use the default server settings listed in [Table 14-4](#) for its configured Syslog servers:

**Table 14-4 Syslog Server Default Settings**

| Parameter | Default Setting          |
|-----------|--------------------------|
| facility  | local4                   |
| severity  | 8 (accepting all levels) |
| descr     | no description applied   |
| port      | UDP port 514             |

Use the following commands to change these settings either during or after enabling a new server.

### Displaying System Logging Defaults

To display system logging defaults, or all logging information, including defaults:

```
show logging {default|all}
```

### Modifying Default Settings

You can change factory default logging settings using one of the following methods.

- To specify logging parameters during or after new server setup:

```
set logging server index ip-addr ip-addr [facility facility] [severity severity] [descr descr] [port port] state enable
```

If not specified, optional server parameters will be set to the system defaults listed in [Table 14-4](#). Refer back to [Filtering by Severity and Facility](#) and to [Table 14-1](#) for more information on how these parameters operate.

- To change default parameters for all servers:

```
set logging default {[facility facility] [severity severity] [port port]}
```

### Examples

This example shows how to configure the switch to forward messages from facility category local6 at severity levels 3, 2, and 1 to Syslog server 1 at IP address 134.141.89.113:

```
Switch1(rw)->set logging server 1 ip-addr 134.141.89.113 facility local6 severity 3
```

This example shows how to change Syslog defaults so that messages from the local2 facility category at a severity level of 4 will be forwarded to all servers. These settings will apply to all newly-configured servers, unless explicitly configured with the **set logging server** command:

```
Switch1(rw)->set logging default facility local2 severity 4
```

## Reviewing and Configuring Logging for Applications

By default, all applications running on Enterasys switch devices are allowed to forward messages at severity levels 6 through 1 to all configured destinations (Syslog servers, the console, or the file system).

## Displaying Current Application Severity Levels

To display logging severity levels for one or all applications currently running on your device:

```
show logging application {mnemonic | all}
```

### Example

This example shows output from the **show logging application all** command. A numeric and mnemonic value for each application is listed with the severity level at which logging has been configured and the server(s) to which messages will be sent. In this case, logging for applications has not been changed from the default severity level of 6. This means that notifications and messages with severity values 6 through 1 will be sent to configured servers.



**Note:** Depending on your platform, you may see different applications listed from those shown in the following example.

```
System(su)->show logging application all
```

| Application  | Current Severity Level | Server List        |
|--------------|------------------------|--------------------|
| 89 CLIWEB    | 6                      | 1-8, console, file |
| 90 SNMP      | 6                      | 1-8, console, file |
| 91 STP       | 6                      | 1-8, console, file |
| 92 Driver    | 6                      | 1-8, console, file |
| 93 System    | 6                      | 1-8, console, file |
| 94 Stacking  | 6                      | 1-8, console, file |
| 112 UPN      | 6                      | 1-8, console, file |
| 118 Router   | 6                      | 1-8, console, file |
| 120 Security | 6                      | 1-8, console, file |

|                |              |                  |
|----------------|--------------|------------------|
| 1(emergencies) | 2(alerts)    | 3(critical)      |
| 4(errors)      | 5(warnings)  | 6(notifications) |
| 7(information) | 8(debugging) |                  |

## Enabling Console Logging and File Storage

Stackable and standalone switch devices allow you to display logging messages to the console and save to a persistent file.

Console logging allows you to view only as many messages as will fit on the screen. As new messages appear, old messages simply scroll off the console. While this is a temporary means of logging information, it allows you to track very specific activities quickly and easily. Console log messages can also be saved to a persistent file.

Use the following commands to review and configure console logging and file storage.

### Displaying to the Console and Saving to a File

To display log messages to the console and save to a persistent file:

```
set logging local console enable file enable
```



**Note:** The **set logging local** command requires that you specify both console and file settings. For example, **set logging local console enable** would not execute without also specifying **file enable** or **disable**.

## Configuration Examples

### Enabling a Server and Console Logging

[Procedure 14-1](#) shows how you would complete a basic Syslog configuration. In this example, the default application severity level has not been modified, allowing all applications to forward messages to configured destinations. One Syslog server is configured on IP address 10.1.1.2, logging all messages. Console logging is enabled, but persistent file storage is not.

#### Procedure 14-1 Configuring a Server and Console Logging

| Step | Task                                                                                                     | Command(s)                                                |
|------|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| 1.   | Configure Syslog server 1 and accept default settings (listed in <a href="#">Table 14-4</a> on page 10). | <b>set logging server 1 ip-addr 10.1.1.2 state enable</b> |
| 2.   | (Optional) Verify that application logging settings are at default values for the enabled server.        | <b>show logging application all</b>                       |
| 3.   | Enable console logging and disable file storage.                                                         | <b>set logging local console enable file disable</b>      |



**Note:** The **set logging local** command requires that you specify both console and file settings. For example, **set logging local console enable** would not execute without also specifying **file enable** or **disable**.

### Adjusting Settings to Allow for Logging at the Debug Level

[Procedure 14-2](#) shows how you would adjust the previous Syslog configuration so that all AAA-related authentication messages (level 8) could be forwarded to Server 2 at IP address 10.1.1.3, displayed on the console and saved to persistent file storage. This would enable all Syslog messaging capabilities for this particular application. Since the severity for this new server has not changed from the default of level 8, there is no need to adjust this setting.

#### Procedure 14-2 Adjusting Settings for an Application

| Step | Task                                                                                                     | Command(s)                                                |
|------|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| 1.   | Configure Syslog server 2 and accept default settings (listed in <a href="#">Table 14-4</a> on page 10). | <b>set logging server 2 ip-addr 10.1.1.3 state enable</b> |
| 2.   | Set the severity level for the AAA application to level 8.                                               | <b>set logging application AAA level 8 servers 2</b>      |
| 3.   | Enable console logging and file storage.                                                                 | <b>set logging local console enable file enable</b>       |

## Configuring Spanning Tree

This chapter provides the following information about configuring and monitoring the Spanning Tree protocol on Enterasys stackable and standalone fixed switches.

| For information about...                                              | Refer to page... |
|-----------------------------------------------------------------------|------------------|
| <a href="#">Spanning Tree Protocol Overview</a>                       | 15-1             |
| <a href="#">STP Operation</a>                                         | 15-3             |
| <a href="#">Functions and Features Supported on Enterasys Devices</a> | 15-6             |
| <a href="#">Spanning Tree Basics</a>                                  | 15-9             |
| <a href="#">Configuring STP and RSTP</a>                              | 15-19            |
| <a href="#">Configuring MSTP</a>                                      | 15-24            |
| <a href="#">Understanding and Configuring SpanGuard</a>               | 15-29            |
| <a href="#">Understanding and Configuring Loop Protect</a>            | 15-31            |
| <a href="#">Terms and Definitions</a>                                 | 15-36            |

### Spanning Tree Protocol Overview

The Spanning Tree Protocol (STP) resolves the problem of physical loops in a network by establishing one primary path between any two devices. Duplicate paths are barred from use and become standby or “blocked” paths until the primary path fails, at which point the redundant path can be brought into service.

STP operates by forming a fully connected tree of data loop free LAN connected bridges (switches) through the exchange of Bridge Protocol Data Units (BPDUs). Each bridge port transmits BPDUs on a periodic basis. The information contained in the BPDU is used by the receiving bridge to calculate a port role for each bridge port. There is one bridge in the network chosen to be the root bridge, based on its bridge ID. Ports that directly connect bridges to the root bridge or are connected through another bridge are assigned one of four roles:

- Root Port – The best path to the root
- Designated Port – Ports which either provide a path to the root for other bridges or connect end users
- Backup Port – A port attached to a LAN where another port of the same bridge is a designated port. This backup port takes over the designated role should the LAN’s designated port become disabled
- Alternate Port – A port providing a path to the root that is not root, designated, or backup

For a summary of port roles, see [Table 15-2](#) on page 15-13.

While the network is in a steady state, alternate and backup ports are in blocking state; root and designated ports are in forwarding state.

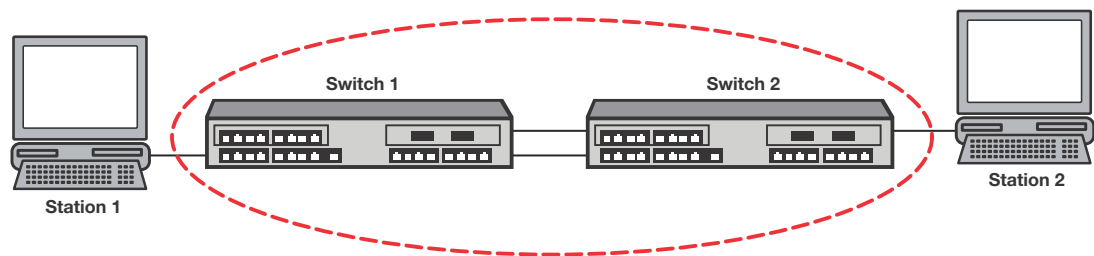
STP allows for the automatic reconfiguration of the network. When bridges are added to or removed from the network, root election takes place and port roles are recalculated.

## Why Use Spanning Trees?

Redundant links must be factored into even the simplest of topologies to protect against data loss and downtime due to any single point of failure. STP prevents redundant links from forming data loops which would consume all available network bandwidth. STP manages redundant links by keeping them in a blocking state and automatically unblocking them when changes in topology require that they be used. See [Table 15-3](#) on page 15-13 for a summary of Spanning Tree port states.

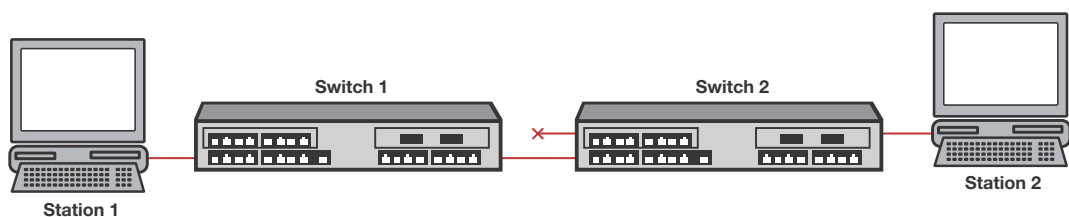
As shown in [Figure 15-1](#), a planned redundant link between Switch 1 and Switch 2 makes it possible for a bridging loop to occur. If Station 1 transmits a multicast or broadcast packet to Station 2 in this scenario, the packet would continue to circulate endlessly between both switching devices. Without Spanning Tree blocking one of the links, there would be nothing at layer 2 to stop this loop from happening and unnecessarily consuming network resources. As administrator, you would be forced to manually disable one of the links between Switch 1 and 2 for the [Figure 15-1](#) network to operate.

**Figure 15-1 Redundant Link Causes a Loop in a Non-STP Network**



STP automatically blocks redundant paths, as shown in [Figure 15-2](#). In the event that the primary (unblocked) path fails, STP places the blocked path into service. If the original primary path recovers, the redundant path will once again block and the primary path will be used.

**Figure 15-2 Loop Avoided When STP Blocks a Duplicate Path**



## Spanning Tree on Enterasys Platforms

By default, Spanning Tree is enabled globally on stackable, and standalone fixed switch devices and is enabled on all ports. The design of the Spanning Tree protocol and the default configuration values on these devices make user configuration unnecessary in order to add redundant ports to your network. You will want to make configuration changes to select a root bridge, take advantage of Multiple Spanning Tree, or use any of the advanced features described below. Before configuring STP it is important to understand how it works.



## STP Operation

Enterasys switch devices support the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP) as defined in the following standards and described in IEEE 802.1Q:

- IEEE 802.1D (Spanning Tree Protocol)
- IEEE 802.1w (Rapid Spanning Tree Protocol)
- IEEE 802.1s (Multiple Spanning Tree Protocol)
- IEEE 802.1t (Update to 802.1D)

STP forms a network of bridges connected by LANs into a tree that is:

- Predictable – A given set of configured bridges always yields the same topology when the network reaches steady state
- Optimized – STP selects the best path to the root bridge
- Fully connected – Each bridge communicates with every other bridge in the network
- Free from data loops – One root port is chosen in a bridge and the remaining ports with paths to the root bridge are put into blocking mode

The root bridge is the bridge with the lowest bridge ID in the network and functions as the logical center of the STP network. Each bridge calculates its best path to the root using the information contained in BPDUs received from its neighbor bridges. Non-root bridges select the root port among all the ports receiving BPDUs. BPDUs advertise a bridge's cost to the root bridge. The root port is chosen from the ports with received BPDUs indicating a path to the root. The root port will have the lowest cost path to the root. In the case of multiple ports offering identical costs, tie breaking is based upon the transmitting bridge ID, transmitting port ID, and receive port ID. For MSTP there are additional fields to consider – internal path cost and regional root ID. These are all discussed in more detail below.

Once the root port has been established, STP determines the other port roles. Ports providing a path to root but are not the root port become alternate ports because they provide an alternate path to the root. Other operational ports that provide a path to the root for attached bridges have the designated role. There is another type of port known as a backup port. A backup port attaches to a LAN where another port of the same bridge is a designated port. A backup port does not become part of the active topology unless the LAN's designated port is disabled and the backup port takes over the designated role.

The alternate and backup ports are set to blocking state while the root and designated ports move to the forwarding state.

Bridge priority, port path cost, and port priority are configurable parameters that are part of the port role calculation and may be modified to create the desired topology.

**Bridge Priority** – A typical network configuration would place two or more bridges in the core. To preserve root in the core, the core bridges would each have their bridge priority set to a lower value than bridges you do not desire to be root. The default bridge priority value is 32768. If you desire a particular bridge to be root, set its bridge priority to a lower value than bridges that should not be root. Otherwise the bridge with the lowest MAC address is set to root.

**Port Path Cost** – If it is desired for a bridge to use one link over another, the administrative port path cost may be modified. The default of zero ensures that the link with the highest speed gets chosen.

**Port Priority** – Port Priority may be set but is not typically modified, as Link Aggregation is usually run on multiple links between two bridges.

## Rapid Spanning Tree Operation

Rapid Spanning Tree (RSTP) optimizes convergence in a properly configured network by significantly reducing the time to reconfigure the network's active topology when physical topology or configuration parameter changes occur. RSTP is defined in the IEEE 802.1w standard. Spanning Tree's primary goal is to ensure a fully connected, loop-free topology. A secondary goal, realized with the introduction of RSTP, is to move root and designated ports to the forwarding state as quickly as possible.

In a stable topology all the root and designated ports will be forwarding and the alternate and backup ports will be blocking. When there is a network topology change, Spanning Tree recalculates port roles. Ports which are no longer part of the active topology will be put into blocking state. New designated ports will only forward after receiving an acknowledgement or, in the case of a port being connected to a non-RSTP device (802.1d), after a sufficient amount of time has passed.

When a topology change occurs, a change in port operational status or new information contained in BPDUs is immediately acted upon. A new root port moves to forwarding state as soon as any recent former root port is put into blocking state. A designated port moves to forwarding state once the connected device acknowledges agreement with the new topology information. This is typically an exchange of two BPDUs. These rules ensure an orderly transition from the old topology to the new topology by preventing transient loops.

## Multiple Spanning Tree Operation

The Multiple Spanning Tree Protocol (MSTP) provides for traffic forwarding on multiple ports for each bridge. A single Spanning Tree only allows for single root port forwarding per bridge. MSTP provides for a number of common network requirements that cannot be configured on a single Spanning Tree (for example, the segregation of traffic over multiple VLANs or optimizing the utilization of redundant links between switching devices in a network).

An MSTP configuration is made up of one or more:

- Multiple Spanning Tree (MST) Regions – A set of connected bridges that share the same MST configuration ID
- MST configuration IDs – A unique identifier for each MST region
- Spanning Tree Identifiers (STIs) – A unique identifier for each Spanning Tree

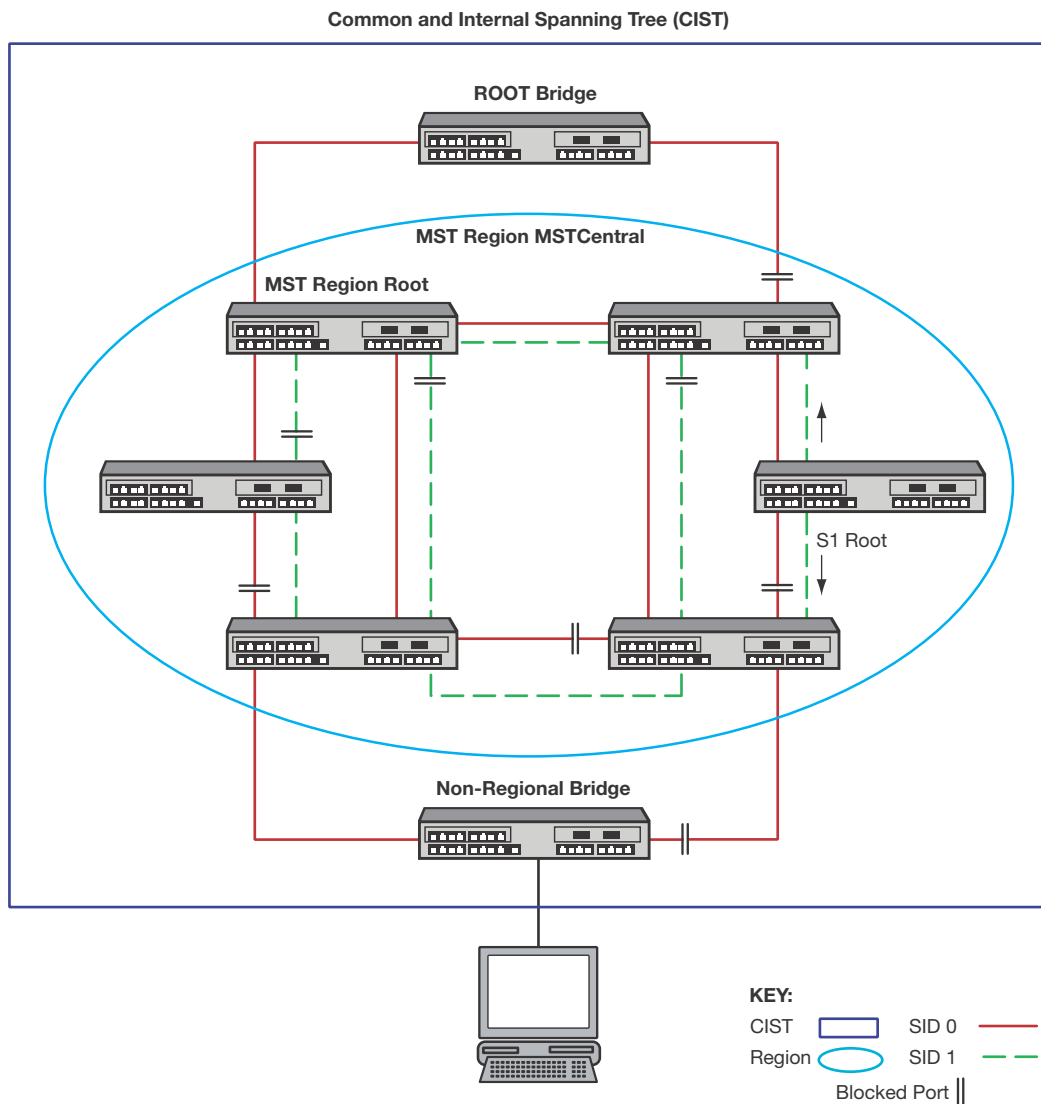
An MSTP configuration is made up of zero or more Multiple Spanning Tree Instances (MSTIs). An MSTI is an STI that exists within an MST region other than the default STI 0.

All bridges in the Spanning Tree network are inter-connected by STI 0 and can belong to:

- The Common Spanning Tree (CST) – A Spanning Tree defined in the IEEE 802.1q standard that assumes one Spanning Tree instance for the entire bridged network, regardless of the number of VLANs
- An Internal Spanning Tree (IST) instance – A Spanning Tree instance that extends the CST inside the MST region and represents the entire MST region as a single CST virtual bridge to the outside world.

One or more MSTs can be part of the Common and Internal Spanning Tree (CIST). The CIST represents the connectivity of the entire network. [Figure 15-3](#) on page 15-5 provides an overview of an MST configuration with one MST region within the CIST. The MST region's configuration ID name is **MSTCentral**.

Figure 15-3 Multiple Spanning Tree Overview



SID 0 is the default Spanning Tree and interconnects all bridges to the Root Bridge. SID 0 within the MST is the Internal Spanning Tree (IST) and provides connectivity out to the CST as well as functioning as another Spanning Tree instance within the MST region. SID 1 is an MSTI configured within the MST region.

Each SID has a root bridge. In Figure 15-3 the SID 0 root bridge belongs to the CST. The SID 0 root bridge functions as root for SID 0 Spanning Tree instance in both the CST and MST. SID 1 only exists within the **MSTCentral** region. The root for SID 1 is a bridge within the MSTCentral region. SID 1 can provide traffic segmentation by forwarding traffic on a second VLAN within the MSTCentral region or provide for optimization of redundant links by forwarding traffic within the MSTCentral region on the same VLAN.

See “[Configuring MSTP](#)” on page 15-24 for examples of MSTP traffic segregation and optimization of redundant links.



**Note:** MSTP and RSTP are fully compatible and interoperable with each other and with legacy STP.

# Functions and Features Supported on Enterasys Devices

## Spanning Tree Versions

MSTP and RSTP automatically detect the version of Spanning Tree being used on a LAN. RSTP bridges receiving MSTP BPDUs interpret them as RSTP BPDUs. MSTP and RSTP bridges receiving STP BPDUs will switch to use STP BPDUs when sending on the port connected to the STP bridge. MSTP incorporates a force version feature that allows you to administratively force MSTP to behave as STP or RSTP. This will cause all ports of the bridge to transmit STP or RSTP BPDUs. Use the force version feature when the MSTP bridge is attached to a device that cannot properly handle a non-STP BPDU.



**Note:** Forcing a bridge to STP will prevent it from joining a region and will disable rapid reconfiguration.

## Maximum SID Capacities

By default, Multiple Spanning Tree mode is globally enabled on Enterasys switching devices and a single Spanning Tree is configured as SID 0.

Maximum device SID capacities are (specified values are in addition to SID 0):

**Table 15-1 Maximum SID Capacities Per Platform**

| Platform   | Maximum SID Capacity                                          |
|------------|---------------------------------------------------------------|
| Stackable  | 4 SID, except for the C5 which supports up to 8 SID instances |
| Standalone | 4 SID instances                                               |

## Network Diameter

Enterasys switching devices support a default 20-bridge span from and including the root bridge. You can configure support for a maximum span of up to 40 bridges from the Spanning Tree root in the Common Spanning Tree (CST) or the Common and Internal Spanning Tree (CIST) regional root within an MST region. Max age defines the diameter for the CST and Maxhops defines the diameter within a region. See [“Defining the Maximum Age Time”](#) on page 15-23.

## Port Forwarding

MSTP and RSTP use rapid forwarding mechanisms to get ports to the forwarding state. However, there is a difference in forwarding time between user ports and inter-switch links (ISLs). If a user port is defined as `admindedge TRUE` using the `set spantree adminedge` command, it will forward as soon as the port becomes operational. An ISL will forward based on an exchange of BPDUs. By default, `autoedge` is set to `TRUE` and `admindedge` is set to `FALSE`. These settings satisfy most requirements. `Autoedge` allows a port defined as `admindedge FALSE` to discover in a short period of time that it is an edge port. The only time it is necessary to set `admindedge` to `TRUE` is when the attached user device cannot tolerate the several seconds required for autodetection to detect the port as a user port and move it to forwarding. Setting an ISL to `admindedge TRUE` should be avoided because it can lead to transient data loops.

## Disabling Spanning Tree

Spanning Tree may be disabled globally or on a per port basis. If Spanning Tree is disabled globally all linked ports will be in a forwarding state and the Spanning Tree Protocol will not run. Additionally, a received BPDU will be treated as any multicast packet and flooded out all ports.

If Spanning Tree is disabled on a port by setting portadmin to disabled using the **set spantree portadmin** command, the port will be in a forwarding state and the protocol will not run for that port. A received BPDU will be consumed. The intention is that the port terminates the Spanning Tree domain. For instance, the port may be attached to a router. If this port were accidentally attached to another switching port, a data loop may result.

## STP Features

Enterasys switching devices provide seamless Spanning Tree functionality by:

- Creating a single Spanning Tree from any arrangement of switching or bridging elements.
- Compensating automatically for the failure, removal, or addition of any switching device in an active data path.
- Achieving port changes in short time intervals, which establishes a stable active topology quickly with minimal network disturbance.
- Using a minimum amount of communications bandwidth to accomplish the operation of the Spanning Tree Protocol.
- Reconfiguring the active topology in a manner that is transparent to stations transmitting and receiving data packets.
- Managing the topology in a consistent and reproducible manner through the use of Spanning Tree Protocol parameters.
- Increasing security and reliability with SpanGuard, as described below and in [“Understanding and Configuring SpanGuard”](#) on page 15-29.
- Further protecting your network from loop formation with Loop Protect, as described below and in [“Understanding and Configuring Loop Protect”](#) on page 15-31.
- Supporting more port density and faster port speeds as described in [“Updated 802.1t”](#) on page 15-8

### SpanGuard

The Enterasys SpanGuard feature helps protect your network from two situations that can cause a Denial of Service (DoS) condition: repeated topology change notifications and an unwanted bridge being inserted into and forcing traffic through the topology. SpanGuard increases security and reliability by preventing Spanning Tree respans that can occur when BPDUs are received on user ports and notifies network management that they were attempted.

If a SpanGuard enabled port receives a BPDU, it becomes locked and transitions to the blocking state. It will only transition out of the blocking state after a globally specified time or when it is manually unlocked. By default, SpanGuard is globally disabled on stackable and standalone fixed switch devices and must be globally enabled to operate on all user ports. For a more detailed discussion of the SpanGuard feature, refer to [“Understanding and Configuring SpanGuard”](#) on page 15-29.

### Loop Protect

The Loop Protect feature prevents or short circuits loop formation caused by redundant paths in your network by requiring ports to receive BPDUs (RSTP/MSTP only) on point-to-point ISLs

before their states are allowed to become forwarding. Further, if a BPDU timeout occurs on a port, its state becomes listening until a new BPDU is received. In this way, both upstream and downstream facing ports are protected.

When a root or alternate port loses its path to the root bridge, due to message age expiration, it takes on the role of designated port and will not forward traffic until a BPDU is received. When a port is intended to be the designated port in an ISL, it constantly proposes and will not forward until a BPDU is received. It will revert to listening if it stops getting a response. Loop Protect also overrides the port admin setting. This protects against misconfiguration (such as disabling STP on a port using the **set spantree portadmin port-string disable** command) and protocol failure by the connected bridge. By default, the Loop Protect feature is globally disabled on Enterasys switch devices and must be globally enabled to operate on all ports. For configuration information, refer to “[Understanding and Configuring Loop Protect](#)” on page 15-31.

## Updated 802.1t

IEEE 802.1t is enabled by default on Enterasys switch devices. This updated Spanning Tree protocol supports multiple Spanning Trees, more switch port density, and faster port speeds.

802.1t includes the following updates:

- New bridge identifier encoding (4-bit priority, 12-bit system ID extension, 48-bit bridge address)
- New port identifier encoding (4-bit priority, 12-bit port number)
- Bridge detection state machine (for edge port identification)
- Path cost default values (the ability to switch between 802.1t and 802.1d mode and cost values)

## Multisource Detection

Multisource detection is a feature that prevents network disruption due to excessive topology changes caused by a full duplex port transmitting multiple BPDUs with different source MAC addresses, and hence different BPDU information.

When a port is point-to-point, the received priority information comes from the most recently received BPDU. When a port is non-point-to-point, the received information reflects the best priority information out of all the received BPDUs. Typical scenarios for multisource detection are when a switch is connected to a device which

- has been improperly configured to forward received BPDUs out other ports, or
- has been configured to not run the Spanning Tree protocol and treats BPDUs as multicast packets by transmitting them out all other forwarding ports.

In these situations, the connected port is effectively acting as a shared media device. The way to detect shared media is the duplex setting. Since the port is full duplex, it treats the connection as point-to-point.

Multisource Detection, which is always enabled, will recognize the multiple source MAC addresses and set the port’s operational point-to-point status to false, treating the port as a shared media device. The port is constantly monitored. If the situation is resolved, as determined by receiving a unique address for a sufficient amount of time, the port’s operational point-to-point status will revert to true.

A syslog message is issued when multiple source addresses are detected.



**Note:** When loop protect is configured for the port, if multisource detection is triggered, the port will go to the listening state and no longer be part of the active topology. Loop protect does not operate on shared media ports.

## Spanning Tree Basics

This section provides you with a more detailed understanding of how the Spanning Tree operates in a typical network environment.

| For information about...                                                 | Refer to page... |
|--------------------------------------------------------------------------|------------------|
| <a href="#">Spanning Tree Bridge Protocol Data Units</a>                 | 15-9             |
| <a href="#">Electing the Root Bridge</a>                                 | 15-9             |
| <a href="#">Assigning Path Costs</a>                                     | 15-9             |
| <a href="#">Paths to Root</a>                                            | 15-10            |
| <a href="#">Identifying Designated, Alternate, and Backup Port Roles</a> | 15-12            |
| <a href="#">Assigning Port States</a>                                    | 15-13            |
| <a href="#">RSTP Operation</a>                                           | 15-14            |
| <a href="#">MSTP Operation</a>                                           | 15-14            |

### Spanning Tree Bridge Protocol Data Units

The most elemental task of a Spanning Tree Bridge is to control the forwarding state of each port. The bridge evaluates the information received from its immediate neighbors in the form of BPDUs, along with its own configured information. From this information a root is elected and then port roles may be selected for each port. For the root port and designated ports the desired state is forwarding. These ports will become forwarding by subsequent exchange of BPDUs or through the expiration of protocol timers according to the state machines defined by the Spanning Tree Protocol. The remaining ports will become discarding (shorthand for the states of blocking, listening, and learning).

To facilitate this process, the bridge transmits BPDUs out each port on a periodic basis as well as in response to events such as changes in port operational status, configuration changes, timer expiration, and changes in topology derived from received BPDUs.

### Electing the Root Bridge

The network topology is determined by the selection of the root bridge. The topology is based on each bridge's best path to root. Root election occurs on each bridge when new information is received from a neighboring bridge in a BPDU, when link is lost on a port connecting a neighboring bridge, or when the bridge's priority is administratively changed.

The root is elected by comparing the root IDs received in BPDUs as well as the bridge's own bridge ID. The bridge with the lowest ID is chosen as root. The bridge ID is an 8-byte value with the 2 most significant bytes being the bridge priority and the 6 least significant bytes being the bridge MAC address. Root may be forced to a particular bridge by the configuration of bridge priority. Among bridges with the same bridge priority, the one with the lowest MAC address is elected root. If a bridge receives no BPDUs indicating a better bridge ID than its own, it becomes the root bridge.

### Assigning Path Costs

Path costs are one factor in determining port roles. Each LAN segment has an operational path cost associated with it. The cost is based on the port speed, by default. The higher the speed, the lower the cost. Port costs for link aggregations are based on the aggregate speed of all the

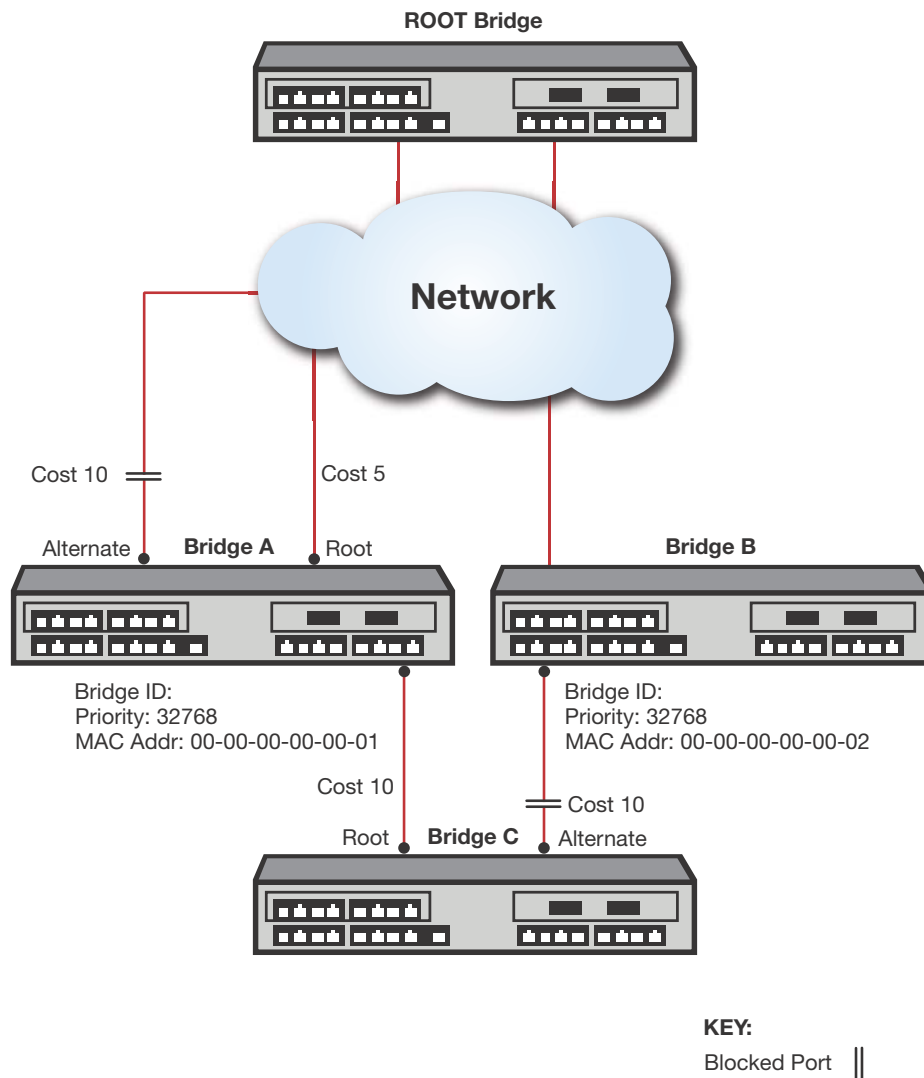


underlying physical ports. The port cost value may also be administratively assigned using the `set spantree adminpathcost` command. This may be done to choose a particular path.

## Paths to Root

If the bridge is not elected as root, one or more ports provide a path back to the root bridge. The port with the best path is selected as the root port. The best path is the one that has the lowest designated cost. The lowest cost is the aggregate cost of all the LANs traversed between the port and the root bridge. [Figure 15-4](#) on page 15-10 displays root port configuration based upon lowest cost for Bridge A. If multiple ports have the same lowest cost, the one with the lowest bridge ID becomes the root port. [Figure 15-4](#) displays root port configuration based upon lowest bridge ID for Bridge C.

**Figure 15-4 Root Port Selection Based On Lowest Cost or Bridge ID**

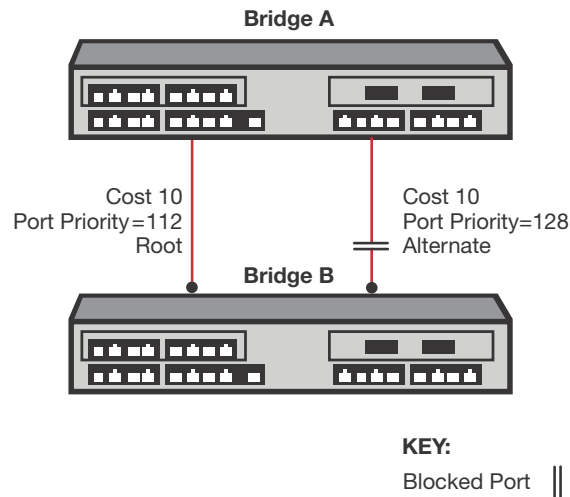


If there are ports with the same bridge ID, the port ID is used as a tie breaker. The port with the lowest port ID is chosen as root port. The port ID is a 2-byte value with the 4 most significant bits being the port priority and the 12 least significant bits being the bridge port number. Because the port priority occupies the most significant bits in the port ID, setting a lower port priority assures



that port will be selected as root. In the case of no single port having a lowest port priority, the root port is selected based upon the overall port ID value. [Figure 15-5](#) on page 15-11 presents a root port configuration for Bridge B determined by the port priority setting. If there is still a tie, these ports are connected via a shared medium. The final tie breaker is the receiving port ID.

**Figure 15-5 Root Port Selection Based On Lowest Port ID**

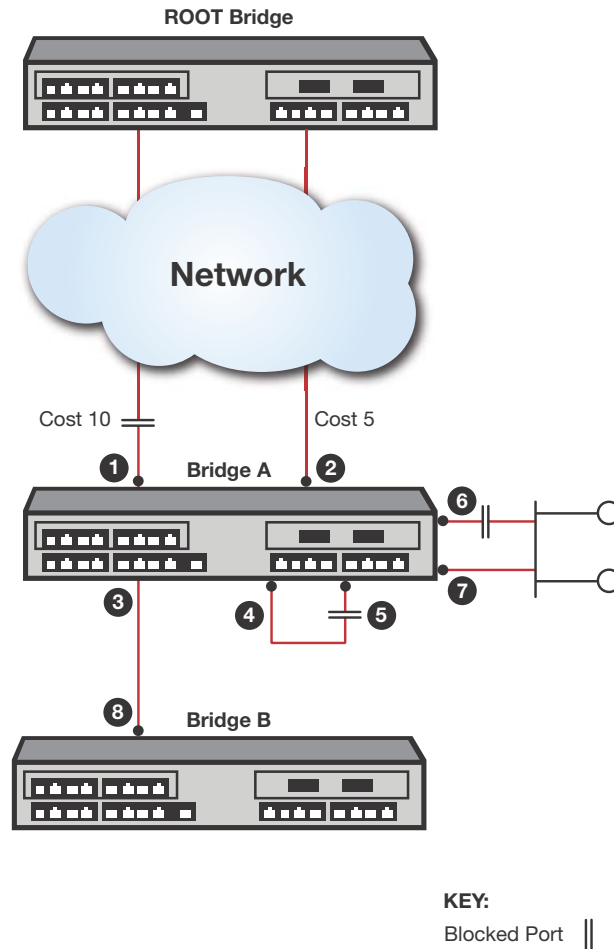


After selecting the root port, the bridge's cost to root is the total of the root port's designated cost as advertised in the received BPDU, plus the path cost associated with that port. In a hierarchically designed network, the designated cost for ports attached to the next higher level will be less than the bridge's cost to the root. Ports attached to bridges on the same level will have designated costs equal to the bridge's cost to the root. Likewise, this bridge's port will advertise the bridge's cost to the root. Thus one port connected to the LAN will be the designated port and the other(s) will be alternate. The port on the bridge with the lower ID will be the designated port.

## Identifying Designated, Alternate, and Backup Port Roles

Ports in a Spanning Tree configuration are assigned one of four roles: root, designated, alternate, or backup. [Figure 15-6](#) presents an overview of Spanning Tree port roles.

**Figure 15-6 Spanning Tree Port Role Overview**



- |   |                                   |   |                                   |
|---|-----------------------------------|---|-----------------------------------|
| 1 | Port 1, Bridge A, Alternate Port  | 5 | Port 5, Bridge A, Backup Port     |
| 2 | Port 2, Bridge A, Root Port       | 6 | Port 6, Bridge A, Backup Port     |
| 3 | Port 3, Bridge A, Designated Port | 7 | Port 7, Bridge A, Designated Port |
| 4 | Port 4, Bridge A, Designated Port | 8 | Port 1, Bridge B, Root Port       |

All ports which act as edge ports take on the designated port role. If the bridge has been elected root, all ports connected to ports on other bridges are also designated ports.

On non-root bridges, Spanning Tree identifies ports which provide a path to the root bridge and selects the best path among these as the root port as described in “[Paths to Root](#)” on page 15-10 ([Figure 15-6](#), call out 2). There may be only a single port providing a path to root, in which case that is the root port and the remaining ports are designated. If there are other ports providing a path to root, these ports are selected as alternate paths. Should the root port become disabled, one of the alternate ports will be selected as the new root port. ([Figure 15-6](#), call out 1)

A port which is not a designated port, but is connected to another port on the same bridge ([Figure 15-6](#), call out 5) or connected to a shared LAN on which this bridge already provides a

designated port (Figure 15-6, call out 6), takes the role of backup port. In the shared LAN example it may take over as designated port if the original designated port is disabled.

All operational ports which are not root, alternate or backup are designated ports. These ports provide a path to the root for attached devices.

Table 15-2 provides a summary of STP port roles.

**Table 15-2 Spanning Tree Port Roles**

| Port Role  | Description                                                                                                                                         |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Root       | The one port that is used to connect to the root bridge. It is elected based on its least “path-cost” to the root bridge and is forwarding traffic. |
| Alternate  | Any redundant upstream port that provides an alternate path to the root bridge (other than the root port). Alternate ports are set to blocking.     |
| Designated | Any downstream port that provides a path back to the root bridge for a downstream bridge. This port is forwarding traffic.                          |
| Backup     | A port that acts as a redundant designated port on a shared LAN. Backup ports are set to blocking.                                                  |

## Assigning Port States

All ports are blocking when the operational status switches from disabled to enabled. By default, automatic edge detection is enabled and ports are configured as non-edge ports. In this scenario a user port will become forwarding in several seconds. A port configured as an edge port will forward immediately.

Ports which are selected as alternate or backup ports are immediately put into the discarding state and remain discarding until a new port role is selected. The root port may go to the forwarding state as long as any recent former root ports are synchronized with the new root information. Designated ports may forward as soon as the attached port signals agreement as specified by RSTP. In the absence of the above conditions, root and designated ports get to the forwarding state through the use of timers. The value of the timers is dependent on the value of ForceVersion. The default value is MSTP. If the value is StpCompatible, the timer values are derived from forward delay. Otherwise the values are derived from hello time.

Table 15-3 provides a summary of STP port states.

**Table 15-3 Spanning Tree Port States**

| Port State | Behavior                                                                                                                                                                                                              |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Blocking   | Actively preventing traffic from using this path. Still receiving BPDUs, so continuing to monitor for management and STA information.                                                                                 |
| Listening  | Continuing to block traffic while waiting for protocol information to determine whether to go back to the blocking state or continue to the learning state. Listens to BPDUs to ensure no loops occur on the network. |
| Learning   | Learning station location information but continuing to block traffic.                                                                                                                                                |
| Forwarding | Forwarding traffic and continuing to learn station location information.                                                                                                                                              |
| Disabled   | Disabled administratively or by failure.                                                                                                                                                                              |
| Discarding | Used as shorthand for blocking, listening, or learning state.                                                                                                                                                         |

## RSTP Operation

RSTP optimizes convergence by significantly reducing the time to reconfigure the network's active topology when physical topology or configuration parameter changes occur. RSTP provides rapid connectivity following the failure of a switching device, switch port, or the addition of a switch into the network.

A new root port may forward as soon as any recent root ports are put into blocking.

A designated port may forward with the exchange of two BPDUs in rapid succession. The designated port presents new BPDU information with a proposal request. The attached port processes the BPDU and may respond immediately with an agreement. Upon reception of that agreement BPDU, the designated port may move to forwarding. Another feature of RSTP is that designated ports transmit periodic BPDUs regardless of reception of BPDUs at the root port. This insulates the network from jitter in receiving BPDUs, particularly at the edge.

Important STP timers are max age, hello time, and forward delay. The default values for the timers are:

- Hello time – 2 seconds
- Forward delay – 15 seconds
- Max age – 20 seconds

The operational values from these timers are derived from the root bridge. The current IEEE standard for Spanning Tree fixes hello time at 2 seconds. The Enterasys switches covered in this document do not enforce this restriction to allow existing configurations to remain compatible. It is not recommended that a value other than 2 seconds be used. Other values may not interact well with other non-variable protocol times such as edgeDelayWhile or mDelayWhile. The max age timer may be adjusted to change the network diameter. Take care to consider that failure in the network may cause the topology to “unravel” causing the diameter to become larger than anticipated. An insufficient value could cause devices near or at the edge of the network to become unreachable. For example, in a ring topology of 10 bridges, no bridge is more than 5 hops from the root. A max age that accounts for 6 hops would be sufficient. A failure of ports immediately interconnecting a bridge with the root would break the ring topology and change the furthest hop from the root from 5 to 9. Any bridges beyond the configured network diameter of 6 would cause the Spanning Tree topology not to converge.

## MSTP Operation

MSTP makes it possible for VLAN switching devices to use multiple Spanning Trees, allowing traffic belonging to different VLANs to flow over potentially different paths within the LAN. It builds upon the advancements of RSTP with its decreased time for network re-spans. MSTP's principle objective is to increase bandwidth utilization by allowing:

- Frames assigned to different VLANs to follow different data routes
- Ports to block for some Spanning Trees and forward for others
- Every inter-switch link in the topology to be forwarding for at least one Spanning Tree

MSTP is the default Spanning Tree mode on all Enterasys switch devices.

## Common and Internal Spanning Tree (CIST)

MSTP uses all Spanning Tree region information to create a single Common and Internal Spanning Tree (CIST) that represents the connectivity of the entire network. This is equivalent to the single Spanning Tree used for STP and RSTP.

The MSTP enabled network may contain any combination of Single Spanning Tree (SST) regions and Multiple Spanning Tree (MST) regions. A typical network may contain multiple MST regions as well as separate LAN segments running legacy STP and RSTP Spanning Tree protocols. The CIST contains a root bridge, which is the root of the Spanning Tree for the network. The CIST root may be, but is not necessarily, located inside an MST region. Each MST region contains a CIST regional root which may be the CIST root if the CIST root is internal to the region. If the CIST root is external to the region, the CIST regional root provides the connectivity to the CIST root. Bridges in an MSTP topology compare their received BPDUs to calculate their shortest path to the CIST root, CIST regional root, and MSTI regional root.

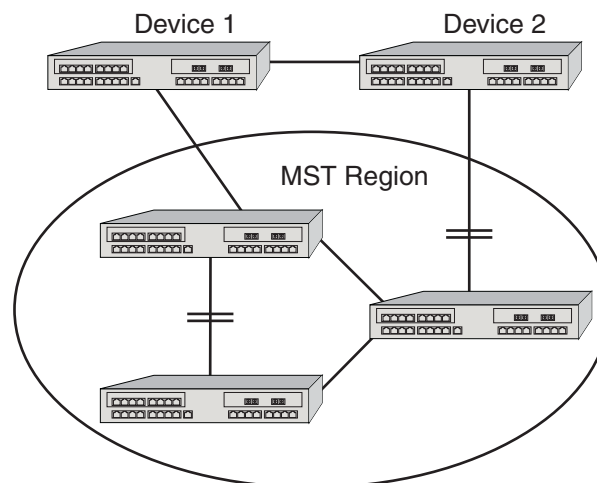
Ideally, there should be one all-encompassing region. This is not always possible, for example, when non-MSTP bridges exist such as those shown in [Figure 15-3](#) on page 15-5. From the outside, the region appears as a single Spanning Tree bridge which is part of the Common Spanning Tree (CST). A port which connects to a bridge not having the same MST configuration ID, or which is not running MSTP, forms part of the boundary of the region. The region attaches to the CST at the root port of the CIST regional root. All other region boundary ports which provide paths to the root are alternate ports and remain blocking until the topology changes, causing a new regional root port to be chosen. Ports which provide a path to the root for other bridges at the region boundary are designated ports. At boundary ports, port states for MSTIs follow the states of the CIST for the port.

## MST Region

An MST region is a group of devices that are configured together to form a logical region. The MST region presents itself to the rest of the network as a single switching device, which simplifies administration. Path cost is only incremented when traffic enters or leaves the region, regardless of the number of devices within the region. Each LAN can only be a member of one region.

[Figure 15-7](#) shows that the MST region appears as a single switching device to devices 1 and 2, but really consists of three devices.

**Figure 15-7 Example of an MST Region**



For a switching device to be considered as part of an MST region, it must be administratively configured with the same configuration identifier information as all other devices in the MST region. The configuration identifier consists of four parts:

- Format Selector – One octet in length and is always 0. It cannot be administratively changed.
- Configuration Name – A user-assigned, case sensitive name given to the region. The maximum length of the name is 32 octets. A bridge's default configuration name is a character

string corresponding to the bridge MAC address. This guarantees that the default behavior of a bridge is to not be part of an MST region.

- Revision Level – Two octets in length. The default value of 0 may be administratively changed.
- Configuration Digest – 16-octet HMAC-MD5 signature created from the configured VLAN Identification (VID)/Filtering Identification (FID) to Multiple Spanning Tree Instances (MSTI) mappings. All devices must have identical mappings to have identical configuration digests.

By default, each bridge is in its own MST region and has a default configuration name derived from the bridge MAC address. For example, if the bridge MAC address is **00-1f-45-9a-6c-b7**, the default MSTP configuration name is **“00:1f:45:9a:6c:b7”**. When grouping two or more bridges into a single MST region, you must assign the same configuration name to each member of the region. MD5 digests are derived from a mapping of a Filtering Database ID (FID) to a Spanning Tree ID (SID), referred to as a FID-to-SID mapping (see [“Multiple Spanning Tree Instances \(MSTI\)”](#) on page 15-16 for more information). Since there is a small probability of different mappings resulting in the same digest, the addition of administratively assigned name and version configuration ID parameters guarantee the uniqueness of the region.

SIDs exist within an MST region, each having a separate topology. Within an MST region there always exists the Internal Spanning Tree (IST) which is SID 0. There are zero or more Multiple Spanning Tree Instances (MSTIs). Each MSTI corresponds to a set of VIDs. One or more VIDs may be mapped to an SID using a FID-to-SID mapping. The IST and each MSTI may have different root bridges. Port path costs and bridge priorities may be different for each port/instance. Each bridge port has a unique port state per instance. With proper configuration, redundant links may be utilized to their maximum extent by each forwarding for one or more instances. See [“Configuring MSTP”](#) on page 15-24 for more detail on how to do this.

## Multiple Spanning Tree Instances (MSTI)

Inside the MST region, a wholly contained set of topologies is maintained separate from the outside world. For example, MSTI 1 in MST region A has no correspondence to MSTI 1 in MST region B.

**Table 15-4 Multiple Spanning Tree Instance Support**

| Platform                                                     | Number of Instances |
|--------------------------------------------------------------|---------------------|
| All stackables and standalones (except for the C5 stackable) | 4                   |
| C5 stackable                                                 | 8                   |

The Enterasys switch device by default maps VLAN IDs (VIDs) to Filtering IDs (FIDs) in a one-to-one correlation for bridges with the VLAN learning mode set to individual VLAN learning (IVL). The Enterasys fixed switches only support IVL.

For example, in an IVL bridge, FID 3 may contain VID 3 and FID 4 may contain VID 4. Regardless of the type of VLAN learning taking place, one or more FIDs may be mapped to a Spanning Tree Instance (SID). The end result is a mapping of VIDs to SIDs. SID topologies may then be configured to provide a type of load balancing. Note that without further configuration, each SID will have the same topology as the IST. Typically, load balancing will be achieved by choosing different root bridges in the core for the different instances.

## Determining FID-to-SID Mappings

VLANs are mapped to MSTIs through a FID-to-SID mapping which is the key element in an MSTP configuration. Each VLAN is associated to a FID and is mapped to Spanning Tree IDs using their FID association. The mapping is performed by the **set spantree mstmap** command. This mapping is represented within the MST configuration digest described in the previous section and

displayed in the following example. By default, every bridge will have a FID-to-SID mapping that equals VLAN FID 1/SID 0.

Use the **show spantree mstcfgid** command to determine MSTI configuration identifier information, and whether or not there is a misconfiguration due to non-matching configuration identifier components:

This example shows how to display MSTI configuration identifier information. In this case, this bridge belongs to "Region1":

```
Enterasys->show spantree mstcfgid
MST Configuration Identifier:
 Format Selector: 0
 Configuration Name: Region1
 Revision Level: 88
 Configuration Digest: 6d:d7:93:10:91:c9:69:ff:48:f2:ef:bf:cd:8b:cc:de
```

In order for other bridges to belong to Region1, all four elements of those bridges' configuration id output must match. The default value that must be changed for this to happen is the configuration name setting. Also, the MSTIs must be created and the FIDs mapped to them.

Use the **set spantree mstcfgid** command to change the configuration name from the default bridge MAC address value.

This example changes the default bridge configuration name to **Region1**:

```
Enterasys->set spantree mstcfgid cfgname Region1
```

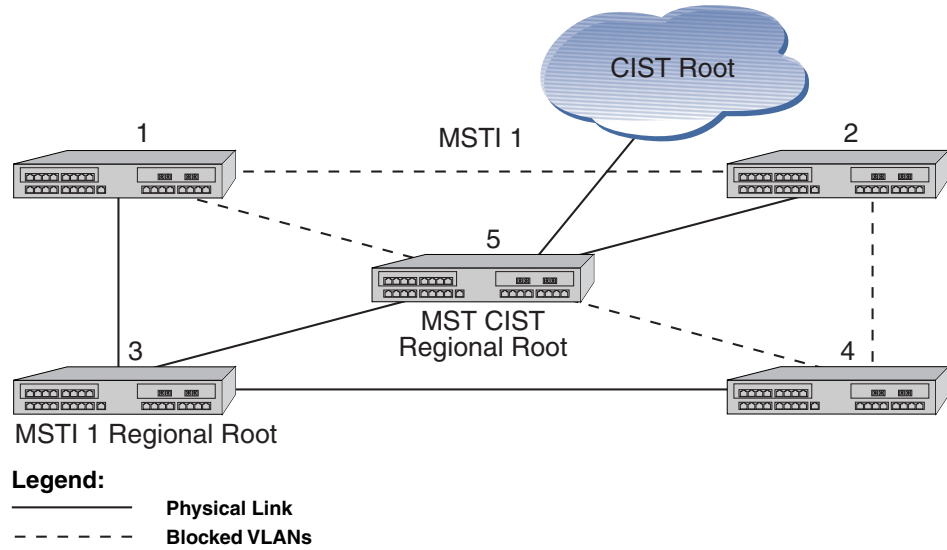
For the configuration digest to match, the mapping of VIDs to SIDs must match. Use these commands to configure the SIDs, map the FIDs to the SIDs and display the VID-SID and FID-SID mappings:

```
Enterasys->set spantree msti sid 3 create
Enterasys->set spantree msti sid 4 create
Enterasys->set spantree mstmap 3 sid 3
Enterasys->set spantree mstmap 4 sid 4
Enterasys->show spantree mstilist
Configured Multiple Spanning Tree Instances:
 3 4
Enterasys->show spantree mstmap
Fid 3 is mapped to Sid 3
Fid 4 is mapped to Sid 4
Enterasys->show spantree vlanlist
Vlan 3 is mapped to Sid 3
Vlan 4 is mapped to Sid 4
```

Since an MSTI is a separate Spanning Tree, each MSTI has its own root inside the MST region. [Figure 15-8](#) on page 15-18 and [Figure 15-9](#) on page 15-18 show two MSTIs in a single region. Switching device 3 is the root for MSTI 1, switching device 2 is the root for MSTI 2, and switching device 5 is the CIST regional root. Traffic for all the VLANs attached to an MSTI follow the MSTI's spanned topology.

Various options may be configured on a per-MSTI basis to allow for differing topologies between MSTIs. To reduce network complexity and processing overhead needed to maintain MSTIs, you should only create as many MSTIs as needed.

**Figure 15-8 MSTI 1 in a Region**



**Figure 15-9 MSTI2 in the Same Region**

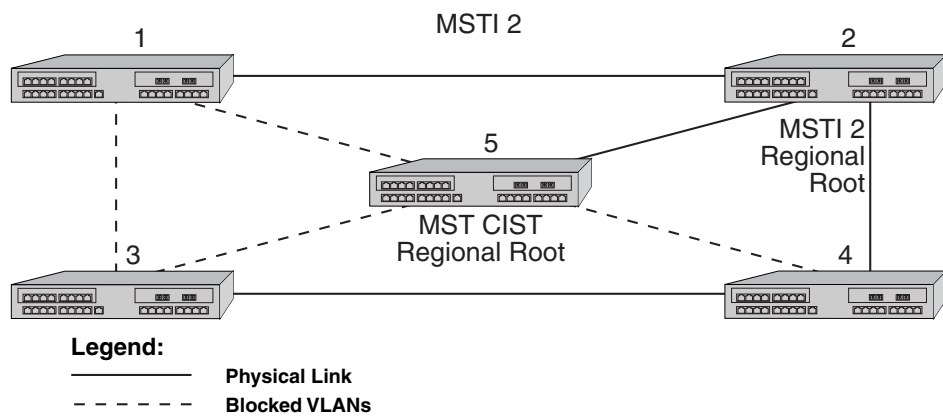


Figure 15-10 on page 15-19 shows 3 regions with five MSTIs. Table 15-5 on page 15-19 defines the characteristics of each MSTI. Ports connected to PCs from devices 1, 3, 9, and 11 will be automatically detected as edge ports. Devices 4 and 10 are the CIST regional roots. Each MSTI can be configured to forward and block various VLANs.



Figure 15-10 Example of Multiple Regions and MSTIs

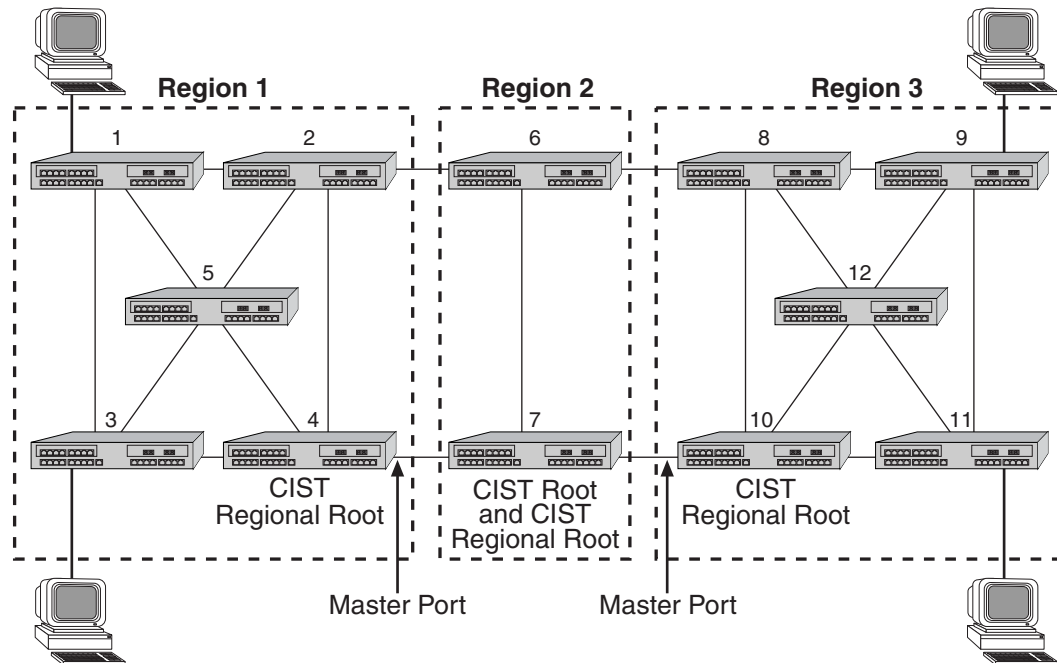


Table 15-5 MSTI Characteristics for Figure 15-10

| MSTI / Region      | Characteristics                                                  |
|--------------------|------------------------------------------------------------------|
| MSTI 1 in Region 1 | Root is switching device 4, which is also the CIST regional root |
| MSTI 2 in Region 1 | Root is switching device 5                                       |
| MSTI 1 in Region 2 | Root is switching device 7, which is also the CIST root          |
| MSTI 1 in Region 3 | Root is switching device 11                                      |
| MSTI 2 in Region 3 | Root is switching device 12                                      |
|                    | Switching device 10 is the CIST regional root                    |

## Configuring STP and RSTP



**Caution:** Spanning Tree configuration should be performed only by personnel who are very knowledgeable about Spanning Trees and the configuration of the Spanning Tree Algorithms. Otherwise, the proper operation of the network could be at risk.

| For information about...                             | Refer to page... |
|------------------------------------------------------|------------------|
| <a href="#">Reviewing and Enabling Spanning Tree</a> | 15-20            |
| <a href="#">Adjusting Spanning Tree Parameters</a>   | 15-20            |
| <a href="#">Enabling the Backup Root Function</a>    | 15-23            |
| <a href="#">Adjusting RSTP Parameters</a>            | 15-23            |

## Reviewing and Enabling Spanning Tree

By default, Spanning Tree is enabled globally on Enterasys switch devices and enabled on all ports. On all switching devices, the default Spanning Tree version is set to MSTP (802.1s) mode. Since MSTP mode is fully compatible and interoperable with legacy STP and RSTP bridges, in most networks, this default should not be changed.

Use the following commands to review, re-enable, and reset the Spanning Tree mode.

1. Review the current configuration on one or more SIDs, ports, or both:

```
show spantree stats [port port-string] [sid sid] [active]
```

Specifying **active** will display information for port(s) that have received BPDUs since boot.

2. If necessary, globally enable Spanning Tree:

```
set spantree stpmode ieee8021
```

3. Review the status of Spanning Tree on one or more ports:

```
show spantree portadmin [port port-string]
```

4. If necessary, re-enable Spanning Tree on one or more ports:

```
set spantree portadmin port-string enable
```

### Example

This example shows how to display the device's Spanning Tree configuration:

```
Enterasys->show spantree stats
SID - 1
Spanning tree mode - enabled
Designated Root - 00-e0-63-6c-9b-6d
Designated Root Priority - 0
Designated Root Cost - 1
Designated Root Port - ge.5.1
Root Max Age - 20 sec
Root Hello Time - 2 sec
Root Forward Delay - 15 sec
Bridge ID MAC Address - 00-e0-63-9d-b5-87
Bridge priority - 32768
Bridge Max Age - 20 sec
Bridge Hello Time - 2 sec
Bridge Forward Delay - 15 sec
Topology Change Count - 6539
Time Since Top Change - 00 days 00:00:00
```



**Note:** By default, Spanning Tree is enabled globally on stackable, and standalone fixed switch devices and enabled on all ports.

## Adjusting Spanning Tree Parameters

You may need to adjust certain Spanning Tree parameters if the default values are not suitable for your bridge configuration. Parameters affecting the entire Spanning Tree are configured with

variations of the global bridge configuration commands. Interface-specific parameters are configured with variations of the Spanning Tree port configuration commands. Default settings are listed in [Table 15-6](#):

**Table 15-6 Spanning Tree Port Default Settings**

| Setting                       | Default Value                                    |
|-------------------------------|--------------------------------------------------|
| Bridge priority mode          | 802.1t                                           |
| Bridge priority               | 32768                                            |
| Port priority                 | 128                                              |
| Port cost                     | 0 (automatically calculated based on port speed) |
| Hello time (bridge and ports) | 2 seconds                                        |
| Bridge forward delay          | 15 seconds                                       |
| Bridge maximum aging time     | 20 seconds                                       |

Use the commands in the following sections to adjust these defaults.



**Note:** Poorly chosen adjustments to these parameters can have a negative impact on network performance. Please refer to the IEEE 802.1D specification for guidance.

## Setting Bridge Priority Mode and Priority

Bridge priority mode affects the range of priority values used to determine which device is selected as the Spanning Tree root. By default, switching devices are set to 802.1t mode as described in “[Updated 802.1t](#)” on page 15-8.

Use this command to set the bridge priority mode:

```
set spantree bridgeprioritymode 802.1t | 802.1d
```

In addition to setting priority mode, you can globally configure the priority of an individual bridge. When two bridges tie for position as the root bridge, this setting affects the likelihood that a bridge will be selected. The lower the bridge’s priority, the more likely the bridge will be selected as the root bridge.

Use this command to set the bridge priority:

```
set spantree priority priority [sid]
```

Valid *priority* values are:

- For 802.1t priority mode: **0–61440** (in increments of 4096), with 0 indicating high priority and 61440 low priority. Values will automatically be rounded up or down, depending on the 802.1t value to which the entered value is closest.
- For 802.1D priority mode: **0–65535** (in increments of 1), with 0 indicating high priority and 65535 low priority.

Valid *sid* values are **0–4094**. If not specified, SID 0 will be assumed.

## Setting a Port Priority

You can set a Spanning Tree port priority. Port priority is used to break a tie when choosing the root port for a bridge, in a case where the choice is between ports connected to the same bridge. The port with the lowest value will be elected.

Use this command to set a port priority:

```
set spantree portpri port-string priority [sid sid]
```

Valid *priority* values are **0–240** (in increments of 16) with 0 indicating high priority.

Valid *sid* values are **0–4094**. If not specified, SID 0 will be assumed.

## Assigning Port Costs

Each interface has a Spanning Tree port cost associated with it, which helps to determine the quickest path between the root bridge and a specified destination. By convention, the higher the port speed, the lower the port cost. By default, this value is set to 0, which forces the port to recalculate Spanning Tree port cost based on the speed of the port and whether or not legacy (802.1D) path cost is enabled.

Use this command to assign different Spanning Tree port costs:

```
set spantree adminpathcost port-string cost [sid sid]
```

Valid *cost* values are:

- **0–65535** if legacy path cost is enabled.
- **0–200000000** if legacy path cost is disabled.

Valid *sid* values are **0–4094**. If not specified, SID 0 will be assumed.



**Notes:** Please refer to the IEEE 802.1D specification for guidance in setting appropriate cost values for your port speeds.

By default, legacy path cost is disabled. Enabling the device to calculate legacy path costs affects the range of valid values that can be administratively assigned.

To check the status of legacy path cost, use **show spantree legacypathcost**.

To disable legacy path cost, if necessary use **set spantree legacypathcost disable**.

## Adjusting Bridge Protocol Data Unit (BPDU) Intervals

Use the commands in this section to adjust default BPDU interval values.

**Table 15-7 BPDU Interval Defaults**

| BPDU Interval                 | Default Value |
|-------------------------------|---------------|
| Hello time (bridge and ports) | 2 seconds     |
| Forward delay                 | 15 seconds    |
| Maximum age time              | 20 seconds    |

### Adjusting the Bridge Hello Time



**Caution:** Poorly chosen adjustments to bridge and port hello time parameters can have a negative impact on network performance. It is recommended that you do not change these parameters unless you are familiar with Spanning Tree configuration and have determined that adjustments are necessary. Please refer to the IEEE 802.1D specification for guidance.

Hello time is the interval, in seconds, at which the bridge or individual ports send BPDU messages. By default, bridge hello mode is enabled, meaning the device uses a single bridge administrative hello time.

Adjust the bridge hello time as follows:

1. Check the current value of bridge hello time:

```
show spantree stats
```

2. Set a new hello time interval:

```
set spantree hello interval
```

Valid *interval* values are 1–10.

### Adjusting the Forward Delay Interval

When rapid transitioning is not possible, forward delay is used to synchronize BPDU forwarding. The forward delay interval is the amount of time spent listening for topology change information after an interface has been activated for bridging and before forwarding actually begins. This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state. Otherwise, temporary data loops might result.

Use this command to adjust the forward delay interval setting:

```
set spantree fwddelay delay
```

Valid *delay* values are 4–30.

### Defining the Maximum Age Time

If a bridge does not hear BPDUs from the root bridge within the interval (number of seconds) specified as maximum age time, it assumes that the network has changed and recomputes the Spanning Tree topology. By adjusting this value, you can configure support for a maximum diameter from the STP root of up to 40 bridges. By default, Enterasys switching devices are set with a maximum age time of 20 seconds, supporting a 20-bridge span from the root bridge.

Use this command to adjust the maximum age setting:

```
set spantree maxage agingtime
```

Valid *agingtime* values are 6–40 (seconds).

## Enabling the Backup Root Function

Disabled by default on stackable, and standalone fixed switch devices, the backup root function works only when the backup root-enabled bridge is directly connected to the root bridge. The backup root function prevents stale Spanning Tree information from circulating throughout the network in the event that the link between the root bridge and the backup root-enabled bridge is lost. If this happens, the backup root will dynamically lower its bridge priority relative to the existing root bridge's priority, causing it to immediately be selected as the new root bridge.

Use this command to enable the backup root function on an SID:

```
set spantree backuproot sid enable
```

When SNMP trap messaging is configured and the backup root function is enabled, a trap message will be generated when the backup becomes the new root of the network.

## Adjusting RSTP Parameters

Since rapid link reconfiguration can happen only on a point-to-point link or an edge port (a port that is known to be on the edge of a bridged LAN), in some cases you may want to define them administratively. However, since edge port and point-to-point links are automatically detected on Enterasys switching devices, in most cases you will not need to change these default port designations.

## Defining Edge Port Status

By default, edge port status is disabled on all ports. When enabled, this indicates that a port is on the edge of a bridged LAN. You can use the following commands to review and, if necessary, change the edge port detection status on the device and the edge port status of Spanning Tree ports.

Review and define edge port status as follows:

1. Display the status of edge port detection:

```
show spantree autoedge
```

2. If desired, enable edge port detection:

```
set spantree autoedge enable
```

3. Display the edge port operating status of one or more port(s):

```
show spantree operedge [port port-string]
```

A status of "true" or "Edge-Port" indicates the port is operating as an edge port.

A status of "false" or "Non-Edge-Port" indicates it is not.

If *port-string* is not specified, edge port status will be displayed for all Spanning Tree ports.

4. Display the edge port administrative status of one or more port(s):

```
show spantree adminedge [port port-string]
```

A status of "true" or "Edge-Port" indicates the port is administratively set to be considered an edge port.

A status of "false" or "Non-Edge-Port" indicates the port is administratively set to be considered a non edge port.

If *port-string* is not specified, edge port administrative status will be displayed for all Spanning Tree ports.

5. If necessary, change the edge port administrative status of one or more port(s):

```
set spantree adminedge port-string true
```

## Configuring MSTP

In order for MSTP to provide multiple forwarding paths, the following must happen:

- The configuration identifier must match on all bridges within the region.
- All bridges must be within the same region.
- All bridges must be connected to MSTP-aware bridges. (They can be connected using a shared media such as a repeater provided that a single Spanning Tree device does not reside on that LAN).



**Note:** A single Spanning Tree device between two MSTP bridges will terminate the ability to have multiple forwarding paths.

| For information about...                                                      | Refer to page... |
|-------------------------------------------------------------------------------|------------------|
| <a href="#">Example 1: Configuring MSTP for Traffic Segregation</a>           | 15-25            |
| <a href="#">Example 2: Configuring MSTP for Maximum Bandwidth Utilization</a> | 15-27            |
| <a href="#">Adjusting MSTP Parameters</a>                                     | 15-28            |

For information about...

Refer to page...

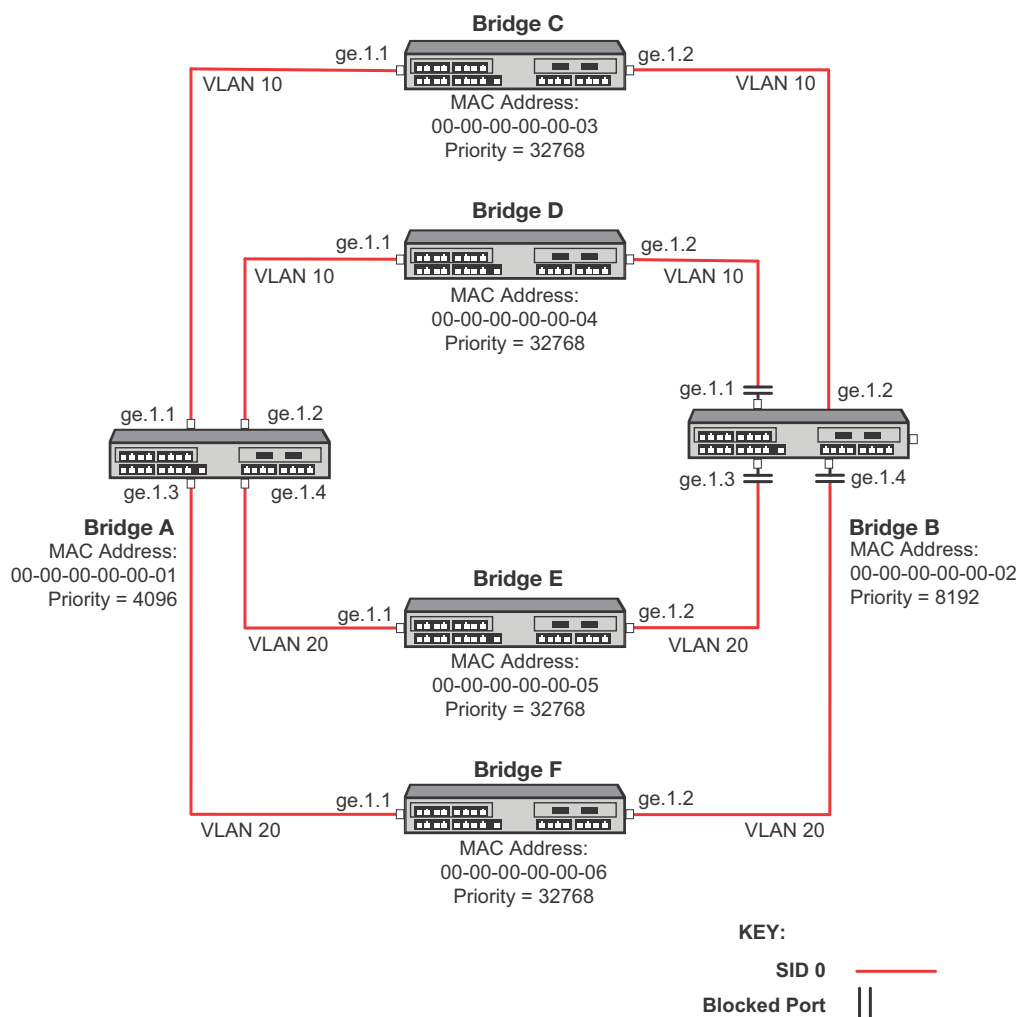
Monitoring MSTP

15-29

## Example 1: Configuring MSTP for Traffic Segregation

This example illustrates the use of MSTP for traffic segregation by VLAN and SID. Bridges A, B, C and D participate in VLAN 10. Bridges A, B, E and F participate in VLAN 20. [Figure 15-11](#) shows the problem that arises when using a single Spanning Tree configuration for traffic segregation with redundancy.

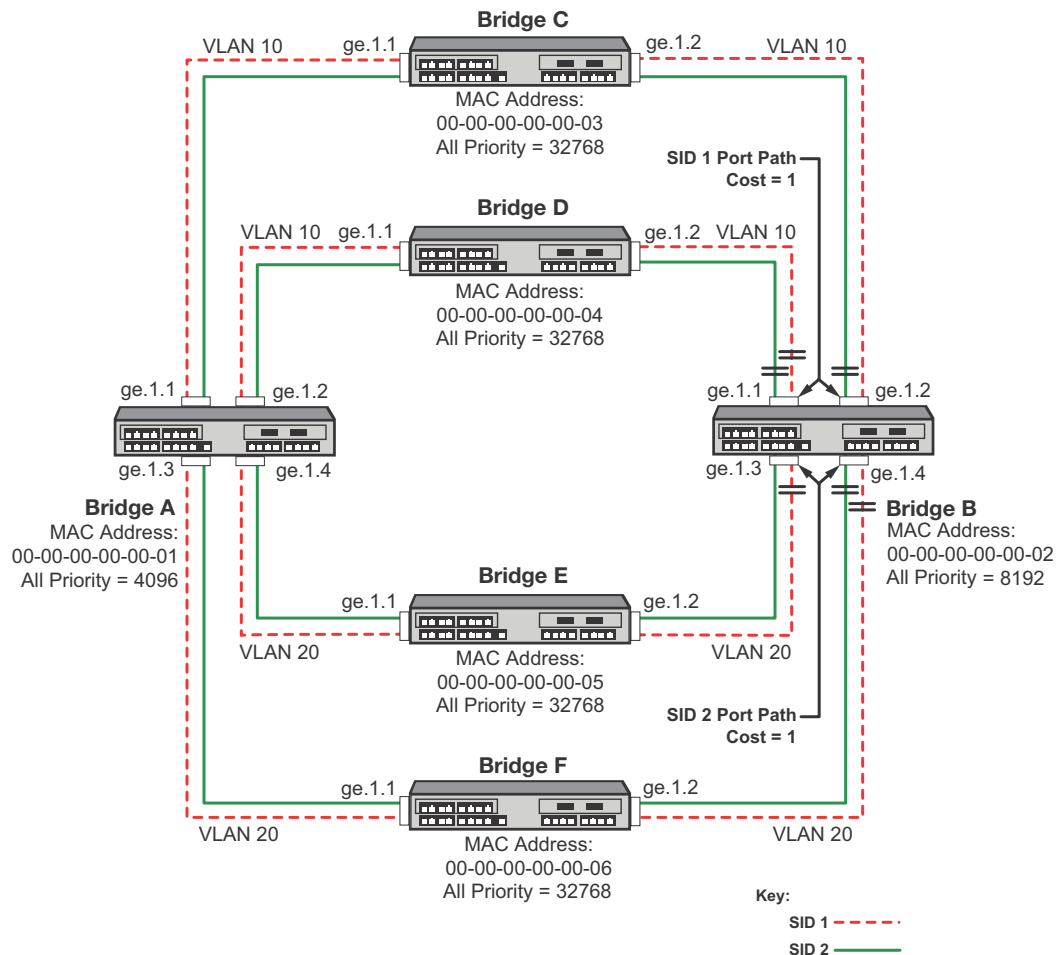
**Figure 15-11 Traffic Segregation in a Single STP Network Configuration**



In a single Spanning Tree configuration a bridge can only have one port forwarding towards the root for all traffic. Bridge A has the lowest priority and is the root. Bridge B forwards traffic towards the root on port ge.1.2. All other ports are blocked. For this configuration, Bridge B will not have any active links forwarding for VLAN 20.

[Figure 15-12](#) on page 15-26 shows the solution using MSTP. By configuring separate Spanning Tree instances to overlay the two VLAN topologies, Bridge B port ge.1.2 forwards on VLAN 10 for SID 1 and port ge.1.3 forwards on VLAN 20 for SID 2.

Figure 15-12 Traffic Segregation in an MSTP Network Configuration



o configure the traffic segregation MSTP example on all bridges:

- Configure the MST configuration ID with the same name  
`set spantree mstcfgid cfgname name`
- Create SIDs 1 and 2  
`set spantree msti sid sid create`
- Create the FID to SID mappings VLAN 10 to SID 1 and VLAN 20 to SID 2  
`set spantree mstmap vlan-id sid sid`

To configure Bridge A as root, set the priority to 4096 for both SID 1 and SID 2.

`set spantree priority priority sid`

To configure Bridge B as the backup should Bridge A fail:

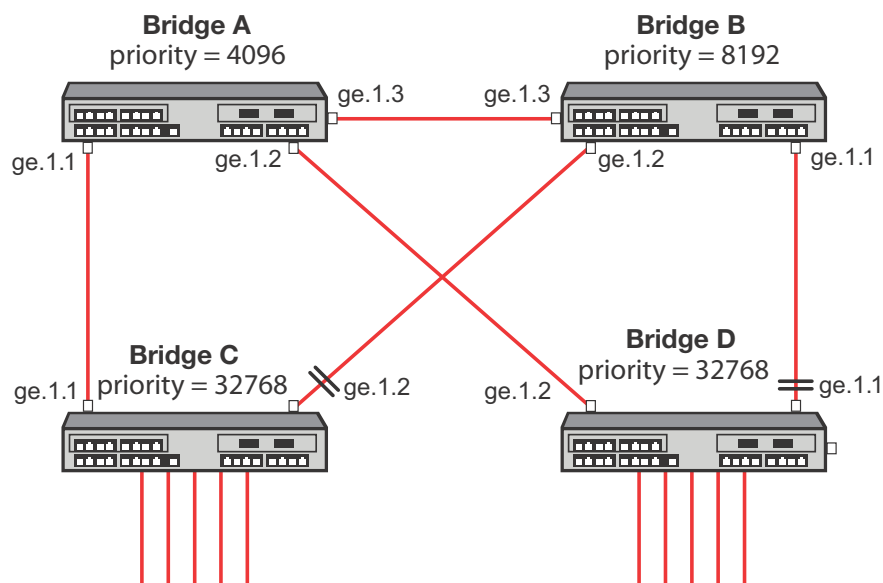
- Set the Spanning Tree priority to 8192 for both SID 1 and SID 2  
`set spantree priority priority sid`
- Set the admin path cost on ports ge.1.1-2 to 1 for SID 1
- Set the admin path cost on ports ge.1.3-4 to 1 for SID 2  
`set spantree adminpathcost port-id cost sid`



## Example 2: Configuring MSTP for Maximum Bandwidth Utilization

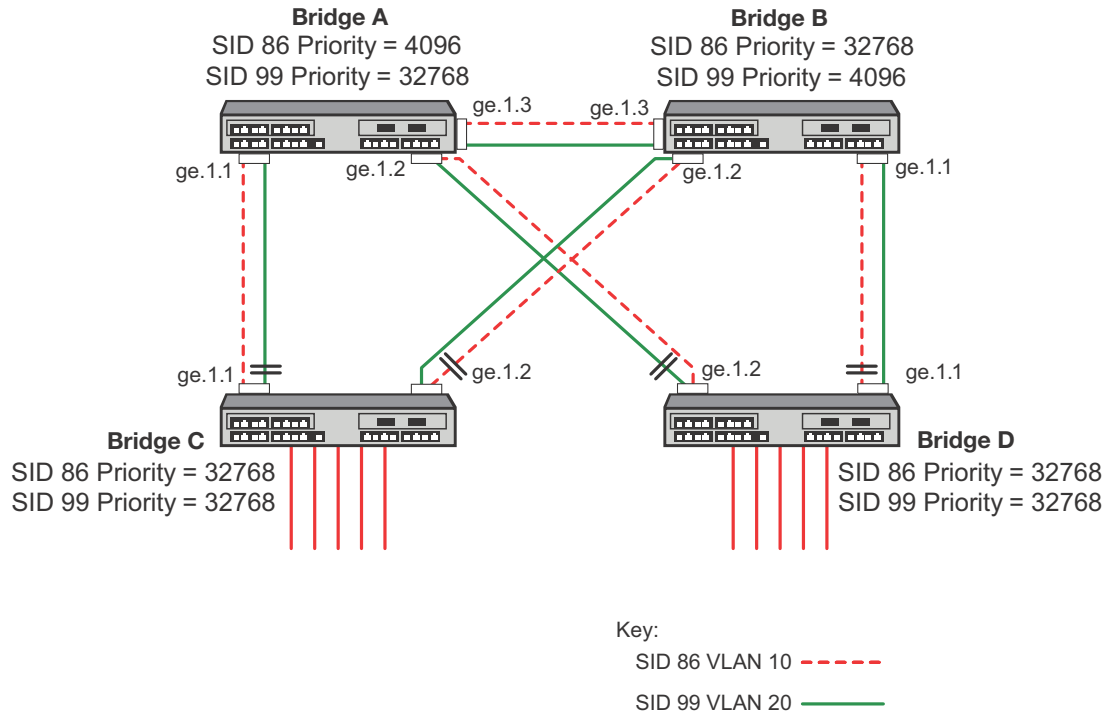
This example illustrates the use of MSTP for maximum bandwidth utilization. Maximum bandwidth utilization takes place when all bridges participate on all VLANs. [Figure 15-13](#) shows that with a single Spanning Tree configuration, only a single link towards the root forwards on a bridge. The alternate ports are blocking.

**Figure 15-13** Maximum Bandwidth Utilization in a Single STP Network Configuration



In [Figure 15-13](#), Bridge A is the root of the Spanning Tree because it has the lowest priority. Bridge D port ge.1.2 forwards traffic to Bridge A. Bridge D port ge.1.1 is blocking. Bridge C port ge.1.1 forwards traffic to Bridge A. Bridge C port ge.1.2 is blocking. This single Spanning Tree configuration prevents maximum bandwidth utilization for this network.

[Figure 15-14](#) on page 15-28 shows that with an MSTP configuration each link can be forwarding for some VLAN and each VLAN has a path to the root bridge.

**Figure 15-14 Maximum Bandwidth in an MSTP Network Configuration**

To configure the MSTP maximum bandwidth utilization example on all bridges:

- Create VLANs 10 and 20
 

```
set vlan create vlan-id
```
- Configure the MST configuration ID with the same name
 

```
set spantree mstcfgid cfgname name
```
- Create SIDs 86 and 99
 

```
set spantree msti sid sid create
```
- Create the FID to SID mappings VLAN 10 to SID 86 and VLAN 20 to SID 99
 

```
set spantree mstmap vlan-id sid sid
```

Additionally, the root of each SID is chosen to be in a different bridge. This will spread out the traffic. The bridges on the next level down have a link to each of the root bridges.

To configure Bridge A as root for SID 86, set the priority to 4096 for SID 86.

```
set spantree priority priority sid
```

To configure Bridge B as the root for SID 99, set the priority to 4096 for SID 99.

## Adjusting MSTP Parameters

You may need to adjust certain Spanning Tree parameters if the default values are not suitable for your bridge configuration. Refer back to [“Adjusting Spanning Tree Parameters”](#) on page 15-20 and [“Adjusting RSTP Parameters”](#) on page 15-23 for information on adjusting Spanning Tree defaults. Changes made to global and port-related Spanning Tree defaults will take affect if the device is running in STP, RSTP, or MSTP.

## Monitoring MSTP

Use the commands in [Table 15-8](#) to monitor MSTP statistics and configurations on stackable, and standalone switch devices. You can also use the show commands described in [“Reviewing and Enabling Spanning Tree”](#) on page 15-20 to review information related to all Spanning Tree protocol activity.

**Table 15-8 Commands for Monitoring MSTP**

| Task                                                                                                                                                          | Command                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| Verify that MSTP is running on the device.                                                                                                                    | <code>show spantree version</code>                                     |
| Display a list of MSTIs configured on the device.                                                                                                             | <code>show spantree mstlist</code>                                     |
| Display the mapping of one or more filtering database IDs (FIDs) to Spanning Trees. Since VLANs are mapped to FIDs, this shows to which SID a VLAN is mapped. | <code>show spantree mstmap [fid fid]</code>                            |
| Display the Spanning Tree ID(s) assigned to one or more VLANs.                                                                                                | <code>show spantree vlanlist [vlan-list]</code>                        |
| Display MST configuration identifier elements, including format selector, configuration name, revision level, and configuration digest.                       | <code>show spantree mstcfgid</code>                                    |
| Display protocol-specific MSTP counter information.                                                                                                           | <code>show spantree debug [port port-string] [sid sid] [active]</code> |

## Understanding and Configuring SpanGuard

| For information about...              | Refer to page...      |
|---------------------------------------|-----------------------|
| <a href="#">What Is SpanGuard?</a>    | <a href="#">15-29</a> |
| <a href="#">How Does It Operate?</a>  | <a href="#">15-31</a> |
| <a href="#">Configuring SpanGuard</a> | <a href="#">15-30</a> |

### What Is SpanGuard?

As described previously in the overview of [“SpanGuard”](#) on page 15-7, this feature enables Enterasys switching devices to detect unauthorized bridges in your network, resolving the threat of repeated topology change notifications or new root bridge announcements causing a Denial of Service (DoS) condition. It prevents Spanning Tree respans that can occur when BPDUs are received on user ports and notifies you (network management) they were attempted.

If a SpanGuard enabled port receives a BPDU, it becomes locked and transitions to the blocking state. It will only transition out of the blocking state after a globally specified time or when it is manually unlocked.

By default, SpanGuard is globally disabled on stackable, and standalone switch devices and must be globally enabled to operate on all user ports. For configuration information, refer to [“Configuring SpanGuard”](#) on page 15-30.

## How Does It Operate?

SpanGuard helps protect against Spanning Tree Denial of Service (DoS) SpanGuard attacks as well as unintentional or unauthorized connected bridges, by intercepting received BPDUs on configured ports and locking these ports so they do not process any received packets.

When enabled, reception of a BPDU on a port that is administratively configured as a Spanning Tree edge port (`admedge = True`) will cause the port to become locked and the state set to blocking. When this condition is met, packets received on that port will not be processed for a specified timeout period. The port will become unlocked when:

- the timeout expires,
- the port is manually unlocked,
- the port is no longer administratively configured as `admedge = True`, or
- the SpanGuard function is disabled.

The port will become locked again if it receives another offending BPDU after the timeout expires or it is manually unlocked.

In the event of a DoS attack with SpanGuard enabled and configured, no Spanning Tree topology changes or topology reconfigurations will be seen in your network. The state of your Spanning Tree will be completely unaffected by the reception of any spoofed BPDUs, regardless of the BPDU type, rate received or duration of the attack.

By default, when SNMP and SpanGuard are enabled, a trap message will be generated when SpanGuard detects that an unauthorized port has tried to join a Spanning Tree.

## Configuring SpanGuard

Use the following commands to configure device ports for SpanGuard, to enable the SpanGuard function, and to review SpanGuard status on the device.

### Reviewing and Setting Edge Port Status



**Note:** To use the SpanGuard function, you must know which ports are connected between switching devices as ISLs (inter-switch links). Also, you must configure edge port status (`admedge = true` or `false`) on the entire switch, as described in [“Defining Edge Port Status”](#) on page 15-24, before SpanGuard will work properly.

Review and set edge port status as follows:

1. Use the show commands described in [“Defining Edge Port Status”](#) on page 15-24 to determine edge port administrative status on the device.
2. Set edge port administrative status to `false` on all known ISLs.
3. Set edge port administrative status to `true` on any remaining ports where SpanGuard protection is desired. This indicates to SpanGuard that these ports are not expecting to receive any BPDUs. If these ports do receive BPDUs, they will become locked.

### Enabling and Adjusting SpanGuard

Use this command to enable SpanGuard on the device:

```
set spantree spanguard enable
```

Use this command to adjust the SpanGuard timeout value. This sets the length of time that a SpanGuard-affected port will remain locked:

```
set spantree spanguardtimeout timeout
```

Valid values are 0–65535 seconds. Default is 300 seconds. Setting the value to 0 will set the timeout to forever.

Use this command to manually unlock a port that was locked by the SpanGuard function. This overrides the specified timeout variable:

```
set spantree spanguardlock port-string
```

## Monitoring SpanGuard Status and Settings

Use the commands in [Table 15-9](#) to review SpanGuard status and settings.

**Table 15-9 Commands for Monitoring SpanGuard**

| Task                                                                    | Command                                                            |
|-------------------------------------------------------------------------|--------------------------------------------------------------------|
| Display the status of SpanGuard on the device.                          | <code>show spantree spanguard</code>                               |
| Display the status of the SpanGuard lock function on one or more ports. | <code>show spantree spanguardlock [port <i>port-string</i>]</code> |
| Display the SpanGuard timeout setting.                                  | <code>show spantree spanguardtimeout</code>                        |
| Display the status of the SpanGuard trap function.                      | <code>show spantree spanguardtrapeenable</code>                    |

## Understanding and Configuring Loop Protect

| For information about...                 | Refer to page... |
|------------------------------------------|------------------|
| <a href="#">What Is Loop Protect?</a>    | 15-31            |
| <a href="#">How Does It Operate?</a>     | 15-31            |
| <a href="#">Configuring Loop Protect</a> | 15-33            |

### What Is Loop Protect?

As described previously in the overview of “[Loop Protect](#)” on page 15-7, this feature prevents or short circuits loop formation in your network. It does this by requiring ports to receive type 2 BPDUs (RSTP/MSTP) on point-to-point inter-switch links (ISLs) before their states are allowed to become forwarding. Further, if a BPDU timeout occurs on a port, its state becomes non-forwarding until a BPDU is received.

In this way, both upstream and downstream facing ports are protected. When a root or alternate port loses its path to the root bridge due to a message age expiration, it takes on the role of designated port and will not forward traffic until a BPDU is received.

When a port is intended to be the designated port in an ISL, it constantly proposes and will not forward until a BPDU is received. This protects against misconfiguration and protocol failure by the connected bridge.

### How Does It Operate?

Loop Protect operates as a per port, per MST instance feature and should be set on ISLs. It comprises several related functions, including:

- Controlling port forwarding state based on reception of agreement BPDUs
- Controlling port forwarding state based on reception of disputed BPDUs

- Communicating port non-forwarding status through traps and syslog messages
- Disabling a port based on frequency of failure events

## Port Modes and Event Triggers

Ports work in two Loop Protect operational modes. If the port is configured so that it is connected to a switching device known to implement Loop Protect, it uses full functional (enhanced) mode. Otherwise, it operates in limited functional (standard) mode.

Connection to a Loop Protect switching device guarantees that the alternate agreement mechanism is implemented and, therefore, the designated port can rely on receiving a response to its proposal regardless of the role of the connected port. This has two important implications. First, the designated port connected to a non-root port may transition to forwarding. Second, there is no ambiguity when a timeout happens; a Loop Protect event has occurred.

In full mode, when a type 2 BPDU is received and the port is designated and point-to-point, the timer is set to 3 times hello time. Limited mode adds a further requirement that the flags field in the BPDU indicates a root role. If the port is a boundary port, the MSTIs for that port follow the CIST (for example if the MSTI port timers are set according to the CIST port timer). If the port is internal to the region, the MSTI port timers are set independently using the particular MSTI message.

Loop Protect initializes the MSTI timer to zero and does not allow the designated port to transition from listening to learning until the timer becomes non-zero. If the port is not designated, the timer does not apply. Its state is controlled through normal protocol behavior.

A disputed BPDU is one in which the flags field indicates a designated role, a learning state, and the priority vector is worse than that already held by the port. If a disputed BPDU is received, the port is forced to the listening state.

Message age expiration and the expiration of the Loop Protect timer are both events for which Loop Protect generates a notice level syslog message. You can also configure traps to report these events, as well as a syslog message and trap for disputed BPDUs.

In addition, you can configure Loop Protect to force the locking of an SID/port when one or more events occur. When the configured number of events happen within a given window of time, the port will be forced into blocking and held there until you manually unlock it.

## Example: Basic Loop Protect Configuration

The following sample configuration shows how Loop Protect functions in a basic Spanning Tree topology.

In the example in [Figure 15-15](#) on page 15-33, Switch 1 is the root bridge with BPDUs being sent to both Switch 2 and 3. (Designated ports are labeled D and root ports are labeled R.) Switch 3 has placed the port that connects to Switch 2 in a blocking state.

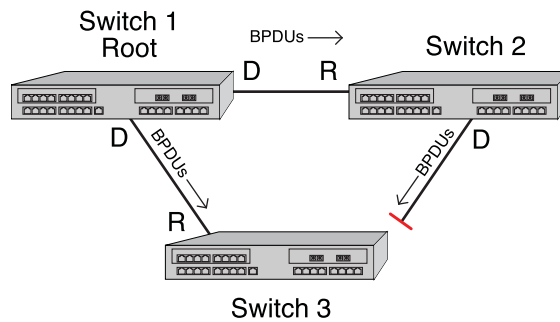
**Figure 15-15 Basic Loop Protect Scenario**

Figure 15-16 shows that, without Loop Protect, a failure could be as simple as someone accidentally disabling Spanning Tree on the port between Switch 2 and 3. Switch 3's blocking port eventually transitions to a forwarding state which leads to a looped condition.

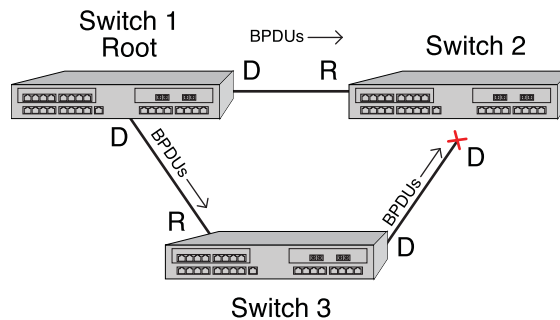
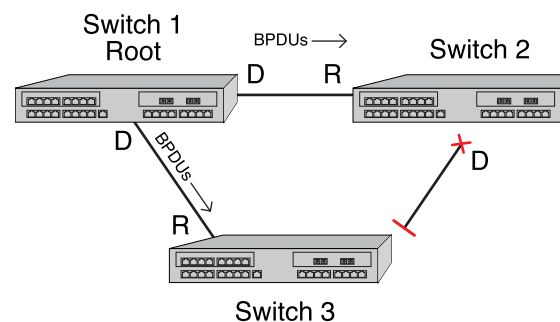
**Figure 15-16 Spanning Tree Without Loop Protect**

Figure 15-17 shows that, with Loop Protect enabled, Switch 3 will not go to a forwarding state until it has received a BPDU from Switch 2.

**Figure 15-17 Spanning Tree with Loop Protect**

## Configuring Loop Protect

| For information about...                           | Refer to page... |
|----------------------------------------------------|------------------|
| <a href="#">Enabling or Disabling Loop Protect</a> | 15-34            |
| <a href="#">Specifying Loop Protect Partners</a>   | 15-34            |

| For information about...                                               | Refer to page... |
|------------------------------------------------------------------------|------------------|
| <a href="#">Setting the Loop Protect Event Threshold and Window</a>    | 15-34            |
| <a href="#">Enabling or Disabling Loop Protect Event Notifications</a> | 15-35            |
| <a href="#">Setting the Disputed BPDUs Threshold</a>                   | 15-35            |
| <a href="#">Monitoring Loop Protect Status and Settings</a>            | 15-35            |

## Enabling or Disabling Loop Protect

By default, Loop Protect is disabled on all ports. Use this command to enable (or, if desired, disable) the feature on one or more ports:

```
set spantree lp port-string {enable | disable} [sid sid]
```

If no SID is specified, SID 0 is assumed.

This command takes precedence over per port STP enable/disable state (portAdmin). Normally, portAdmin disabled would cause a port to go immediately to forwarding. If Loop Protect is enabled, that port should go to listening and remain there.



**Note:** The Loop Protect enable/disable settings for an MSTI port should match those for the CIST port.

## Specifying Loop Protect Partners

By default, each port is not set as a Loop Protect capable partner. If the port is set as a Loop Protect capable partner (true), the full functionality of the Loop Protect feature is used. If the value is false, then there is some ambiguity as to whether an Active Partner timeout is due to a loop protection event or is a normal situation due to the fact that the partner port does not transmit Alternate Agreement BPDUs. Therefore, a conservative approach is taken in that designated ports will not be allowed to forward unless receiving agreements from a port with root role. This type of timeout will not be considered a loop protection event. Loop protection is maintained by keeping the port from forwarding, but since this is not considered a loop event, it will not be factored into locking the port.

Use this command to set the Loop Protect partner state on one or more ports:

```
set spantree lpcapablepartner port-string {true | false}
```

## Setting the Loop Protect Event Threshold and Window

The Loop Protect event threshold is a global integer variable that provides protection in the case of intermittent failures. The default value is 3. If the event counter reaches the threshold within a given period (the event window), the port for the given SID becomes locked (that is, held indefinitely in the blocking state). If the threshold is 0, the ports are never locked.

Use this command to set the Loop Protect event threshold:

```
set spantree lpthreshold value
```

The Loop Protect window is a timer value, in seconds, that defines a period during which Loop Protect events are counted. The default value is 180 seconds. If the timer is set to 0, the event counter is not reset until the Loop Protect event threshold is reached.

Use this command to set the Loop Protect event window value in seconds:

```
set spantree lpwindow value
```



## Enabling or Disabling Loop Protect Event Notifications

Loop Protect traps are sent when a Loop Protect event occurs, that is, when a port goes to listening due to not receiving BPDUs. The trap indicates port, SID and loop protection status.

Use this command to enable or disable Loop Protect event notification. By default, this is disabled:

```
set spantree lptrapenable {enable / disable}
```

## Setting the Disputed BPDUs Threshold

A disputed BPDU is one in which the flags field indicates a designated role and a learning state, and the priority vector is worse than that already held by the port. If a disputed BPDU is received, the port is forced to the listening state. Refer to the 802.1Q-2005 standard, *IEEE Standard for Local and Metropolitan Area Networks – Virtual Bridged Local Area Networks*, for a full description of the dispute mechanism, which prevents looping in cases of one-way communication.

The disputed BPDU threshold is an integer variable that represents the number of disputed BPDUs that must be received on a given port and SID before a disputed BPDU trap is sent and a syslog message is issued. For example, if the threshold is 10, a trap is issued when 10, 20, 30 (and so on) disputed BPDUs have been received. The trap indicates port, SID and total Disputed BPDU count.

Use this command to set the disputed BPDU threshold:

```
set spantree disputedbpduthreshold value
```

Default value is 0, which means that traps are not sent.

## Monitoring Loop Protect Status and Settings

Use the commands in [Table 15-10](#) to monitor Loop Protect settings.

**Table 15-10** Commands for Monitoring Loop Protect

| Task                                                                                                                                                                                                                                                                                                                                        | Command                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Display the Loop Protect status per port, per SID, or both.                                                                                                                                                                                                                                                                                 | <b>show spantree lp</b> [port <i>port-string</i> ] [sid <i>sid</i> ]                  |
| Display the Loop Protect lock status per port, per SID, or both.<br><b>Note:</b> A port can become locked if a configured number of Loop Protect events occur during the configured window of time. Once a port is forced into blocking (locked), it remains locked until manually unlocked with the <b>clear spantree lpllock</b> command. | <b>show spantree lpllock</b> [port <i>port-string</i> ] [sid <i>sid</i> ]             |
| Display the Loop Protect capability of a link partner for one or more ports.                                                                                                                                                                                                                                                                | <b>show spantree lpcapablepartner</b> [port <i>port-string</i> ]                      |
| Display the reason for placing a port in a non-forwarding state due to an exceptional condition.                                                                                                                                                                                                                                            | <b>show spantree nonforwardingreason</b> [port <i>port-string</i> ] [sid <i>sid</i> ] |

### Example

The following example shows a switching device with Loop Protect enabled on port lag.0.2, SID 56:

```
Enterasys->show spantree lp port lag.0.2 sid 56
 LoopProtect is enabled on port lag.0.2, SID 56
Enterasys->show spantree lpllock port lag.0.2 sid 56
```

```

LoopProtect Lock status for port lag.0.2, SID 56_ is UNLOCKED
Enterasys->show spantree lpcapablepartner port lag.0.2
Link partner of port lag.0.2_is LoopProtect-capable.
Enterasys->show spantree nonforwardingreason port lag.0.2
Port lag.0.2 has been placed in listening or blocking state on SID 0 by the
LoopProtect feature.

```

## Terms and Definitions

Table 15-11 lists terms and definitions used in Spanning Tree configuration.

**Table 15-11 Spanning Tree Terms and Definitions**

| Term            | Definition                                                                                                                                                                                                                                                 |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alternate port  | Acts as an alternate path to the root bridge than that provided by the <a href="#">root port</a> .                                                                                                                                                         |
| Backup port     | Acts as an backup for the path provided by a designated port toward the leaves of the Spanning Tree. Backup ports can exist only where two ports are connected together in a loopback mode or bridge with two or more connections to a shared LAN segment. |
| BID             | Bridge identification, which is derived from the bridge's MAC address and bridge priority. The bridge with the lowest BID becomes the root bridge.                                                                                                         |
| BPDU            | Bridge Protocol Data Unit messages. Used by STP to exchange information, including designating a bridge for each switched LAN segment, and one root bridge for the Spanning Tree.                                                                          |
| Bridge          | Switching device.                                                                                                                                                                                                                                          |
| Bridge priority | Assigns the bridge's relative priority compared to other bridges.                                                                                                                                                                                          |
| CIST            | Common and Internal Spanning Tree created by MSTP to represent the connectivity of the entire network. This is equivalent to the single Spanning Tree used for STP and RSTP. Communications between MST regions occurs using the CIST.                     |
| CST             | A Spanning Tree defined in the IEEE 802.1q standard that assumes one Spanning Tree instance for the entire bridged network, regardless of the number of VLANs.                                                                                             |
| Designated port | A forwarding port within an active topology elected for every switched LAN segment.                                                                                                                                                                        |
| Edge port       | Port on the edge of a bridged LAN.                                                                                                                                                                                                                         |
| FID             | Filter Identifier. Each VLAN is associated to a FID. VLANs are mapped to SIDs using their FID association.                                                                                                                                                 |
| Forward delay   | Time interval (in seconds) the bridge spends in listening or learning mode before it begins forwarding BPDUs.                                                                                                                                              |
| Hello time      | Time interval (in seconds) at which the bridge sends BPDUs.                                                                                                                                                                                                |
| ISL             | Inter-Switch Link.                                                                                                                                                                                                                                         |
| IST             | A Spanning Tree instance that extends the CST inside the MST region and represents the entire MST region as a single CST virtual bridge to the outside world.                                                                                              |
| Loop Protect    | Prevents or short circuits loop formation in a network with redundant paths by requiring ports to receive type 2 BPDUs (RSTP/MSTP) on point-to-point inter-switch links (ISLs) before their states are allowed to become forwarding.                       |
| Master port     | The MSTI port whose connecting CIST port is root port for an entire MST region.                                                                                                                                                                            |

**Table 15-11 Spanning Tree Terms and Definitions (continued)**

| Term          | Definition                                                                                                                                                                                                                                                                  |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Max age       | Maximum time (in seconds) the bridge can wait without receiving a configuration message (bridge “hello”) before attempting to reconfigure.                                                                                                                                  |
| MST region    | An MSTP group of devices configured together to form a logical region. The MST region presents itself to the rest of the network as a single device, which simplifies administration.                                                                                       |
| MSTI          | Multiple Spanning Tree Instance. See <a href="#">Table 15-4</a> on page 15-16 for MSTI support per platform.                                                                                                                                                                |
| Path cost     | Sum of the port costs in the best path to the root bridge.                                                                                                                                                                                                                  |
| Port cost     | Value assigned to a port based on the speed of the port. The faster the speed, the lower the cost. This helps to determine the quickest path between the root bridge and a specified destination. The segment attached to the root bridge normally has a path cost of zero. |
| Port priority | Assigns a port’s priority in relation to the other ports on the same bridge.                                                                                                                                                                                                |
| Root bridge   | Logical center of the Spanning Tree, used by STP to determine which paths to block and which to open.                                                                                                                                                                       |
| Root port     | Port in an active topology through which the root bridge can be reached.                                                                                                                                                                                                    |
| SID           | Spanning tree identifier. By default, SID 0 is assumed. VLANs are mapped to SIDs using their FID association.                                                                                                                                                               |
| SpanGuard     | Prevents Spanning Tree respans that can occur when BPDUs are received on user ports and notifies network management that they were attempted.                                                                                                                               |



## Configuring Policy

This chapter provides an overview of Enterasys policy operation, describes policy terminology, and explains how to configure policy on Fixed Switch platforms using the CLI. However, Enterasys Networks strongly recommends that you use NetSight Policy Manager, not CLI commands, to configure policy in your network.

| For information about...                      | Refer to page... |
|-----------------------------------------------|------------------|
| <a href="#">Using Policy in Your Network</a>  | 16-1             |
| <a href="#">Policy Configuration Overview</a> | 16-2             |
| <a href="#">Configuring Policy</a>            | 16-9             |
| <a href="#">Policy Configuration Example</a>  | 16-12            |
| <a href="#">Terms and Definitions</a>         | 16-18            |

### Using Policy in Your Network

Policy is a component of Secure Networks that provides for the configuration of role-based profiles for securing and provisioning network resources based upon the role the user or device plays within the enterprise. By first defining the user or device role, network resources can be tailored to a specific user, system, service, or port-based context by configuring and assigning rules to the policy role. On the Fixed Switches, a policy role can be configured for any combination of Class of Service, VLAN assignment, or default behavior based upon L2, L3, and L4 packet fields.

The three primary benefits of using Enterasys Secure Networks policy in your network are provisioning and control of network resources, security, and centralized operational efficiency using the Enterasys NetSight Policy Manager.

Policy provides for the provisioning and control of network resources by creating policy roles that allow you to determine network provisioning and control at the appropriate network layer, for a given user or device. With a role defined, rules can be created based upon traffic classification types for traffic drop or forwarding. A Class of Service (CoS) can be associated with each role for purposes of setting priority, flood control, and rate limiting.

Security can be enhanced by allowing only intended users and devices access to network protocols and capabilities. Some examples are:

- Ensuring that only approved stations can use SNMP, preventing unauthorized stations from viewing, reading, and writing network management information.
- Preventing edge clients from spoofing network services that are appropriately restricted to data centers and managed by the enterprise IT organization — services such as DHCP and DNS.

- Identifying and restricting routing to legitimate routing IP addresses to prevent DoS, spoofing, data integrity and other routing related security issues.
- Ensuring that FTP/TFTP file transfers and firmware upgrades only originate from authorized file and configuration management servers.
- Preventing clients from using legacy protocols such as IPX, Apple Talk, and DECnet that should no longer be running on your network.

Enterasys NetSight Policy Manager provides a centralized point and click configuration, and one click pushing of defined policies out to all network elements. Use the Enterasys NetSight Policy Manager for ease of initial configuration and faster response to security and provisioning issues that may come up during real-time network operation.

## Standard and Enhanced Policy on Enterasys Platforms

There are two sets of policy capabilities supported on Enterasys switching platforms. Standard policy represents the base policy features supported on all Enterasys platforms. Enhanced policy is an additional set of policy capabilities supported only on the modular switch platforms which use custom switches ASICs designed by Enterasys. These modular switches include the N-Series, S-Series, and K-Series product lines.

The Fixed Switch product lines, which use commercially available switching ASICs, support only standard policy capabilities. Since this document describes how to configure the Fixed Switch products, only standard policy capabilities are discussed.

For information about enhanced policy capabilities, refer to the NetSight Policy Manager online help, the *Configuring Policy Feature Guide*, or the modular switch *Configuration Guides*.

## Implementing Policy

To implement policy:

- Identify the roles of users and devices in your organization that access the network
- Create a policy role for each identified user role
- Associate classification rules with each policy role
- Optionally, configure class of service and associate it directly with policy profiles and/or rules
- Apply policies, either statically or dynamically

## Policy Configuration Overview

This section provides an overview of policy configuration. Policy is implemented on an Enterasys platform by associating users and devices in the network with defined enterprise roles (such as sales, engineering, or administration) that are configured in a policy role. The policy role is associated with rules that define how network resources will be provisioned and controlled for role members, as well as how security will be applied to the role member.

## Using the Enterasys NetSight Policy Manager

Enterasys NetSight Policy Manager is a management GUI that automates the definition and enforcement of network-wide policy profiles and rules. It eliminates the need to configure policies on a device-by-device basis using complex CLI commands. The Policy Manager's GUI simplifies rule and policy role creation. You only define policies once using a point and click GUI— and

regardless of the number of moves, adds, or changes to the policy role, Policy Manager automatically enforces roles on Enterasys security-enabled infrastructure devices.

This document presents policy configuration from the perspective of the Fixed Switch CLI. Though it is possible to configure policy from the CLI, CLI policy configuration in even a small network can be prohibitively complex from an operational point of view. It is highly recommended that policy configuration be performed using the NetSight Policy Manager. The NetSight Policy Manager provides:

- Ease of rule and policy role creation
- The ability to store and retrieve roles and policies
- The ability, with a single click, to enforce policy across multiple devices

The official Policy Manager documentation is accessed using online help from within the application. This online documentation completely covers the configuration of policy in a Policy Manager context. For access to the Policy Manager data sheet or to setup a demo of the product, see <http://www.enterasys.com/products/visibility-control/netsight-policy-manager.aspx>.

## Understanding Roles in a Secure Network

The capacity to define roles is directly derived from the ability of supported Enterasys devices to inspect Layer 2, Layer 3, and Layer 4 packet fields while maintaining line rate. This capability allows for the granular application of a policy. On the Fixed Switches, you can apply a policy to a:

- Specific user (MAC source address)
- Port

Because users, devices, and applications are all identifiable, a network administrator has the capacity to define and control network access and usage by the actual role the user or device plays in the network. The nature of the security challenge, application access, or amount of network resource required by a given attached user or device, is very much dependent upon the “role” that user or device plays in the enterprise. Defining and applying each role assures that network access and resource usage align with the security requirements, network capabilities, and legitimate user needs as defined by the network administrator.

### The Policy Role

A role, such as sales, admin, or engineering, is first identified and defined in the abstract as the basis for configuring a policy role. Once a role is defined, a policy role is configured and applied to the appropriate context using a set of rules that can control and prioritize various types of network traffic. The rules that make up a policy role contain both classification definitions and actions to be enforced when a classification is matched. Classifications include Layer 2, Layer 3, and Layer 4 packet fields. Policy actions that can be enforced include VLAN assignment, filtering, inbound rate limiting, L2 priority, and ToS/DSCP.

## Defining Policy Roles

The policy role is a container that holds all aspects of policy configuration for a specific role. Policy roles are identified by a numeric profile-index value between 1 and the maximum number of roles supported on the platform. Please see your device’s firmware release notes for the maximum number of roles supported. On the Fixed Switches, policy roles are configured using the **set policy profile** command.

A policy role can also be identified by a text name of between 1 and 64 characters. This name value is used by the RADIUS Filter-ID attribute to identify the policy role to be applied by the switch with a successful authentication.

The following example creates a policy profile with a profile-index value of 1 and a profile name, **student**, that can be used by the RADIUS Filter-ID functionality:

```
System(rw)->set policy profile 1 name student
```

## Setting a Default VLAN for a Role

A default VLAN can be configured for a policy role. The policy VLAN will always be used unless an Ether type-to-VLAN classification rule exists and is hit.

To configure a default VLAN, using the **set policy profile** command, enable port VLAN ID (PVID) override with the **pvid-status** parameter, and specify the VLAN to be used for the role. Port VLAN ID override is disabled by default.



**Note:** Enterasys supports the assignment of port VLAN-IDs 1 - 4094. VLAN-IDs 0 and 4095 can not be assigned as port VLAN-IDs, but do have special meanings within a policy context and can be assigned to the **pvid** parameter. Within a policy context:

- **0** - Specifies deny all traffic
- **4095** - Specifies permit all traffic

The following example creates a policy profile with a profile-index value of 1, enables port VLAN ID overwrite, and associates with it a default VLAN with an ID value of 2.

```
System(rw)->set policy profile 1 pvid-status enable pvid 2
```

## Adding Tagged, Untagged, and Forbidden Ports to the VLAN Egress Lists

The VLAN egress list contains a list of ports that a frame for this VLAN can exit. Specified ports are assigned to the VLAN egress list for this policy role as tagged, untagged, or forbidden. Ports are added to the VLAN egress list using the **egress-vlans**, **forbidden-vlans**, and **untagged-vlans** options of the **set policy profile** command.

The following example creates a policy profile named “Engr” with a profile index value of 1, enables PVID override and a PVID of 400, and specifies that the port to which this profile is applied should be added to the egress list of VLAN 400. Packets will be untagged.

```
System(rw)->set policy profile 1 name Engr pvid-status enable pvid 400
untagged-vlans 400
```

## Assigning a Class of Service to a Role

How a packet is treated as it transits the network can be configured in a Class of Service (CoS). It is through a CoS that Quality of Service (QoS) is implemented. A CoS can be configured with the following values:

- 802.1p priority
- IP Type of Service (ToS/DSCP) rewrite value
- Inbound rate limiter (IRL)

CoS configurations are identified by a numeric value between 0 - 255. Values 0 - 7 are fixed 802.1p CoS configurations. CoS configurations 8 - 255 are user configurable. Policy uses the **cos** option in the **set policy profile** command, followed by the CoS configuration ID value to associate a CoS with a policy role. A CoS can also be associated with a rule associated with the role, or profile.



**Note:** On the Fixed Switches, only a CoS IRL associated with a policy profile will be used. A CoS IRL associated with a policy rule will be ignored.



QoS configuration details are beyond the scope of this chapter. See [Chapter 17, Configuring Quality of Service](#) in this book for a complete discussion of QoS configuration.

The following example creates a policy profile with a profile-index value of 1, enables CoS overwrite, and associates with the profile a user configured CoS 8:

```
System(rw)->set policy profile 1 cos-status enable cos 8
```

## Defining Policy Rules

There are two types of policy rules: admin rules and traffic classification rules.

### Admin Rules

An admin rule can be used to map incoming tagged frames to a policy role (profile). There can be only one admin rule configured globally per system (stack), although other admin rules can be applied to specific ports. Typically, this rule is used to implement the “User + IP phone” legacy feature. Refer to [“Configuring User + IP Phone Authentication”](#) on page 10-22 for more information. You would configure a policy profile/role for IP phones (for example, assigning a high priority and TOS/DSCP), then associate that policy profile with the admin rule, and associate the admin rule with the desired ports. Users authenticating over the same port will typically use a dynamically assigned policy role (see [“Applying Policies Dynamically”](#) on page 16-8).

Admin rules are supported only when the port’s number of authenticated users is set to 2 or greater for multi-user authentication. (Refer to [“Multi-User Authentication”](#) on page 10-4.)

[Table 16-1](#) lists the parameters used to create an admin rule.

**Table 16-1 Admin Rule Parameters**

| Parameter                             | Description                                                                                                                              |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan-tag</b> <i>vlan-id</i>        | Specifies the VLAN tag used to classify traffic.                                                                                         |
| <b>admin-pid</b> <i>profile-index</i> | Specifies the policy profile to apply to the classified traffic.                                                                         |
| <b>port-string</b> <i>port-string</i> | Optionally assigns the VLAN-to-policy mapping rule to the specified ports and also sets those ports as tagged egress ports for the VLAN. |

The following example creates an admin rule that maps frames tagged for VLAN 100 ingress on ports ge.1.1 through ge.1.4 to policy profile 10. Ports ge.1.1 through ge.1.4 will also be set as tagged egress ports for VLAN 100.

```
System(su)->set policy rule admin-profile vlan-tag 100 admin-pid 10 port-string ge.1.1-4
```

### Traffic Classification Rules

A policy traffic classification rule has two main parts: Traffic Description or classification, and Actions. The Traffic Description identifies the type of traffic to which the rule will apply. Actions specify whether that traffic will be dropped or forwarded, or have a CoS applied to it.

On the Fixed Switch platforms, for the ether type classification type only, an additional action is to assign the traffic to a VLAN if the port’s number of users is set to 1 for multi-user authentication (refer to [“Multi-User Authentication”](#) on page 10-4).

[Table 16-2](#) provides the supported policy rule traffic classification command options and definitions for the Fixed Switches.

A detailed discussion of supported traffic classifications is available in the “Traffic Classification Rules” section of the NetSight Policy Manager online help.

**Table 16-2 Policy Rule Traffic Descriptions/Classifications**

| Traffic Classification | Description                                                                         | Precedence Level |
|------------------------|-------------------------------------------------------------------------------------|------------------|
| <b>macsource</b>       | Classifies based on MAC source address.                                             | <b>1</b>         |
| <b>macdest</b>         | Classifies based on MAC destination address.                                        | <b>2</b>         |
| <b>ipsourcesocket</b>  | Classifies based on source IP address and optional post-fixed L4 TCP/UDP port.      | <b>12</b>        |
| <b>ipdestsocket</b>    | Classifies based on destination IP address and optional post-fixed L4 TCP/UDP port. | <b>13</b>        |
| <b>udpsourceport</b>   | Classifies based on UDP source port.                                                | <b>15</b>        |
| <b>udpdestport</b>     | Classifies based on UDP destination port.                                           | <b>16</b>        |
| <b>tcpsourceport</b>   | Classifies based on TCP source port.                                                | <b>17</b>        |
| <b>tcpdestport</b>     | Classifies based on TCP destination port.                                           | <b>18</b>        |
| <b>iptos</b>           | Classifies based on Type of Service field in IP packet.                             | <b>21</b>        |
| <b>ipproto</b>         | Classifies based on protocol field in IP packet.                                    | <b>22</b>        |
| <b>ether</b>           | Classifies based on type field in Ethernet II packet.                               | <b>25</b>        |

Table 16-3 provides the **set policy rule data** values that can be entered for a particular classification type, and the *mask* bits that can be entered for each classifier.

**Table 16-3 Valid Data Values for Traffic Classification Rules**

| Classification Rule Parameter                                                         | data value                                                                                                   | mask bits                                                                                                                                                                 |
|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ether                                                                                 | Type field in Ethernet II packet:<br><b>1536 - 65535</b> or <b>0x600 - 0xFFFF</b>                            | Not applicable.                                                                                                                                                           |
| ipproto                                                                               | Protocol field in IP packet:<br><b>0 - 255</b> or <b>0 - 0xFF</b>                                            | Not applicable.                                                                                                                                                           |
| Destination or Source IP Address:<br>ipdestsocket<br>ipsourcesocket                   | IP Address in dotted decimal format: <b>000.000.000.000</b> and (Optional) post-fixed port: <b>0 - 65535</b> | <b>1 - 48</b><br><b>Note:</b> If no mask value is specified, a default mask of 32 is applied to IP addresses and a default mask of 48 is applied to IP address plus port. |
| iptos                                                                                 | Type of Service field in IP packet:<br><b>0 - 255</b> or <b>0 - 0xFF</b>                                     | Not applicable.                                                                                                                                                           |
| Destination or Source MAC:<br>macdest<br>macsource<br>(Not supported on the I-Series) | MAC Address:<br><b>00-00-00-00-00-00</b>                                                                     | <b>1 - 48</b>                                                                                                                                                             |
| Destination or Source TCP port:<br>tcpdestport<br>tcpsourceport                       | TCP Port Number:<br><b>0 - 65535</b> or <b>0 - 0xFFFF</b>                                                    | <b>1 - 16</b>                                                                                                                                                             |
| Destination or Source UDP port:<br>udpsourceport<br>udpdestport                       | UDP Port Number:<br><b>0 - 65535</b> or <b>0 - 0xFFFF</b>                                                    | <b>1 - 16</b>                                                                                                                                                             |

## Examples

This example assigns a rule to policy profile 3 that will filter Ethernet II Type 1526 frames to VLAN 7:

```
C5(su)->set policy rule 3 ether 1526 vlan 7
```

This example assigns a rule to policy profile 5 that will forward UDP packets from source port 45:

```
C5(su)->set policy rule 5 udpsourceport 45 forward
```

This example assigns a rule to policy profile 1 that will drop IP source traffic from IP address 1.2.3.4, UDP port 123.

```
C5(su)->set policy rule 1 ipsourcesocket 1.2.3.4:123 mask 48 drop
```

## Applying Policy

Once policy profiles and rules have been configured, you can apply them to ports and users (devices). When you assign a policy profile to a port with the **set policy port** command, the policy is called a Default policy. Only one default policy can be applied to a port.

Also, admin rules can be used to map VLAN-tagged frames to an existing policy. As part of creating an admin rule, you can optionally specify the ingress ports to which the rule will apply, which also sets those ports as tagged egress ports for the VLAN. If no ports are specified, the rule is applied globally, but VLAN tagged egress will not be set for any ports. You would then need to configure VLAN egress by some other method, such as dynamic egress, static VLAN egress, or policy, for example. Note that only one global admin rule can exist per system (stack).

When a policy profile is assigned to a user through the authentication process, it is called dynamic policy assignment. Information is returned as part of authentication that allows the switch to assign an existing policy to the user.

A typical scenario for using default policy assignment and dynamic policy assignment in a network might include applying a restrictive default policy to all user ports and then, when users authenticate, dynamically applying a different policy profile appropriate to their role.

For example, assume you configure three policy profiles:

- A default policy for ports that allows access only to the Internet (DHCP, DNS, HTTP). See [“Configuring Guest Policy on Edge Platforms”](#) on page 16-15 for an example of configuring such a policy.
- A policy for employees with the role of “sales” that allows authenticated sales employees to have access to the network resources needed by the sales team. See [“Configuring Policy for the Edge Student Fixed Switch”](#) on page 16-15 for an example of configuring such a policy.
- A policy for employees with the role of “admin” that allows authenticated network administrators to have access to all network resources.

The restrictive default policy is applied to a port. When a guest or visitor logs in through that port, they will not be able to authenticate to the network and therefore will use the default policy.

When an employee from the sales team logs in on the same port and authenticates to the network, the “sales” policy is dynamically applied, giving the employee access to the network resources needed by the sales team.

When a network administrator logs in on the same port and authenticates to the network, the “admin” policy is dynamically applied.

All three users are on the same port at the same time, but they have different levels of access to the network, different VLANs, and different CoS.

## Applying a Default Policy

The following example assigns a default policy with index 100 to all user ports (ge.1.1 through ge.1.22) on a switch:

```
System(su)-> set policy port ge.1.1-22 100
```

## Applying Policies Dynamically

Dynamic policy assignment requires that users authenticate through a RADIUS server. Information is returned in the RADIUS Access-Accept response message that tells the switch that the user has successfully authenticated and what policy profile to assign to the user.

The RADIUS server can return a Filter-ID attribute that specifies the name of the policy to apply to the authenticated user. Alternatively, the RADIUS server can return VLAN-tunnel-attributes that can be used to assign the user to a VLAN and/or a policy.

Refer to “[Remote Authentication Dial-In Service \(RADIUS\)](#)” on page 10-7 for more information about configuring dynamic policy assignment as part of the authentication process.

## Blocking Non-Edge Protocols at the Edge Network Layer

Edge clients should be prevented from acting as servers for a number of IP services. If non-edge IP services accidentally or maliciously attach to the edge of the network, they are capable of disrupting network operation. IP services should only be allowed where and when your network design requires. [Table 16-4](#) identifies several IP Services you should consider blocking at the edge unless allowing them is part of your network architecture. See “[Assigning Traffic Classification Rules](#)” on page 16-16 for an example of how to configure a subset of these recommended IP services to drop traffic at the edge.

**Table 16-4 Non-Edge Protocols**

| Protocol                                              | Policy Effect                                                                                                                                                                                                                                                              |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DHCP Server Protocol</b>                           | Every network needs DHCP. Automatically mitigate the accidental or malicious connection of a DHCP server to the edge of your network to prevent DoS or data integrity issues, by blocking DHCP on the source port for this device.                                         |
| <b>DNS Server Protocol</b>                            | DNS is critical to network operations. Automatically protect your name servers from malicious attack or unauthorized spoofing and redirection, by blocking DNS on the source port for this device.                                                                         |
| <b>Routing Topology Protocols</b>                     | RIP, OSPF, and BGP topology protocols should only originate from authorized router connection points to ensure reliable network operations.                                                                                                                                |
| <b>Router Source MAC and Router Source IP Address</b> | Routers and default gateways should not be moving around your network without approved change processes being authorized. Prevent DoS, spoofing, data integrity and other router security issues by blocking router source MAC and router source IP addresses at the edge. |
| <b>SMTP/POP Server Protocols</b>                      | Prevent data theft and worm propagation by blocking SMTP at the edge.                                                                                                                                                                                                      |
| <b>SNMP Protocol</b>                                  | Only approved management stations or management data collection points need to be speaking SNMP. Prevent unauthorized users from using SNMP to view, read, or write management information.                                                                                |
| <b>FTP and TFTP Server Protocols</b>                  | Ensure file transfers and firmware upgrades are only originating from authorized file and configuration management servers.                                                                                                                                                |

**Table 16-4 Non-Edge Protocols (continued)**

| Protocol                   | Policy Effect                                                                                                                                                                                                                               |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Web Server Protocol</b> | Stop malicious proxies and application-layer attacks by ensuring only the right Web servers can connect from the right location at the right time, by blocking HTTP on the source port for this device.                                     |
| <b>Legacy Protocols</b>    | If IPX, AppleTalk, DECnet or other protocols should no longer be running on your network, prevent clients from using them. Some organizations even take the approach that unless a protocol is specifically allowed, all others are denied. |

## Configuring Policy

This section presents configuration procedures and command descriptions.



**Note:** In a CLI configuration context, policy roles are configured by means of policy profiles, which are created using the **set policy profile** command.

[Procedure 16-1](#) describes how to configure policy profiles and traffic classification rules.

Refer to the *CLI Reference* for your platform for command details.

### Procedure 16-1 Configuring Policy Roles

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Command                                                                                                                                                                                                                   |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | <p>Create a policy role / profile, give it an index number, and:</p> <ul style="list-style-type: none"> <li> <b>name</b> – (Optional) Specifies a name for this policy profile used by the Filter-ID attribute. This is a string from 1 to 64 characters.<br/>           The policy name must match the name in the Filter-ID attribute returned in the RADIUS Access-Accept message for the policy to be dynamically assigned to users.         </li> <li> <b>pvid-status</b> – (Optional) Enables or disables PVID override for this policy profile. If all the ether type-to-VLAN classification rules associated with this profile are missed, then this parameter, if specified, determines the default VLAN for this profile.         </li> <li> <b>pvid</b> – (Optional) Specifies the VLAN to assign to frames using this policy, if PVID override is enabled.         </li> <li> <b>cos-status</b> – (Optional) Enables or disables Class of Service override for this policy profile. If all the classification rules with assigned CoS associated with this profile are missed, then this parameter, if specified, determines the default CoS assignment.         </li> <li> <b>cos</b> – (Optional) Specifies a CoS value to assign to packets, if CoS override is enabled. Valid values are 0 to 255.         </li> </ul> | <p><b>set policy profile</b> <i>profile-index</i></p> <p><b>[name</b> <i>name</i>]</p> <p><b>[pvid-status {enable   disable}] [pvid</b> <i>pvid</i> ]</p> <p><b>[cos-status {enable   disable}] [cos</b> <i>cos</i> ]</p> |

**Procedure 16-1 Configuring Policy Roles (continued)**

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Command                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <ul style="list-style-type: none"> <li>• <b>egress-vlans</b> – (Optional) Specifies the port to which this policy profile is applied should be added to the egress list of the VLANs defined with this parameter. Frames will egress as tagged.</li> <li>• <b>forbidden-vlans</b> – (Optional) Specifies the port to which this policy profile is applied should be added as forbidden to the egress list of the VLANs defined with this parameter.</li> <li>• <b>untagged-vlans</b> – (Optional) Specifies the port to which this policy profile is applied should be added to the egress list of the VLANs defined with this parameter. Frames will egress as untagged.</li> <li>• <b>append</b> – (Optional) Appends any egress, forbidden, or untagged specified VLANs to the existing list. If append is not specified, all previous VLAN-egress settings for the policy profile will be replaced.</li> <li>• <b>clear</b> – (Optional) Clears any egress, forbidden, or untagged VLANs specified from the existing list.</li> </ul> | <p>[<b>egress-vlans</b> <i>egressvlans</i>]</p> <p>[<b>forbidden-vlans</b> <i>forbidden-vlans</i> ]</p> <p>[<b>untagged-vlans</b> <i>untagged-vlans</i> ]</p> <p>[<b>append</b> ] [<b>clear</b>]</p>                                                                                                                                                                                                                 |
| 2.   | <p>Create traffic classification rules and associate them with a policy profile.</p> <ul style="list-style-type: none"> <li>• Specify the classification type, data, and optionally, the mask for the data</li> </ul> <p>Refer to <a href="#">Table 16-2</a> on page 16-6 for descriptions of classification types and <a href="#">Table 16-3</a> on page 16-6 for valid data and mask values.</p> <ul style="list-style-type: none"> <li>• Specify the action to take when the rule is hit.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <p><b>set policy rule</b> <i>profile-index</i></p> <p>{<b>ether</b>   <b>ipproto</b>   <b>ipdestsocket</b>   <b>ipsourcesocket</b>   <b>iptos</b>   <b>macdest</b>   <b>macsource</b>   <b>tcpdestport</b>   <b>tcpsourceport</b>   <b>udpdestport</b>   <b>udpsourceport</b>} <i>data</i> [<b>mask</b> <i>mask</i>]</p> <p>{<b>[vlan</b> <i>vlan</i>] [<b>cos</b> <i>cos</i>]   [<b>drop</b>   <b>forward</b>]}</p> |
| 3.   | <p>If the policy is intended to be a default port policy, apply the policy to the desired ports.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <p><b>set policy port</b> <i>port-string profile-index</i></p>                                                                                                                                                                                                                                                                                                                                                       |

[Procedure 16-2](#) describes how to configure an admin rule. Refer to the *CLI Reference* for your platform for command details.

**Procedure 16-2 Configuring an Admin Rule**

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Command(s)                                                                                                                                                               |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | <p>Create an admin rule:</p> <ul style="list-style-type: none"> <li>• <b>vlantag</b> -- Specifies the VLAN tag on which this rule will classify traffic</li> <li>• <b>admin-pid</b> – Specifies the policy profile that will be applied to traffic classified by the VLAN tag. Valid values are 1 - 1023.</li> <li>• <b>port-string</b> – (Optional) Applies this admin rule to one or more ingress ports.</li> </ul> <p>The ports will also be set as tagged egress ports for the VLAN.</p> | <p><b>set policy rule admin-profile</b></p> <p><b>vlantag</b> <i>vlan-id</i></p> <p><b>admin-pid</b> <i>admin-pid</i></p> <p>[<b>port-string</b> <i>port-string</i>]</p> |

[Table 16-5](#) on page 16-11 describes how to display policy information and statistics.

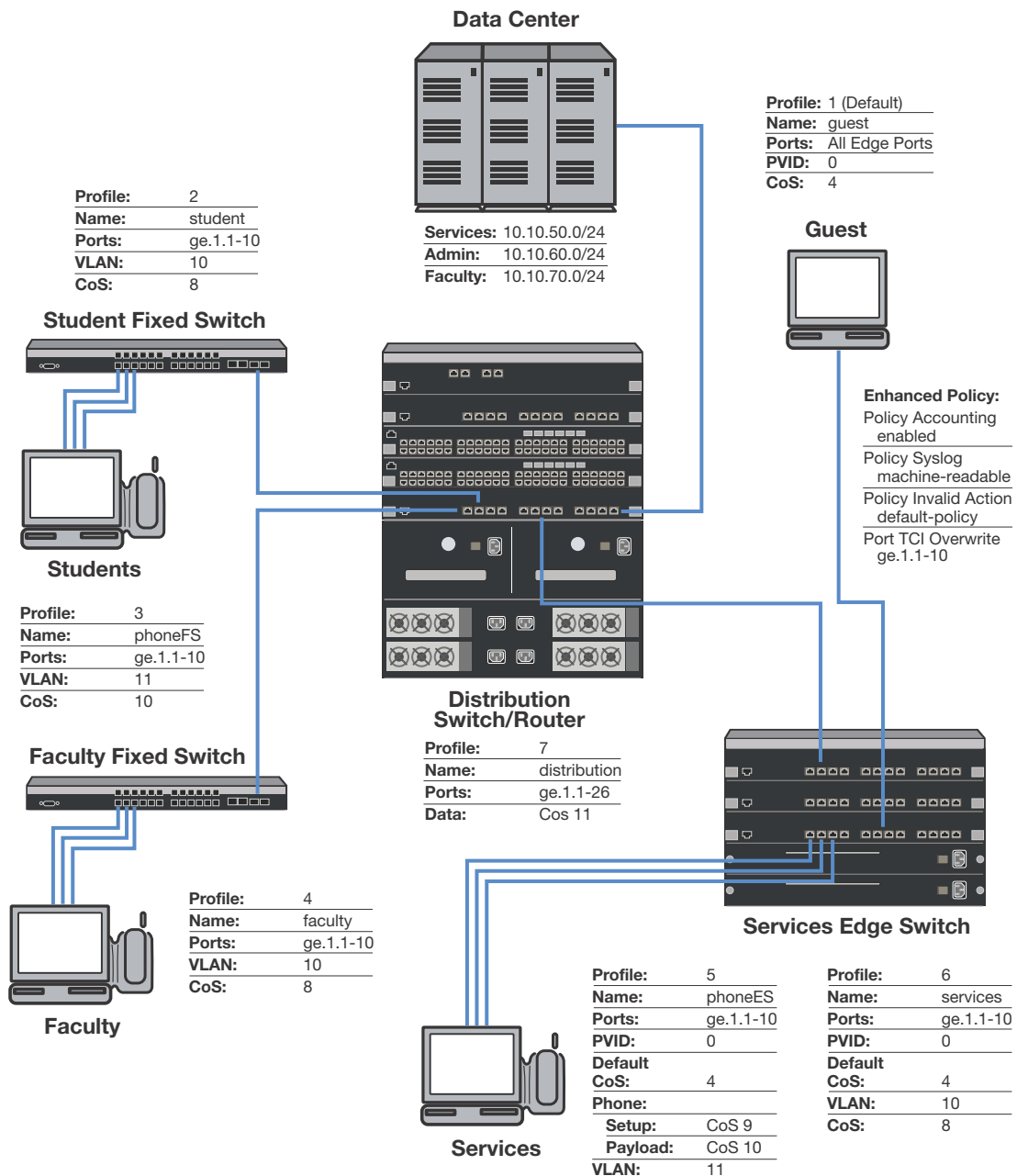
**Table 16-5 Displaying Policy Configuration and Statistics**

| Task                                                            | Command(s)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display policy role information.                                | <b>show policy profile</b> { <b>all</b>   <i>profile-index</i> [ <i>consecutive-pids</i> ] [- <b>verbose</b> ]}                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Display policy classification and admin rule information.       | <b>show policy rule</b> [ <b>all</b>   <b>admin-profile</b>   <i>profile-index</i> ] [ <i>classification-type</i> [ <i>data</i> ]] [ <b>mask</b> <i>mask</i> ] [ <b>port-string</b> <i>port-string</i> ] [ <b>rule-status</b> { <b>active</b>   <b>not-in-service</b>   <b>not-ready</b> }] [ <b>storage-type</b> { <b>non-volatile</b>   <b>volatile</b> }] [ <i>vlan</i> <i>vlan</i> ]   [ <b>drop</b>   <b>forward</b> ] [ <b>dynamic-pid</b> <i>dynamic-pid</i> ] [ <b>cos</b> <i>cos</i> ] [ <b>admin-pid</b> <i>admin-pid</i> ] [- <b>verbose</b> ] [ <b>usage-list</b> ] [ <b>display-if-used</b> ] |
| Display all policy classification capabilities for this device. | <b>show policy capability</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

# Policy Configuration Example

This section presents a college-based policy configuration example. Figure 16-1 displays an illustration of the policy configuration of a example infrastructure. Although the illustration shows an installation that includes Enterasys S-Series switches (as a distribution switch/router and as a services edge switch), and the following discussion describes the roles and policy domains applied to the complete infrastructure, the CLI platform examples will include only the fixed switch configurations.

Figure 16-1 College-Based Policy Configuration





## Roles

The example defines the following roles:

- **guest** – Used as the default policy for all unauthenticated ports. Connects a PC to the network providing internet only access to the network. Provides guest access to a limited number of the edge switch ports to be used specifically for internet only access. Policy is applied using the port level default configuration.
- **student** – Connects a dorm room PC to the network through a “Student” Fixed Switch port. A configured CoS rate limits the PC. Configured rules deny access to administrative and faculty servers. The PC authenticates using RADIUS. The **student** policy role is applied dynamically using the Filter-ID attribute. If all rules are missed, the settings configured in the **student** policy profile are applied.
- **phoneFS** – Connects a dorm room or faculty office VoIP phone to the network using a stackable fixed switch port. A configured CoS rate limits the phone and applies a high priority. The phone authenticates using RADIUS. Policy is applied dynamically using the Filter-ID returned in the RADIUS response message. If all rules are missed, the settings configured in the phoneFS policy profile are applied.
- **faculty** – Connects a faculty office PC to the network through a “Faculty” Fixed Switch port. A configured CoS rate limits the PC. A configured rule denies access to the administrative servers. The PC authenticates using RADIUS. The **faculty** policy role is applied dynamically using the Filter-ID attribute. If all rules are missed, the settings configured in the **faculty** policy profile are applied.
- **phoneES** – Connects a services VoIP phone to the network using a Services Edge Switch port. A configured CoS rate limits the phone for both setup and payload, and applies a high priority. The phone authenticates using RADIUS. Tunnel authentication is enabled. The base VLAN is applied using the tunnel attributes returned in the RADIUS response message. Policy is applied using a mappable configuration. If all rules are missed, the settings configured in the **phoneES** policy profile are applied.
- **services** – Connects a services PC to the network through the Services Edge Switch port. A configured CoS rate limits the PC. Services are denied access to both the student and faculty servers. The PC authenticates using RADIUS. The base VLAN is applied using the tunnel attributes returned in the RADIUS response message for the authenticating user. The **services** policy role is applied using a policy mappable setting. The policy accounting, syslog, invalid action and TCI overwrite are enabled for this role. If all rules are missed, the settings configured in the **services** policy profile are applied.
- **distribution** – The Distribution policy role is applied at the Distribution Switch providing rate limiting.

## Policy Domains

It is useful to break up policy implementation into logical domains for ease of understanding and configuration. For this example, it is useful to consider four domains: basic edge, standard edge on the Fixed Switch, premium edge on the Services Edge Switch, and premium distribution on the Distribution Switch.

### Basic Edge

Protocols not appropriate to the edge should be blocked. For this example we will block DHCP, DNS, SNMP, SSH, Telnet and FTP at the edge on the data VLAN. We will forward destination port DHCP and DNS and source port for IP address request to facilitate auto configuration and IP address assignment. See “[Blocking Non-Edge Protocols at the Edge Network Layer](#)” on page 16-8 for a listing of protocols you should consider blocking at the edge.

## Standard Edge

Edge Switch platforms will be rate-limited using a configured CoS that will be applied to the student and faculty, and phoneFS policy roles. Policies will be applied dynamically at authentication using a RADIUS authentication server and the Filter-ID attribute.

## Premium Edge

The S-Series Edge Switch will be rate-limited using a configured CoS that is applied to the services and phoneES policy role. This premium edge platform will be enabled for the following capabilities:

- Policy Accounting
- Syslog rule usage enabled and set to machine-readable
- Invalid policy action set to drop
- TCI overwrite enabled

## Premium Distribution

The S-Series Distribution Switch Router will be rate-limited using a configured CoS. Premium distribution will be enabled for the following policy capabilities:

- Policy Accounting
- Syslog Rule Usage enabled and set to machine-readable
- Invalid policy action set to drop
- TCI overwrite enabled

## Platform Configuration

This section will provide the CLI-based policy configuration on the following platforms:

- Student Fixed Switch
- Faculty Fixed Switch

The CLI configuration for the Services Edge Switch and Distribution Switch are not presented here. Refer to the *S-Series Configuration Guide* for that information.

CLI configuration is performed on each platform individually. When using the NetSight Policy Manager, configuration takes place at a central location and is pushed out to the appropriate network devices.

For this configuration example, we assume that CoS related configuration has already been performed. See [Chapter 17, Configuring Quality of Service](#) in this book for a complete discussion of QoS configuration.



**Note:** CLI command prompts used in this configuration example have the following meaning:

- Enterasys(rw)-> – Input on all platforms used in this example.
- Fixed Switch(rw)-> – Input on all Fixed Switches.
- StudentFS-> – Input on the student Fixed Switch.
- FacultyFS-> – Input on the faculty Fixed Switch.

## Configuring Guest Policy on Edge Platforms

All edge ports will be set with a default **guest** policy using the **set policy port** command. This guest policy provides for an internet-only access to the network. Users on all ports will attempt to authenticate. If the authentication succeeds, the policy returned by authentication overrides the default port policy setting. If authentication fails, the guest policy is used.



**Note:** The CLI configuration for the Services Edge Switch is not presented here. Refer to the *S-Series Configuration Guide* for that information.

### Configuring the Policy Role

The guest role is configured with:

- A profile-index value of **1**
- A name of **guest**
- A PVID set to **0** (deny all traffic)
- A CoS set to **4** (note that CoS has previously been configured)

Create the guest policy profile on all platforms:

```
Enterasys(rw)->set policy profile 1 name guest pvid-status enable pvid 0
cos-status enable cos 4
```

### Assigning Traffic Classification Rules

For cases where discovery must take place to assign an IP address, DNS and DHCP traffic must be allowed. Forwarding of traffic is allowed on UDP source port 68 (IP address request) and UDP destination ports 53 (DNS) and 67 (DHCP).

```
Enterasys(rw)->set policy rule 1 udpsourceport 68 mask 16 forward
Enterasys(rw)->set policy rule 1 udpdestport 53 mask 16 forward
Enterasys(rw)->set policy rule 1 udpdestport 67 mask 16 forward
```

Guest policy allows internet traffic. TCP destination Ports 80, 8080, and 443 will be allowed traffic forwarding.

```
Enterasys(rw)->set policy rule 1 tcpdestport 80 mask 16 forward
Enterasys(rw)->set policy rule 1 tcpdestport 443 mask 16 forward
Enterasys(rw)->set policy rule 1 tcpdestport 8080 mask 16 forward
```

ARP forwarding is required on ether port 0x806.

```
Enterasys(rw)->set policy rule 1 ether 0x806 mask 16 forward
```

### Assigning the Guest Policy Profile to All Edge Ports

Assign the guest policy profile to all Fixed Switch and Services Edge Switch ports.

```
Enterasys(rw)->set policy port ge.*.* 1
```

## Configuring Policy for the Edge Student Fixed Switch

### Configuring the Policy Role

The student role is configured with:

- A profile-index value of **2**
- A name of **student**
- A port VLAN of **10**

- A CoS of 8

Create a policy role that applies a CoS 8 to data VLAN 10 and configures it to rate-limit traffic to 200,000 kbps with a moderate priority of 5.

```
StudentFS(rw)->set policy profile 2 name student pvid-status enable pvid 10
cos-status enable cos 8
```

### Assigning Traffic Classification Rules

Forward traffic on UDP source port for IP address request (68), and UDP destination ports for protocols DHCP (67) and DNS (53). Drop traffic on UDP source ports for protocols DHCP (67) and DNS (53). Drop traffic for protocols SNMP (161), SSH (22), Telnet (23) and FTP (20 and 21).

```
StudentFS(rw)->set policy rule 2 udpsourceport 68 mask 16 forward
StudentFS(rw)->set policy rule 2 udpdestport 67 mask 16 forward
StudentFS(rw)->set policy rule 2 udpdestport 53 mask 16 forward
StudentFS(rw)->set policy rule 2 udpsourceport 67 mask 16 drop
StudentFS(rw)->set policy rule 2 udpsourceport 53 mask 16 drop
StudentFS(rw)->set policy rule 2 udpdestport 16 mask 16 drop
StudentFS(rw)->set policy rule 2 tcpdestport 22 mask 16 drop
StudentFS(rw)->set policy rule 2 tcpdestport 23 mask 16 drop
StudentFS(rw)->set policy rule 2 tcpdestport 20 mask 16 drop
StudentFS(rw)->set policy rule 2 tcpdestport 21 mask 16 drop
```

Students should only be allowed access to the services server (subnet 10.10.50.0/24) and should be denied access to both the administrative server (subnet 10.10.60.0/24) and the faculty server (subnet 10.10.70.0/24).

```
StudentFS(rw)->set policy rule 2 ipdestsocket 10.10.60.0 mask 24 drop
StudentFS(rw)->set policy rule 2 ipdestsocket 10.10.70.0 mask 24 drop
```

### Configuring Dynamic Policy Assignment

Configure the RADIUS server user accounts with the appropriate information using the Filter-ID attribute for student role members and devices. When a student authenticates through the RADIUS server, the name of the **student** policy is returned in the RADIUS Access-Accept response message and that policy is applied by the switch to the student user.

## Configuring PhoneFS Policy for the Edge Fixed Switch

### Configuring the Policy Role

The phoneFS role is configured on both the dorm room and faculty office Fixed Switches with:

- A profile-index of 3
- A name of **phoneFS**
- A port VLAN of 11
- A CoS of 10

Because we can not apply separate rate limits to the phone setup and payload ports on the Fixed Switch using policy rules, apply CoS 10 with the higher payload appropriate rate limit of 100k bps and a high priority of 6 to the phoneFS role.

```
Fixed Switch(rw)->set policy profile 3 name phoneFS pvid-status enable pvid 11
cos-status enable cos 10
```

### Assigning Traffic Classification Rules

Drop traffic for protocols SNMP (161), SSH (22), Telnet (23) and FTP (20 and 21) on the phone VLAN. Forward traffic on UDP source port for IP address request (68) and forward traffic on UDP

destination ports for protocols DHCP (67) and DNS (53) on the phone VLAN, to facilitate phone auto configuration and IP address assignment.

```
Fixed Switch(rw)->set policy rule 3 udpdestport 161 mask 16 drop
Fixed Switch(rw)->set policy rule 3 tcpdestport 22 mask 16 drop
Fixed Switch(rw)->set policy rule 3 tcpdestport 23 mask 16 drop
Fixed Switch(rw)->set policy rule 3 tcpdestport 20 mask 16 drop
Fixed Switch(rw)->set policy rule 3 tcpdestport 21 mask 16 drop
Fixed Switch(rw)->set policy rule 3 udpsourceport 68 mask 16 forward
Fixed Switch(rw)->set policy rule 3 udpdestport 67 mask 16 forward
Fixed Switch(rw)->set policy rule 3 udpdestport 53 mask 16 forward
```

## Configuring Dynamic Policy Assignment

Configure the RADIUS server user accounts with the appropriate policy Filter-ID for phoneFS role members and devices. When a phone authenticates through the RADIUS server, the name of the **phoneFS** policy is returned in the RADIUS Access-Accept response message and that policy is applied by the switch to the phone device.

## Configuring Policy for the Edge Faculty Fixed Switch

### Configuring the Policy Role

The faculty role is configured with:

- A profile-index value of **4**
- A name of **faculty**
- A port VLAN of **10**
- A CoS of **8**

Create a policy role that applies a CoS 8 to data VLAN 10 and configures it to rate-limit traffic to 200,000 kbps with a moderate priority of 5.

```
FacultyFS(rw)->set policy profile 4 name faculty pvid-status enable pvid 10
cos-status enable cos 8
```

### Assigning Traffic Classification Rules

Forward traffic on UDP source port for IP address request (68), and UDP destination ports for protocols DHCP (67) and DNS (53). Drop traffic on UDP source ports for protocols DHCP (67) and DNS (53). Drop traffic for protocols SNMP (161), SSH (22), Telnet (23) and FTP (20 and 21) on both the data and phone VLANs.

```
FacultyFS(rw)->set policy rule 4 udpsourceport 68 mask 16 forward
FacultyFS(rw)->set policy rule 4 udpdestport 67 mask 16 forward
FacultyFS(rw)->set policy rule 4 udpdestport 53 mask 16 forward
FacultyFS(rw)->set policy rule 4 udpsourceport 67 mask 16 drop
FacultyFS(rw)->set policy rule 4 udpsourceport 53 mask 16 drop
FacultyFS(rw)->set policy rule 4 udpdestport 16 mask 16 drop
FacultyFS(rw)->set policy rule 4 tcpdestport 22 mask 16 drop
FacultyFS(rw)->set policy rule 4 tcpdestport 23 mask 16 drop
FacultyFS(rw)->set policy rule 4 tcpdestport 20 mask 16 drop
FacultyFS(rw)->set policy rule 4 tcpdestport 21 mask 16 drop
```

Faculty should only be allowed access to the services server (subnet 10.10.50.0/24) and the faculty server (subnet 10.10.70.0/24) and should be denied access to the administrative server (subnet 10.10.60.0/24).

```
FacultyFS(rw)->set policy rule 4 ipdestsocket 10.10.60.0 mask 24 drop
```

## Configuring Dynamic Policy Assignment

Configure the RADIUS server user accounts with the appropriate information using the Filter-ID attribute for faculty role members and devices. When a faculty member authenticates through the RADIUS server, the name of the **faculty** policy is returned in the RADIUS Access-Accept response message and that policy is applied by the switch to the faculty user.

## Terms and Definitions

Table 16-6 lists terms and definitions used in this policy configuration discussion.

**Table 16-6 Policy Configuration Terms and Definitions**

| Term                     | Definition                                                                                                                                                                                                                                                                                   |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Admin Rule               | A policy rule that assigns traffic classified by a specific VLAN tag to a policy role.                                                                                                                                                                                                       |
| Class of Service (CoS)   | A logical container for packet priority, ToS/DSCP, and forwarding treatment that determines how the firmware treats a packet as it transits the link.                                                                                                                                        |
| Filter-ID                | A string that is formatted in the RADIUS Access-Accept packet sent back from the authentication server to the switch during the authentication process. In the Enterasys policy context, the string contains the name of the policy role to be applied to the authenticating user or device. |
| Policy                   | A component of Secure Networks that provides for the configuration of a role based profile for the securing and provisioning of network resources based upon the function the user or device plays within the enterprise network.                                                            |
| Policy Profile           | A logical container for the rules that define a particular policy role. In a CLI context, Policy Profile is equivalent to Policy Role.                                                                                                                                                       |
| Policy Rule              | Rules that define how traffic classified by various criteria should be treated.                                                                                                                                                                                                              |
| Role                     | Within NetSight, the grouping of individual users or devices into a logical behavioral profile for the purpose of applying policy. In a CLI context, Role = Policy Profile.                                                                                                                  |
| Rule Precedence          | A value associated with classification types that determines the sequence in which classification rules are applied to a packet.                                                                                                                                                             |
| Traffic Classification   | A policy element that allows MAC or IP address, packet type, port, or VLAN used to be used as the basis for identifying the traffic to which the policy will be applied.                                                                                                                     |
| Untagged and Tagged VLAN | Untagged VLAN frames are classified to the VLAN associated with the port it enters. Tagged VLAN frames are classified to the VLAN specified in the VLAN tag; the PVID is ignored.                                                                                                            |
| VLAN Egress List         | A configured list of ports that a frame for this VLAN can exit.                                                                                                                                                                                                                              |

## Configuring Quality of Service

This chapter describes the following QoS features:

| For information about...                                       | Refer to page... |
|----------------------------------------------------------------|------------------|
| <a href="#">Quality of Service Overview</a>                    | 17-1             |
| <a href="#">CoS Hardware Resource Configuration</a>            | 17-9             |
| <a href="#">The QoS CLI Command Flow</a>                       | 17-14            |
| <a href="#">Port Priority and Transmit Queue Configuration</a> | 17-15            |
| <a href="#">Port Traffic Rate Limiting</a>                     | 17-17            |

### Quality of Service Overview

Quality of Service (QoS) is:

- A mechanism for the management of bandwidth
- The ability to give preferential treatment to some packets over others
- Based upon packet classification and forwarding treatment

You configure packet preference and forwarding treatment based upon a flow's sensitivity to delay, delay variation (jitter), bandwidth, availability, and packet drop.



**Note:** A flow is a stream of IP packets in which the value of a fixed set of IP packet fields is the same for each packet in the stream. Each packet containing the same value for all of these fields is considered part of the same flow, until flow expiration occurs. If a packet is viewed with any set member field value that is different from any current flow, a new flow is started based upon the set field values for that packet.

QoS uses packet priority, in conjunction with queue treatment configuration, to determine the interface's inbound and forwarding behavior for a packet. Packet preference and forwarding treatment for a given flow can be applied to roles configured in Enterasys policy.

Without QoS, all packets are treated as though the delivery requirements and characteristics of any given packet are equal to any other packet. In other words, non-QoS packet delivery is not able to take into account application sensitivity to packet delay, jitter, amount of bandwidth required, packet loss, or availability requirements of the flow. QoS provides management mechanisms for these flow characteristics.

### Implementing QoS

QoS determines how a flow will be treated as it transits the link. To determine how a flow should be treated, you must first understand the characteristics of the flows on your network, and



secondly, you must identify these flows in a way that QoS can recognize. In this sense, QoS is the third step in a three step process. The three-steps Enterasys recommends for configuring QoS are:

- Understand your network flows using NetFlow
- Associate the flows on your network with a well defined role using Enterasys policy
- Configure the appropriate link behavior for that role by associating the role with a QoS configuration

## Quality of Service Operation

QoS is all about managing the bandwidth in a manner that aligns the delivery requirements of a given flow with the available port resources. In a QoS context, a flow is a stream of packets that are classified with the same class of service as the packets transit the interface. QoS manages bandwidth for each flow by:

- Assigning different priority levels to different packet flows.
- Marking or re-marking the packet priority at port ingress with a Type of Service (ToS).
- Sorting flows by transmit queue. Higher priority queues get preferential access to bandwidth during packet forwarding.
- Limiting the amount of bandwidth available to a given flow by dropping (rate limiting) packets in excess of configured limits.

These QoS abilities collectively make up a Class of Service (CoS). The remainder of this section will describe CoS and its components.

## Class of Service (CoS)

You implement QoS features in a Class of Service (CoS). The hardware resource components that can be configured as part of a CoS are:

- **Inbound Rate Limiters (IRL)** - allow you to configure a threshold above which a port will not process traffic.
- **Flood Control** - configures a threshold above which a port will not receive unknown-unicast, multicast, or broadcast packets.

The CoS configuration of each port hardware resource is optional. IRL and flood control each have a single configurable rate limiting port hardware resource option.

CoS configuration is applied to the ingressing packet based upon the packet's 802.1p priority, port, and policy settings.

How the firmware treats a packet as it transits the link depends upon the priority and forwarding treatments configured in the CoS assigned to the packet. Up to 256 unique CoS entries can be configured. CoS entries 0–7 are configured by default with an 802.1p priority assigned and default forwarding treatment. CoS entries 0–7 cannot be removed. CoS entries 0–7 are reserved for mapping an 802.1p priority to a CoS index. CoS entries 8-255 can be configured and used by policy for the following services:

- 802.1p priority
- IP Type of Service (ToS) marking
- In-bound (IRL) rate limiter
- Flood control



There are up to four areas of CoS configuration depending on what type of hardware resource you want to configure. The terminology associated with CoS configuration is introduced in [Table 17-1](#).

**Table 17-1 CoS Configuration Terminology**

| Term                          | Description                                                                                                                                                                                                                                                                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CoS Setting</b>            | Maps configured resources to a CoS index. When a packet is received, the packet is mapped to a CoS index based on the packet 802.1 priority, port, and policy role, if a policy role is present. The CoS index translates into available hardware resources through indirect mappings to IRL or the administrative state of flood control. |
| <b>CoS Reference</b>          | Provides a means of mapping a CoS setting to a specific hardware resource, such as an IRL.                                                                                                                                                                                                                                                 |
| <b>CoS Port Resource</b>      | Specifies the IRL or flood control rate limiter threshold value that the CoS reference is mapped to.                                                                                                                                                                                                                                       |
| <b>CoS Port Configuration</b> | Specifies the ports to which CoS resource configuration should be applied.                                                                                                                                                                                                                                                                 |

## CoS Settings

Use the CoS settings configuration when mapping the priority of the ingressing packet to a hardware resource reference, flood control state, or 802.1 priority or ToS remarking.

### CoS Hardware Resource Reference

The CoS hardware resource reference can be an inbound rate limiter reference.

### CoS Flood Control State

CoS flood control state enables or disables flood control for the CoS setting.

### CoS Priority and ToS Rewrite

The two parameters configurable for CoS priority are 802.1p and Type of Service (ToS). Each CoS can be mapped to an 802.1p priority and a ToS rewrite value. 802.1p and ToS are specified in the CoS settings configuration layer.

The 802.1p parameter is:

- A subset of ToS with values 0–7 (upper 3 bits of the 8 bit ToS field)
- Supported in both layer 2 and layer 3

The ToS parameter is:

- An 8-bit field with values 0–255
- Supported in layer 3 only
- Also referred to as the Differentiated Services Code Point (DSCP) when limited to the lower 5 bits of the field

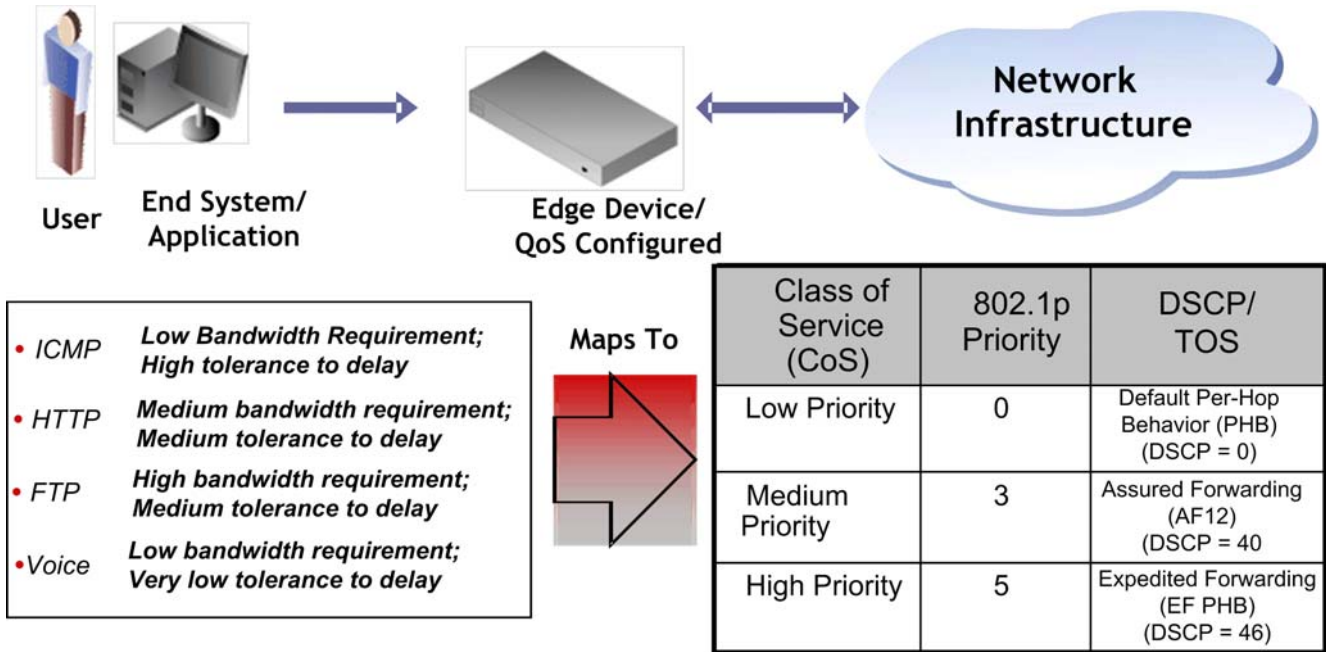
[Figure 17-1](#) on page 17-4 displays the relationship between your application, priority level, 802.1p, and ToS assignments (shown here using DSCP terminology).

QoS priority/ToS configuration:

- Derives its characteristic requirements from the end-system application.
- Is configured on the edge device the application is connected to

- Is propagated through the network in the protocol packet header

**Figure 17-1 Assigning and Marking Traffic with a Priority**



The ICMP protocol, used for error messaging, has a low bandwidth requirement, with a high tolerance for delay and jitter, and is appropriate for a low priority setting. HTTP and FTP protocols, used respectively for browser-generated and file transfer traffic, have a medium to high bandwidth requirement, with a medium to high tolerance for delay and jitter, and are appropriate for a medium priority level. Voice (VoIP), used for voice calls, has a low bandwidth requirement, but is very sensitive to delay and jitter and is appropriate for a high priority level.

See RFC 1349 for further details on ToS. See RFCs 2474 and 2475 for further details on DSCP.

## CoS Reference

Use the CoS reference configuration if you need to map a CoS setting IRL reference to an IRL port resource rate limiter.

The CoS reference configuration is set by specifying the type of hardware resource for the reference (IRL), the port group the reference is being applied to, and the hardware resource reference configured in CoS settings, and the actual rate limiting port resource for this mapping.

## Port Group and Type

CoS port groups provide for grouping ports by CoS feature configuration and port type. Ports are required to be configured by groups — this feature provides a meaningful way of identifying ports by similar functionality and port type.

Groups consist of a group number and port type and are numbered as such, *port-group.port-type*. The port group number is configurable. A port on a fixed switch platform is always port type 0.

For example: port group 0, port type 0 would be numbered port group 0.0. A default port group exists per hardware resource: IR and flood control. The default port group is identified as port group 0 and port type 0 and is indexed as 0.0 for each feature. These default port groups cannot be removed and all physical ports in the system are assigned to one port group for each feature.

Additional port groups, up to eight (0 through 7) total, may be created by changing the port group value. Ports assigned to a new port group cannot belong to another non-default port group entry and must be comprised of the same port type as defined by the port group you are associating it with. The creation of additional port groups could be used to combine similar ports by their function for flexibility. For instance, ports associated with users can be added to a port group called Users and ports associated with uplink ports can be added to a port group called Uplink. Using these port groups, a class of service unique to each group can assign different rate limits to each port group. User ports can be assigned a rate limit configured in one CoS, while Uplink ports can be assigned a different rate limit configured in another CoS.

Port Type is a fixed value that determines the IRL and flood control resource capabilities based upon the device the port belongs to. Knowledge of these capabilities is important when configuring queue behaviors. CoS port type can be determined using the **show cos port-type** command.

## CoS Settings Reference to Port Resource Mapping

Use the CoS reference configuration to map the resource reference from the CoS settings configuration to the port hardware resources being acted upon by this configuration.

- IRL CoS reference – Maps the CoS settings IRL reference to the IRL port resource the rate limit is to be applied to.

## Port Resources

Use the CoS port resource configuration layer to associate actual rate limiter values to a port group and hardware resource. Configure CoS port resource by identifying the CoS hardware resource type (IRL or flood control), port group, and port resource, followed by a rate limiter.

The IRL rate limit is specified as a unit (kbps) and a data rate. The flood control rate limit is specified as packets per second.

- IRL – Setting an IRL rate limiter means that packets ingressing the port will not be allowed to exceed the rate specified by the rate limiter. If the rate is exceeded, you can specify whether packets that exceed the rate limit should be dropped and whether the port should be disabled. You can enable or disable syslog and trap features.

IRL port resources are first referenced using the CoS settings and CoS reference configurations. Ports are applied to the specified CoS port resources using the CoS port configuration.

- Flood control – Setting a flood control rate limiter means that received packets of the specified type that exceed the flood control threshold will be prevented from egressing any port. Configurable packet types are:
  - unknown unicast
  - multicast
  - broadcast

If the rate is exceeded, you can specify whether the port should be disabled. You can enable or disable syslog and trap features.

## Port Configuration

The CoS port configuration layer applies a port list to the port group. Configure CoS port configuration by identifying the CoS hardware resource type (IRL or flood control) and port group for this port configuration, a name for this configuration, a port list of ports assigned to this port group, and whether the port list should be cleared or be appended to any existing port list.

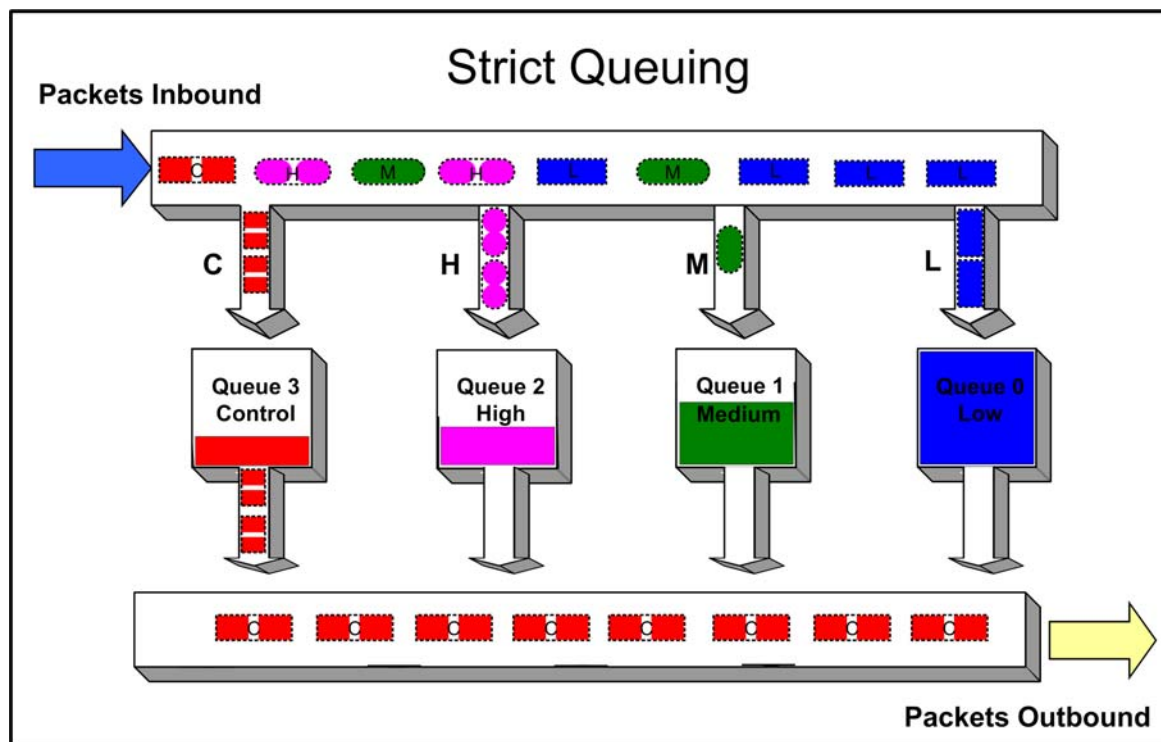
## Preferential Queue Treatment for Packet Forwarding

There are three types of preferential queue treatments for packet forwarding: strict priority, weighted fair, and hybrid.

### Strict Priority Queuing

With Strict Priority Queuing, a higher priority queue must be empty before a lower priority queue can transmit any packets. Strict priority queuing is illustrated in Figure 17-2. Inbound packets enter on the upper left and proceed to the appropriate queue, based upon the TxQ configuration in the CoS. Outbound packets exit the queues on the lower right. At this time only queue 3 packets are forwarded. This will be true until queue 3 is completely empty. Queue 2 packets will then be forwarded. Queue 1 packets will only forward if both queue 2 and queue 3 are empty. Queue 0 packets will only forward if all other queues are empty. Strict priority queuing assures that the highest priority queue with any packets in it will get 100 percent of the bandwidth available. This is particularly useful for one or more priority levels with low bandwidth and low tolerance for delay. The problem with strict priority queuing is that should the higher level queues never fully empty, lower level queues can be starved of bandwidth.

Figure 17-2 Strict Priority Queuing Packet Behavior

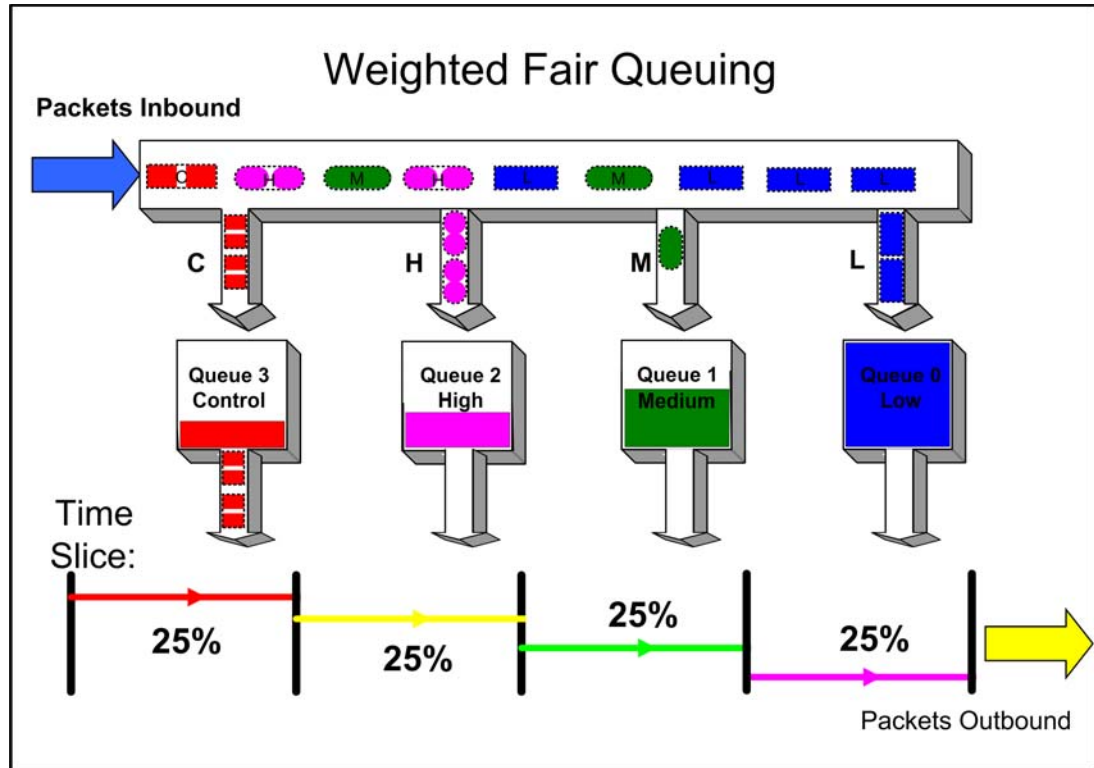


### Weighted Fair Queuing

With weighted fair queuing, queue access to bandwidth is divided up by percentages of the time slices available. For example, if 100 percent is divided into 64 time slices, and each queue is configured for 25 percent, each queue will get 16 time slices, after which the next lowest priority queue will get the next 16, and so on. Should a queue empty before using its current share of time slices, the remaining time slices are shared with all remaining queues. Figure 17-3 on page 17-7 depicts how weighted fair queuing works. Inbound packets enter on the upper left of the box and proceed to the appropriate priority queue. Outbound packets exit the queues on the lower right. Queue 3 has access to its percentage of time slices so long as there are packets in the queue. Then

queue 2 has access to its percentage of time slices, and so on round robin. Weighted fair queuing assures that each queue will get at least the configured percentage of bandwidth time slices. The value of weighted fair queuing is in its assurance that no queue is starved for bandwidth. The downside of weighted fair queuing is that packets in a high priority queue, with low tolerance for delay, will wait until all other queues have used the time slices available to them before forwarding. So weighted fair queuing would not be appropriate for applications with high sensitivity to delay or jitter, such as VoIP.

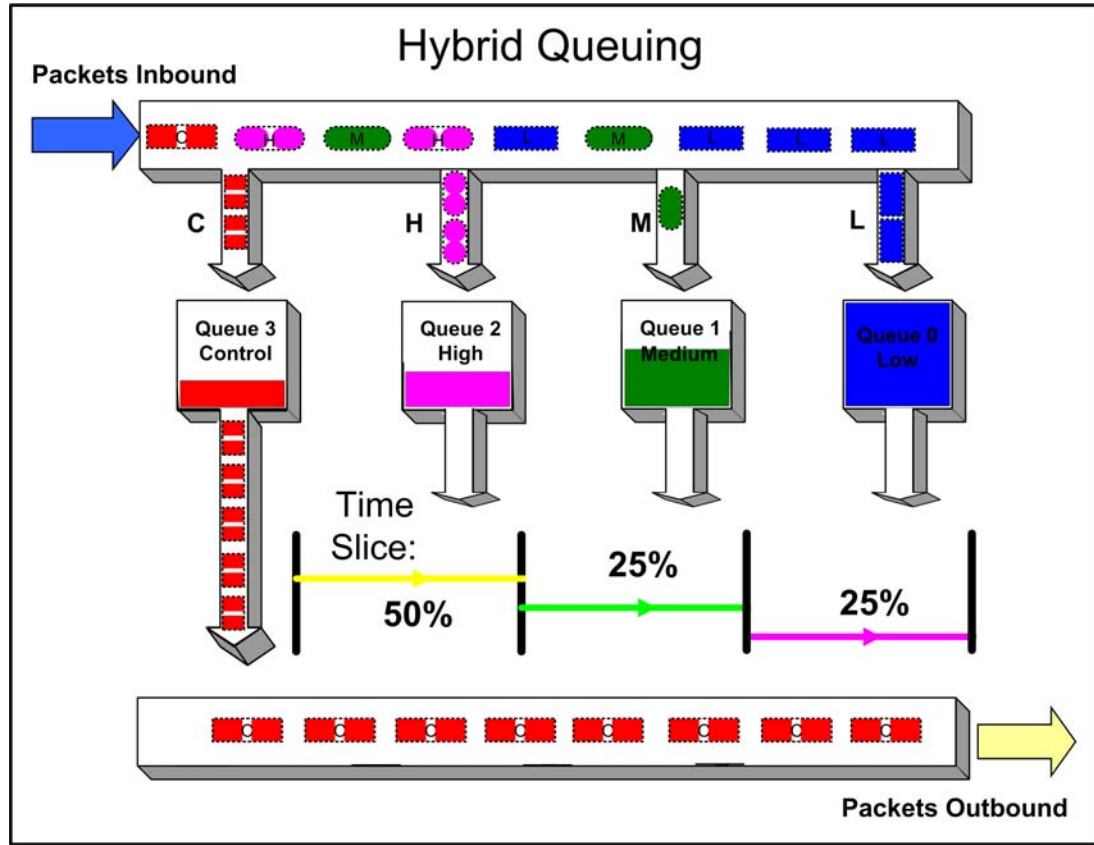
**Figure 17-3 Weighted Fair Queuing Packet Behavior**



## Hybrid Queuing

Hybrid queuing combines the properties of both strict priority and weighted fair queuing. [Figure 17-4](#) on page 17-8, depicts hybrid queuing. The configuration is for strict priority queuing on queue 3 and weighted fair queuing for the remaining queues, with queue 2 receiving 50 percent of the remaining time slices, and the other queues receiving 25 percent each. The benefit of hybrid queuing is that queues configured as strict will receive all the bandwidth that is available in the order of their priority until empty. Remaining bandwidth will be used by the weighted fair queues based upon the time slice percentages configured. The down side remains that anytime strict priority queuing is used, should the strict priority queues never fully empty, remaining queues will be starved of bandwidth.

Figure 17-4 Hybrid Queuing Packet Behavior

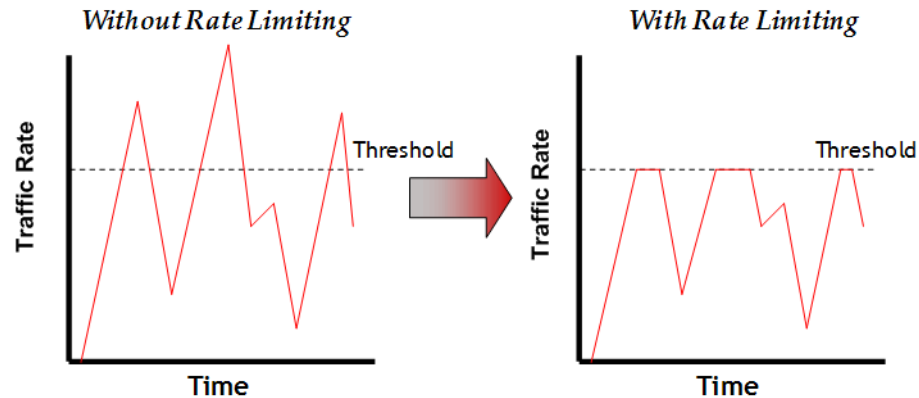


## Rate Limiting

Rate limiting is used to control the rate of traffic entering (inbound) a switch per CoS. Rate limiting allows for the throttling of traffic flows that consume available bandwidth, in the process providing room for other flows. Rate limiting guarantees the availability of bandwidth for other traffic by preventing the rate limited traffic from consuming more than the assigned amount of a network's resources. Rate limiting accomplishes this by setting a cap on the bandwidth utilization of specific types of inbound traffic. When a rate limit has been exceeded, the CoS can be configured to perform one or all of the following: record a Syslog message, send an SNMP trap to inform the administrator, and automatically disable the port.

Figure 17-5 on page 9 illustrates how bursty traffic is clipped above the assigned threshold with rate limiting applied.



**Figure 17-5 Rate Limiting Clipping Behavior**

## Flood Control

CoS-based flood control is a form of rate limiting that prevents configured ports from being disrupted by a traffic storm, by rate limiting specific types of packets through those ports. When flood control is enabled on a port, incoming traffic is monitored over one second intervals. During an interval, the incoming traffic rate for each configured traffic type (unknown unicast, broadcast, or multicast) is compared with the configured traffic flood control rate, specified in packets per second. If, during a one second interval, the incoming traffic of a configured type reaches the traffic flood control rate configured on the port, CoS-based flood control drops the traffic until the interval ends. Packets are then allowed to flow again until the limit is again reached.

## CoS Hardware Resource Configuration

This section provides a configuration example for each CoS hardware resource.

### IRL Configuration

Inbound rate limiters (IRL) allow you to configure a port to prevent the port from processing traffic above a certain threshold. In this example, we are going to configure port group **1.0**, ports **ge.1.3**, **ge.1.4** and **ge.1.5**, to discard packets it receives when the packet maps to CoS Index 1 (802.1 priority 1) and the threshold goes above 10,000 kilobits per second.

The remainder of this section details an IRL configuration that:

- Specifies the port group
- Assigns ports to the port group
- Maps the rate limiter data unit and rate to the IRL rate limiter
- Maps the rate limiter to the IRL reference
- Maps the IRL reference to the CoS setting (802.1 priority)
- Enables CoS
- Provides related show command displays

### CoS Port Configuration Layer

For the CoS port configuration layer, use the **set cos port-config irl** command to assign ports to port group 1.0 for the IRL configuration:

```
System(su)->set cos port-config irl 1.0 ports ge.1.3-5
```

## CoS Port Resource Layer

For the CoS port resource layer, use the **set cos port-resource irl** command to set the kilobits per second rate to 1000 and enable Syslog for this IRL port group 1.0 mapped to IRL resource 0:

```
System(su)->set cos port-resource irl 1.0 0 unit kbps rate 1000 syslog enable
```

## CoS Reference Layer

For the CoS reference layer, using the **set cos reference irl** command, map IRL reference 0 to rate-limit 0 for port group 1.0:

```
System(su)->set cos reference irl 1.0 0 rate-limit 0
```

## CoS Settings Layer

For the CoS settings layer, using the **cos settings** command, map IRL reference 0 to CoS settings 1 (802.1 priority 1):

```
System(su)->set cos settings 1 irl-reference 0
```

## Enable CoS State

CoS configuration must be enabled to become active, using the **set cos state enable** command:

```
System(su)->set cos state enable
```

## IRL Configuration Example Show Command Output

Use the **show cos settings** command to display the IRL resource reference to priority, to CoS index mapping:

```
System(su)->show cos settings
```

| CoS Index | Priority | ToS | IRL | flood-ctrl |
|-----------|----------|-----|-----|------------|
| 0         | 0        | *   | *   | enabled    |
| 1         | 1        | *   | 0   | enabled    |
| 2         | 2        | *   | *   | enabled    |
| 3         | 3        | *   | *   | enabled    |
| 4         | 4        | *   | *   | enabled    |
| 5         | 5        | *   | *   | enabled    |
| 6         | 6        | *   | *   | enabled    |
| 7         | 7        | *   | *   | enabled    |

Use the **show cos reference irl** command for port group 1.0 to display the CoS reference to rate limiter mapping:

```
System(su)->show cos reference irl 1.0
```

| Group | Index | Reference | Type | Rate Limiter |
|-------|-------|-----------|------|--------------|
| 1.0   | 0     | irl       | 0    |              |
| 1.0   | 1     | irl       | none |              |
| 1.0   | 2     | irl       | none |              |
| 1.0   | 3     | irl       | none |              |



```

1.0 4 irl none
1.0 5 irl none
1.0 6 irl none
1.0 7 irl none
1.0 8 irl none
1.0 9 irl none
1.0 10 irl none
...
...
1.0 95 irl none
1.0 96 irl none
1.0 97 irl none
1.0 98 irl none
1.0 99 irl none

```

Use the **show cos port-resource irl** command to display the data rate and unit of the rate limiter for port **1.0**:

```
System(su)->show cos port-resource irl 1.0
```

'?' after the rate value indicates an invalid rate value

| Group | Index | Resource | Type | Unit | Rate | Rate Limit | Type | Action |
|-------|-------|----------|------|------|------|------------|------|--------|
| 1.0   | 0     | irl      | kbps | 1000 |      | drop       |      | syslog |
| 1.0   | 1     | irl      | kbps | 0    |      | drop       |      | none   |
| 1.0   | 2     | irl      | kbps | 0    |      | drop       |      | none   |
| 1.0   | 3     | irl      | kbps | 0    |      | drop       |      | none   |
| 1.0   | 4     | irl      | kbps | 0    |      | drop       |      | none   |
| 1.0   | 5     | irl      | kbps | 0    |      | drop       |      | none   |
| 1.0   | 6     | irl      | kbps | 0    |      | drop       |      | none   |
| 1.0   | 7     | irl      | kbps | 0    |      | drop       |      | none   |
| 1.0   | 8     | irl      | kbps | 0    |      | drop       |      | none   |
| 1.0   | 9     | irl      | kbps | 0    |      | drop       |      | none   |
| 1.0   | 10    | irl      | kbps | 0    |      | drop       |      | none   |
| ...   |       |          |      |      |      |            |      |        |
| ...   |       |          |      |      |      |            |      |        |
| 1.0   | 95    | irl      | kbps | 0    |      | drop       |      | none   |
| 1.0   | 96    | irl      | kbps | 0    |      | drop       |      | none   |
| 1.0   | 97    | irl      | kbps | 0    |      | drop       |      | none   |
| 1.0   | 98    | irl      | kbps | 0    |      | drop       |      | none   |
| 1.0   | 99    | irl      | kbps | 0    |      | drop       |      | none   |

Use the **show cos port-config irl** command to display the port group name and assigned ports for port group **1.0**:

```
System(su)->show cos port-config irl 1.0
```

## Inbound Rate Limiting Port Configuration Entries

```

Port Group Name :
Port Group :1
Port Type :0
Assigned Ports :ge.1.3-5

```

## Flood Control Configuration

Flood control (flood-ctrl) provides for the configuration of a rate limiter to limit the amount of unknown unicast, multicast or broadcast packets a port receives from egressing all other ports. In this example, port ge.1.3 will be configured to limit the reception of unknown unicast packets on CoS Index 3 (802.1 priority 3) to a threshold of 3,000 packets per second.

### CoS Port Configuration Layer

For the CoS port configuration layer, use the **set cos port-config flood-ctrl** command to assign ports to port group 1.0 for the flood control configuration:

```
System(su)->set cos port-config flood-ctrl 1.0 ports ge.1.3 append
```

### CoS Port Resource Layer

For the CoS port resource layer, use the **set cos port-resource flood-ctrl** command to set the packets-per-second rate to 3,000 packets, for this flood control port group 1.0:

```
System(su)->set cos port-resource flood-ctrl 1.0 unicast rate 3000
```

### CoS Reference Layer

The CoS reference layer is not applicable to flood control.

### CoS Settings Layer

The CoS settings layer is not applicable to flood control.

### Enable CoS State

CoS configuration must be enabled to become active, using the **set cos state enable** command:

```
System(su)->set cos state enable
```

### Flood Control Configuration Example Show Command Output

Use the **show cos settings** command to display the flood control state to CoS index (802.1 priority) mapping:

```
System(su)->show cos settings
```

| CoS Index | Priority | ToS | IRL | flood-ctrl |
|-----------|----------|-----|-----|------------|
| 0         | 0        | *   | *   | enabled    |
| 1         | 1        | *   | 0   | enabled    |
| 2         | 2        | *   | *   | enabled    |
| 3         | 3        | *   | *   | enabled    |

|   |   |   |   |         |
|---|---|---|---|---------|
| 4 | 4 | * | * | enabled |
| 5 | 5 | * | * | enabled |
| 6 | 6 | * | * | enabled |
| 7 | 7 | * | * | enabled |

Use the **show cos port-resource flood-ctrl** command to display the flood control unit and rate to flood control resource mapping:

```
System(su)->show cos port-resource flood-ctrl 1.0
```

'?' after the rate value indicates an invalid rate value

| Group Index | Resource | Type       | Unit | Rate    | Rate Limit type | Action |
|-------------|----------|------------|------|---------|-----------------|--------|
| 1.0         | ucast    | flood-ctrl | pps  | 3000    | drop            | none   |
| 1.0         | mcast    | flood-ctrl | pps  | disable | drop            | none   |
| 1.0         | bcast    | flood-ctrl | pps  | disable | drop            | none   |

Use the **show cos port-config flood-ctrl** command to display the port group name and assigned ports for port group 1.0.

```
System(su)->show cos port-config flood-ctrl 1.0
```

```
Flood control Port Configuration Entries
```

```

Port Group Name :
Port Group :1
Port Type :0
Assigned Ports :ge.1.3

```

## Enabling CoS State

CoS state is a global setting that must be enabled for CoS configurations to be applied to a port. When CoS state is enabled, controls configured for CoS supersede port level controls for priority queue mapping and IRL. These port level settings can be configured independent of CoS state, but will have no affect while CoS is enabled. Disabling CoS results in the restoration of current port level settings.

Use the **set cos state enable** command to enable CoS state globally for this system.

Use the **set cos state disable** command to disable CoS state globally for this system.

Use the **show cos state** command to display the current status of CoS state.

## The QoS CLI Command Flow

[Procedure 17-1](#) provides a CLI flow summary of each step in the configuration flow along with the show commands to verify the configuration.

### Procedure 17-1 Class of Service CLI Configuration Command Summary

| Step | Task                                                                                                                                                                                                                                                                                                                              | Command(s)                                                                                                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Inspect both the TxQs and IRL support for the installed ports. This information is used to determine the module port type for port group.                                                                                                                                                                                         | <b>show cos port-type irl</b><br><b>show cos port-type flood-ctrl</b>                                                                                                                                                                                                                                                  |
| 2.   | Set the CoS inbound rate-limit port group configuration by mapping a physical port list to a port group for purposes of IRL configuration, optionally allowing the association of a name for this configuration. Verify the new configuration.                                                                                    | <b>set cos port-config irl</b> <i>port_group.port_type</i><br><b>name</b> <i>name</i> <b>ports</b> <i>ports_list</i><br><b>show cos port-config irl</b>                                                                                                                                                                |
| 3.   | Set the CoS flood control limit port group configuration by mapping a physical port list to a port group for purposes of flood control configuration, optionally allowing the association of a name for this configuration. Verify the new configuration.                                                                         | <b>set cos port-config flood-ctrl</b><br><i>port_group.port_type</i> <b>name</b> <i>name</i> <b>ports</b><br><i>ports_list</i><br><b>show cos port-config flood-ctrl</b>                                                                                                                                               |
| 4.   | Configure a CoS inbound rate limiting index entry, by mapping a port group with a rate-limit value, along with the ability to optionally set syslog, trap, and/or disable port behaviors should the limit be exceeded. This index is used by the rate-limit option when setting an IRL cos reference.                             | <b>set cos port-resource irl</b> <i>port_group.port_type</i><br><i>index</i> <b>unit</b> <i>unit</i> <b>rate</b> <i>rate</i> <b>syslog</b> <i>setting</i> <b>trap</b><br><i>setting</i> <b>disable-port</b> <i>setting</i><br><b>show cos port-resource irl</b><br><i>port_group.port_type</i>                         |
| 5.   | Configure a CoS flood control index entry, by mapping a port group with a traffic type such as multicast or broadcast, along with the ability to optionally set syslog, trap, and/or disable port behaviors should the limit be exceeded. This index is used by the rate-limit option when setting a flood control cos reference. | <b>set cos port-resource flood-ctrl</b><br><i>port_group.port_type</i> <i>traffic-type</i> <b>unit</b> <i>unit</i> <b>rate</b><br><i>rate</i> <b>syslog</b> <i>setting</i> <b>trap</b> <i>setting</i> <b>disable-port</b><br><i>setting</i><br><b>show cos port-resource flood-ctrl</b><br><i>port_group.port_type</i> |
| 6.   | Set a CoS inbound rate limiting reference configuration, by mapping a port group with a rate limiter resource ID and associating the mapping with an IRL reference. Verify the new CoS reference configuration.                                                                                                                   | <b>set cos reference irl</b> <i>port_group.port_type</i><br><i>reference</i> <b>rate-limit</b> <i>IRLreference</i><br><b>show cos reference irl</b> <i>port_group.port_type</i>                                                                                                                                        |
| 7.   | Modify a currently configured CoS or create a new CoS. Verify the new CoS configuration. All IRL to port group mappings are associated with the inbound rate limiter reference.                                                                                                                                                   | <b>set cos settings</b> <i>cos-list</i> [ <b>priority</b> <i>priority</i> ] [ <b>tos-</b><br><b>value</b> <i>tos-value</i> ] [ <b>irl-reference</b> <i>irl-reference</i> ]<br><b>show cos settings</b>                                                                                                                 |
| 8.   | Enable CoS state for the system. Verify the new CoS state.                                                                                                                                                                                                                                                                        | <b>set cos state enable</b><br><b>show cos state</b>                                                                                                                                                                                                                                                                   |
| 9.   | For IRL, associate the CoS with a policy profile.                                                                                                                                                                                                                                                                                 | <b>set policy profile</b> <i>profile-index</i> <b>cos-status</b><br><b>enable cos</b> <i>cos-num</i>                                                                                                                                                                                                                   |

## Port Priority and Transmit Queue Configuration

The fixed switch devices allow you to assign mission-critical data to higher priority through the device by delaying less critical traffic during periods of congestion. The higher priority traffic through the device is serviced first before lower priority traffic. The Class of Service capability of the device is implemented by a priority queuing mechanism. Class of Service is based on the IEEE 802.1D (802.1p) standard specification, and allows you to define eight priorities (0 through 7) and assign them to transmit queues for each port.

A priority 0 through 7 can be set on each port, with 0 being the lowest priority. A port receiving a frame without priority information in its tag header is assigned a priority according to the default priority setting on the port.

You can also map frame priorities to transmit queues, which allows you to configure which transmit queue will be used for frames with specific priorities.

The arbitration methods used by transmit queues can be configured with the **set port txq** command.



**Note:** When CoS override is enabled using the **set policy profile** command, CoS-based classification rules will take precedence over priority settings configured with the **set port priority** command described in this section.

### Setting Port Priority

Use the **set port priority** command to set the 802.1D (802.1p) Class-of-Service transmit priority (0 through 7) on each port. A port receiving a frame without priority information in its tag header is assigned a priority according to the priority setting on the port. For example, if the priority of a port is set to 5, the frames received through that port without a priority indicated in their tag header are classified as a priority 5 and transmitted according to that priority. .

A frame with priority information in its tag header is transmitted according to that priority.

#### Example

This example sets the 802.1p port priority to 4 on ports ge.1.1 through ge.1.3, then shows the current settings.

```
System(su)->set port priority ge.1.1-3 4
```

```
System(su)->show port priority ge.1.1-3
```

```
ge.1.1 is set to 4
```

```
ge.1.2 is set to 4
```

```
ge.1.3 is set to 4
```

### Mapping Port Priority to Transmit Queues

The **set port priority-queue** command enables you to map a transmit queue (0 to 5, with 0 being the lowest priority queue) for each port priority of the selected port. You can apply the new settings to one or more ports. Although ports have 8 queues, only queues 0 through 5 may be configured. Queues 6 and 7 are reserved for management traffic.



**Note:** Priority to transmit queue mapping on an individual port basis can only be configured on Gigabit Ethernet ports (ge.x.x) and LAG ports (lag.0.x). On switches that provide Fast Ethernet ports, when you use the **set port priority-queue** command to configure a Fast Ethernet port (fe.x.x), the mapping values are applied globally to all Fast Ethernet ports on the system.

The default mappings are shown in the following example:

```
System(su)->show port priority-queue ge.1.1
Port P0 P1 P2 P3 P4 P5 P6 P7

ge.1.1 1 0 0 2 3 4 5 5
```

The following table describes the default mappings shown in the output above:

| Frames with priority ... | Are mapped to transmit queue ... |
|--------------------------|----------------------------------|
| 0                        | 1                                |
| 1                        | 0                                |
| 2                        | 0                                |
| 3                        | 2                                |
| 4                        | 3                                |
| 5                        | 4                                |
| 6                        | 5                                |
| 7                        | 5                                |

Use the **clear port priority-queue** command to return mappings to the default values.

### Example

This example maps priority 4 frames received on port ge.1.1 to transmit queue 4, then shows the current settings for the port.

```
System(su)->set port priority-queue ge.1.1 4 4
System(su)->show port priority-queue ge.1.1
Port P0 P1 P2 P3 P4 P5 P6 P7

ge.1.1 1 0 0 2 4 4 5 5
```

## Setting Transmit Queue Arbitration

You can use the **set port txq command** to set QoS transmit queue arbitration values for queues 0 through 5 on physical ports. Queues can be configured for Weighted Round Robin (WRR) or strict priority (SP) or a combination of both (hybrid). Transmit queue arbitration methods are described in [“Preferential Queue Treatment for Packet Forwarding”](#) on page 17-6.

Eight transmit queues are implemented in the switch hardware for each port. You can set the priority mode and weight for each of the available queues (0 through 5) for each physical port on the switch.

Priority queues 6 and 7 are reserved for stacking and control protocols and are run in strict priority. They cannot be modified by the **set port txq** or **clear port txq** commands. Their settings are displayed by the **show port txq** command.

Queues 0 through 5 can be set for strict priority (SP) or weighted round-robin (WRR), or a combination of both.

When configured for WRR, weights must total 100 percent. Strict priority may be assigned to all queues by setting *value5* to 100 percent. When combining SP and WRR, the values of those ports running in WRR must total 100 percent.

You can mix WRR and SP by assigning SP to the higher numbered queues and assigning WRR to the lower numbered queues, making sure that the values assigned to the WRR queues totals 100 percent. For example, you could assign WRR to queues 0 through 4 by assigning 20 percent to each of those queues, and then setting queue 5 to SP.



**Note:** Priority mode and weight cannot be configured on LAGs, only on the physical ports that make up the LAG.

## Examples

This example shows how to change the arbitration values for the queues belonging to ge.1.1 to Strict Priority. Note that, although you can't set queues 6 and 7 with this command, their values are shown by the **show port txq** command.

```
System(su)->set port txq ge.1.1 0 0 0 0 0 100
```

```
System(su)->show port txq ge.1.1
Port Alg Q0 Q1 Q2 Q3 Q4 Q5 Q6 Q7
----- --- --- --- --- --- --- --- ---
ge.1.1 STR SP SP SP SP SP SP SP SP
```

This example shows how to change the arbitration values for the queues belonging to ge.1.1 to WRR:

```
System(su)->set port txq ge.1.1 10 10 20 20 20 20
```

```
System(su)->show port txq ge.1.1
Port Alg Q0 Q1 Q2 Q3 Q4 Q5 Q6 Q7
----- --- --- --- --- --- --- --- ---
ge.1.1 WRR 10 10 20 20 20 20 SP SP
```

This example shows how to change the arbitration values for the queues belonging to ge.1.1 to WRR with SP:

```
System(su)->set port txq ge.1.1 10 10 20 20 40 SP
```

```
System(su)->show port txq ge.1.1
Port Alg Q0 Q1 Q2 Q3 Q4 Q5 Q6 Q7
----- --- --- --- --- --- --- --- ---
ge.1.1 WRR 10 10 20 20 40 SP SP SP
```

## Port Traffic Rate Limiting



**Note:** This feature applies to the A4 fixed switches only.

Use the **set port ratelimit** command to limit the rate of inbound traffic on the A4 device on a per port/priority basis. The allowable range for the rate limiting is 64 kilobytes per second minimum up to the maximum transmission rate allowable on the interface type.

Rate limit is configured for a given port and list of priorities. The list of priorities can include one, some, or all of the eight 802.1p priority levels. Once configured, the rate of all traffic entering the port with the priorities configured to that port is not allowed to exceed the programmed limit. If the rate exceeds the programmed limit, frames are dropped until the rate falls below the limit.

Rate limiting is disabled by default, both globally and per port.

When a CoS is configured with an inbound rate limiter (IRL), and that IRL CoS is configured as part of a policy profile using the **set policy profile** command, CoS-based inbound rate limiting will take precedence over port rate limits set with **set port ratelimit**.

## Examples

This example displays the current ratelimit configuration on port fe.1.1.

```
System(su)->show port ratelimit fe.1.1
Global Ratelimiting status is disabled.
```

| Port Number | Index | Threshold (KBytes) | Action  | Direction | Priority List | Status   |
|-------------|-------|--------------------|---------|-----------|---------------|----------|
| fe.1.1      | 1     | 64                 | discard | inbound   | 0-3           | disabled |
| fe.1.1      | 2     | 64                 | discard | inbound   | 4-7           | disabled |

This example globally enables rate limiting and then configures rate limiting for inbound traffic on port fe.1.1, index 1, priority 0-3, to a threshold of 125 kilobytes per second.

```
System(su)->set port ratelimit enable
System(su)->set port ratelimit fe.1.1 0-3 125 enable inbound 1
```

```
System(su)->show port ratelimit fe.1.1
Global Ratelimiting status is enabled.
```

| Port Number | Index | Threshold (KBytes) | Action  | Direction | Priority List | Status   |
|-------------|-------|--------------------|---------|-----------|---------------|----------|
| fe.1.1      | 1     | 125                | discard | inbound   | 0-3           | enabled  |
| fe.1.1      | 2     | 64                 | discard | inbound   | 4-7           | disabled |

This example returns rate limit parameters for port fe.1.1 to their default values.

```
System(su)->clear port ratelimit fe.1.1
System(su)->show port ratelimit fe.1.1
Global Ratelimiting status is enabled.
```

| Port Number | Index | Threshold (KBytes) | Action  | Direction | Priority List | Status   |
|-------------|-------|--------------------|---------|-----------|---------------|----------|
| fe.1.1      | 1     | 64                 | discard | inbound   | 0-3           | disabled |
| fe.1.1      | 2     | 64                 | discard | inbound   | 4-7           | disabled |



## Configuring Network Monitoring

This chapter describes network monitoring features on the Fixed Switches and their configuration.

| For information about...                          | Refer to page... |
|---------------------------------------------------|------------------|
| <a href="#">Basic Network Monitoring Features</a> | 18-1             |
| <a href="#">RMON</a>                              | 18-5             |
| <a href="#">sFlow</a>                             | 18-9             |

### Basic Network Monitoring Features

#### Console/Telnet History Buffer

The history buffer lets you recall your previous CLI input. The size of the history buffer determines how many lines of previous CLI input are available for recall. By default, the size of this buffer is 20 lines. The configured size can be displayed. The contents of the buffer can be displayed.

To change the size of the history buffer, use the **set history** command, specifying the size of the history buffer. The **default** option configures the specified history buffer setting to persist for all future sessions. Otherwise, the setting only affects this session.

This example shows how to set the size of the command history buffer to 25 lines and make this the default setting:

```
C5(rw)->set history 25 default
```

Use the **show history** command to display the currently configured size of the history buffer.

```
C5(rw)->show history
History size currently set to: 25
C5(rw)->
```

Use the **history** command to display the contents of the history buffer.

```
C5(rw)->history
 1 history
 2 show gvrp
 3 show vlan
 4 show igmp
C5(rw)->
```

## Network Diagnostics

Fixed Switch network diagnostics provide for:

- Pinging another node on the network to determine its availability
- Performing a traceroute through the IP network to display a hop-by-hop path from the device to a specific destination host

Use the **ping** command, in switch mode or in router privileged exec mode, to determine whether the specified node is available.

```
C5(rw)->ping 10.10.10.1
10.10.10.1 is alive
```

Use the **traceroute** command, in switch mode or in router privileged exec mode, to display a hop-by-hop path through an IP network from the device to a specific destination host. The command in switch mode provides more optional parameters than the command in router mode. Refer to the *CLI Reference* for your platform for details.

```
C5(rw)->traceroute 192.167.252.17
Traceroute to 192.167.252.17, 30 hops max, 40 byte packets
 1 192.167.201.40 20.000 ms 20.000 ms 20.000 ms
 2 14.1.0.45 40.000 ms 10.000 ms 20.000 ms
 3 192.167.252.17 50.000 ms 0.000 ms 20.000 ms
```

## Switch Connection Statistics

Switch connection statistics can be displayed for:

- ICMP
- IP
- TCP
- UDP

Use the **show netstat** command to display switch connection statistics. Use the **stats** option to display statistics for all supported protocols.

The following example displays just the ICMP statistics.

```
C5(su)->show netstat icmp
ICMP:
 89 IPv4 messages received
 26 IPv4 echo requests received
 45 IPv4 destination unreachable messages received
 0 IPv4 destination unreachable messages received and socket found
 45 IPv4 destination unreachable messages received and socket not found
 0 IPv4 destination unreachable messages received with bad header code
 0 IPv4 messages with hdrsize less than min hdrsize
 0 IPv4 messages with bad checksum
 0 IPv4 messages with hdrsize type unreachable or time exceeded
 53 IPv4 messages sent
 0 IPv4 messages not sent due to no memory available

 0 IPv6 messages received
 0 IPv6 messages received with error
 0 IPv6 messages received with bad checksum
 0 IPv6 messages dropped due to no memory available
 0 IPv6 messages not sent due to no memory available
```

## Users

You can display information about the active console port or Telnet session(s) logged in to the switch. You can also close an active console port or Telnet session from the switch CLI.

Use the **show users** command to display information for active console port or Telnet sessions on the switch. Use the **disconnect** command to close a console or Telnet session.

```
C5(rw)->show users
 Session User Location
 ----- -
* console admin console (via com.1.1)
 telnet rw 134.141.192.18
C5(rw)->disconnect 134.141.192.18
An active telnet session is closed.
```

## RMON

RMON (Remote Network Monitoring) is an industry standard specification that provides comprehensive network fault diagnosis, planning, and performance tuning information and allows for interoperability between SNMP management stations and monitoring agents. RMON extends the SNMP MIB capability by defining additional MIBs that generate a much richer set of data about network usage. These MIB “groups” each gather specific sets of data to meet common network monitoring requirements.

Table 18-1 lists:

- The RMON monitoring groups supported on Fixed Switch devices
- Each group’s function
- The elements it monitors
- The group’s associated commands

**Table 18-1 RMON Monitoring Group Functions and Commands**

| RMON Group | What It Does...                                                                                                                                                                                     | What It Monitors...                                                                                                                                                              | CLI Command(s)                                                                                                        |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Statistics | Records statistics measured by the RMON probe for each monitored interface on the device.                                                                                                           | Packets dropped, packets sent, bytes sent (octets), broadcast and multicast packets, CRC errors, oversized and undersized packets, fragments, jabbers, and counters for packets. | <b>show rmon stats</b><br><b>set rmon stats</b><br><b>clear rmon stats</b>                                            |
| History    | Records periodic statistical samples from a network.                                                                                                                                                | Sample period, number of samples and item(s) sampled.                                                                                                                            | <b>show rmon history</b><br><b>set rmon history</b><br><b>clear rmon history</b>                                      |
| Alarm      | Periodically gathers statistical samples from variables in the probe and compares them with previously configured thresholds. If the monitored variable crosses a threshold, an event is generated. | Alarm type, interval, starting threshold, stop threshold.                                                                                                                        | <b>show rmon alarm</b><br><b>set rmon alarm properties</b><br><b>set rmon alarm status</b><br><b>clear rmon alarm</b> |

**Table 18-1 RMON Monitoring Group Functions and Commands (continued)**

| <b>RMON Group</b> | <b>What It Does...</b>                                                                                                                                  | <b>What It Monitors...</b>                         | <b>CLI Command(s)</b>                                                                                                                                             |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Event             | Controls the generation and notification of events from the device.                                                                                     | Event type, description, last time event was sent. | <b>show rmon event</b><br><b>set rmon event properties</b><br><b>set rmon event status</b><br><b>clear rmon event</b>                                             |
| Filter            | Allows packets to be matched by a filter definition. These matched packets form a data stream or “channel” that may be captured or may generate events. | Packets matching the filter definition.            | <b>show rmon channel</b><br><b>set rmon channel</b><br><b>clear rmon channel</b><br><b>show rmon filter</b><br><b>set rmon filter</b><br><b>clear rmon filter</b> |
| Packet Capture    | Allows packets to be captured upon a filter match.                                                                                                      | Packets matching the filter definition.            | <b>show rmon capture</b><br><b>set rmon capture</b><br><b>clear rmon capture</b>                                                                                  |

## RMON Design Considerations

The Fixed Switch devices support RMON Packet Capture/Filter Sampling through both the CLI and MIBs, but with the following constraints:

- RMON Packet Capture/Filter Sampling and Port Mirroring cannot be enabled on the same interface concurrently.
- You can capture a total of 100 packets on an interface, no more and no less.
  - The captured frames will be as close to sequential as the hardware will allow.
  - Only one interface can be configured for capturing at a time.
  - Once 100 frames have been captured by the hardware, the application will stop without manual intervention.
- As described in the MIB, the filter is only applied after the frame is captured, thus only a subset of the frames captured will be available for display.
- There is only one Buffer Control Entry supported.
- Due to the limitations of the hardware, the Buffer Control Entry table will have limits on a few of its elements:
  - MaxOctetsRequested can only be set to the value -1 which indicates the application will capture as many packets as possible given its restrictions.
  - CaptureSliceSize can only be set to 1518.
  - The Full Action element can only be set to “lock” since the device does not support wrapping the capture buffer.
- Due to hardware limitations, the only frame error counted is oversized frames.
- The application does not support Events. Therefore, the following elements of the Channel Entry Table are not supported: TurnOnEventIndex, TurnOffEventIndex, EventIndex, and EventStatus.
- There is only one Channel Entry available at a time.

- There are only three Filter Entries available, and a user can associate all three Filter Entries with the Channel Entry.
- Configured channel, filter, and buffer information will be saved across resets, but not frames within the capture buffer.

## Configuring RMON

This section provides details for the configuration of RMON on the Fixed Switch products.

[Table 18-2](#) lists RMON parameters and their default values.

**Table 18-2 Default RMON Parameters**

| Parameter            | Description                                                                        | Default Value                                |
|----------------------|------------------------------------------------------------------------------------|----------------------------------------------|
| buckets              | The number of RMON history entries to maintain.                                    | 50 entries                                   |
| interval             | The period between RMON history or alarm sampling.                                 | history = 30 seconds<br>alarm = 3600 seconds |
| owner                | The RMON management station entity for a statistics or alarm context.              | monitor                                      |
| type                 | The RMON alarm monitoring method or property or RMON event.                        | alarm = absolute<br>event = none             |
| startup              | The RMON alarm type generated when an event is first enabled.                      | rising                                       |
| rthresh              | The RMON minimum threshold for causing a rising alarm.                             | 0 events                                     |
| fthresh              | The RMON maximum threshold for causing a falling alarm.                            | 0 events                                     |
| revent               | The RMON index event number to be triggered when the rising threshold is crossed.  | 0                                            |
| fevent               | The RMON index event number to be triggered when the falling threshold is crossed. | 0                                            |
| alarm, event status  | Whether an entry is enabled or disabled.                                           | disabled                                     |
| channel action       | The RMON channel entry action.                                                     | packets are accepted on filter matches       |
| channel control      | The RMON channel flow of data control state.                                       | off                                          |
| channel event status | The event to be triggered when the channel is on and a packet is accepted.         | ready                                        |
| channel description  | A user configured description of the channel.                                      | none.                                        |
| capture action       | The RMON capture entry action when the buffer is full.                             | lock                                         |
| capture offset       | The RMON capture first octet from each packet to retrieve.                         | 0                                            |

**Table 18-2 Default RMON Parameters (continued)**

| Parameter        | Description                                                                                  | Default Value                           |
|------------------|----------------------------------------------------------------------------------------------|-----------------------------------------|
| capture asksize  | The RMON capture requested maximum octets to save in the buffer.                             | -1 (request as many octets as possible) |
| capture slice    | The RMON capture maximum number of octets from each packet to be saved to the buffer.        | 1518                                    |
| capture loadsize | The RMON capture maximum number of octets from each packet to be downloaded from the buffer. | 100                                     |

Procedure 18-1 describes how to configure RMON. Refer to “RMON Design Considerations” on page 18-4 before configuring RMON on the Fixed Switches.

**Procedure 18-1 Configuring Remote Network Monitoring**

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Command(s)                                                                                                                                                                                                                       |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | <p>Configure RMON to create entries that record statistics measured by the RMON probe for each specified interface.</p> <ul style="list-style-type: none"> <li><i>index</i> - Specifies the index number for this entry</li> <li><i>port-string</i> - assigns this entry to a specific port</li> <li><b>owner</b> - (Optional) Specifies the management station owner for this entry</li> </ul>                                                                                                                                                                 | <pre>set rmon stats index port-string [owner]</pre>                                                                                                                                                                              |
| 2.   | <p>Optionally, specify the maximum number and period for recorded statistical samples from a network.</p> <ul style="list-style-type: none"> <li><i>index</i> - Specifies the index number for this entry</li> <li><i>port-string</i> - assigns this entry to a specific port</li> <li><b>bucket</b> - (Optional) Specifies the maximum number of entries to maintain</li> <li><b>interval</b> - (Optional) Specifies the period between samples in seconds</li> <li><b>owner</b> - (Optional) Specifies the management station owner for this entry</li> </ul> | <pre>set rmon history index [port-string] [buckets buckets] [interval interval] [owner owner]</pre>                                                                                                                              |
| 3.   | <p>Configure RMON probe variable thresholds that will trigger an alarm if crossed by a sampled probe.</p> <ul style="list-style-type: none"> <li><i>index</i> - Specifies the entry for this set of alarm properties</li> <li><b>interval</b> - (Optional) Specifies the period between samples in seconds</li> <li><b>object</b> - (Optional) Specifies the MIB object to be monitored</li> <li><b>type</b> - (Optional) Specifies a monitoring method</li> </ul>                                                                                              | <pre>set rmon alarm properties index [interval interval] [object object] [type {absolute   delta}] [startup {rising   falling   either}] [rthresh rthresh] [fthresh fthresh] [revent revent] [fevent fevent] [owner owner]</pre> |

---

**Procedure 18-1 Configuring Remote Network Monitoring (continued)**

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Command(s)                                                                                                                                                                                                                                                         |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <ul style="list-style-type: none"> <li>• <b>startup</b> - (Optional) Specifies the alarm type generated when this event is first enabled</li> <li>• <b>rthresh</b> - (Optional) Specifies the minimum threshold that will cause a rising alarm</li> <li>• <b>fthresh</b> - (Optional) Specifies the minimum threshold that will cause a falling alarm</li> <li>• <b>revent</b> - (Optional) Specifies the index number of the RMON event to be triggered when the rising threshold is crossed</li> <li>• <b>fevent</b> - (Optional) Specifies the index number of the RMON event to be triggered when the falling threshold is crossed</li> <li>• <b>owner</b> - (Optional) Specifies the management station owner for this entry</li> </ul> |                                                                                                                                                                                                                                                                    |
| 4.   | Enable a configured alarm entry.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <b>set rmon alarm status <i>index</i> enable</b>                                                                                                                                                                                                                   |
| 5.   | Configure RMON probe variable thresholds that will trigger an event if crossed by a sampled probe. <ul style="list-style-type: none"> <li>• <i>index</i> - Specifies the entry for this set of event properties</li> <li>• <b>description</b> - (Optional) Specifies a text string description for this event</li> <li>• <b>type</b> - (Optional) Specifies the event notification type for this entry</li> <li>• <b>community</b> - (Optional) Specifies an SNMP community name to use if the message type is set to trap</li> <li>• <b>owner</b> - (Optional) Specifies the management station owner for this entry</li> </ul>                                                                                                             | <b>set rmon event properties <i>index</i></b><br><b>[<i>description</i> <i>description</i>] [<i>type</i></b><br><b>{<i>none</i>   <i>log</i>   <i>trap</i>   <i>both</i>}]</b><br><b>[<i>community</i> <i>community</i>] [<i>owner</i></b><br><b><i>owner</i>]</b> |
| 6.   | Enable a configured event entry.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <b>set rmon event status <i>index</i> enable</b>                                                                                                                                                                                                                   |
| 7.   | Configure an RMON channel entry to match packets by a filter equation. <ul style="list-style-type: none"> <li>• <i>index</i> - Specifies the entry value for this channel entry</li> <li>• <i>port-string</i> - Specifies the port on which RMON will monitor traffic</li> <li>• <b>accept</b> - (Optional) Specifies the filters action for this entry</li> <li>• <b>control</b> - (Optional) Enables or disables control of the flow of data through this channel</li> <li>• <b>description</b> - (Optional) Specifies a description for this channel</li> <li>• <i>owner</i> - (Optional) Specifies the management station owner for this entry</li> </ul>                                                                                | <b>set rmon channel <i>index</i> <i>port-string</i></b><br><b>[<i>accept</i> {<i>matched</i>   <i>failed</i>}]</b><br><b>[<i>control</i> {<i>on</i>   <i>off</i>}] [<i>description</i></b><br><b><i>description</i>] [<i>owner</i> <i>owner</i>]</b>               |

---

### Procedure 18-1 Configuring Remote Network Monitoring (continued)

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Command(s)                                                                                                                                                                   |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.   | <p>Configure an RMON filter entry.</p> <ul style="list-style-type: none"> <li><i>index</i> - Specifies the entry value for this filter entry</li> <li><i>port-string</i> - Specifies the channel on which RMON will monitor this filter entry</li> <li><b>offset</b> - Specifies the offset from the beginning of the packet to look for matches</li> <li><b>status</b> - (Optional) Specifies packet status bits that are to be matched</li> <li><b>smask</b> - (Optional) Specifies the mask applied to status to indicate which bits are significant</li> <li><b>snotmask</b> - (Optional) Specifies the inversion mask that indicates which bits should be set or not set</li> <li><b>data</b> - (Optional) Specifies the data to be matched</li> </ul>                                                                                                                                                                                                                                   | <pre>set rmon filter index channel_index [offset offset] [status status] [smask smask] [snotmask snotmask] [data data] [dmask dmask] [dnotmask dnotmask] [owner owner]</pre> |
|      | <ul style="list-style-type: none"> <li><b>dmask</b> - (Optional) Specifies the mask applied to data to indicate which bits are significant</li> <li><b>dnotmask</b> - (Optional) Specifies the inversion mask that indicates which bits should be set or not set</li> <li><i>owner</i> - (Optional) Specifies the management station owner for this entry</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                              |
| 9.   | <p>Configure RMON capture to capture packets upon a filter match.</p> <ul style="list-style-type: none"> <li><i>index</i> - Specifies an entry number for this capture entry</li> <li><i>channel</i> - Specifies the channel to which this capture entry will be applied</li> <li><b>action</b> - (Optional) Specifies buffer behavior when it is full</li> <li><b>slice</b> - (Optional) Specifies the maximum number of octets from each packet to be saved in a buffer. Currently must be 1518.</li> <li><b>loadsize</b> - (Optional) Specifies the maximum number of octets from each packet to be downloaded from the buffer</li> <li><b>offset</b> - (Optional) Specifies the number octets from each packet to be retrieved</li> <li><b>asksize</b> - (Optional) Specifies the maximum number of octets that will be saved in the buffer. Currently, must be -1.</li> <li><b>owner</b> - (Optional) Specifies the name of the management station that configured this entry</li> </ul> | <pre>set rmon capture index {channel [action {lock}] [slice 1518] [loadsize loadsize] [offset offset] [asksize -1] [owner owner]}</pre>                                      |



Table 18-3 describes how to manage remote network monitoring.

**Table 18-3 Managing RMON**

| Task                                                          | Command                                                              |
|---------------------------------------------------------------|----------------------------------------------------------------------|
| To delete one or more RMON statistics entries:                | <b>clear rmon stats</b> { <i>index</i>   <b>to-defaults</b> }        |
| To delete one or more RMON statistics entries:                | <b>clear rmon stats</b> { <i>index-list</i>   <b>to-defaults</b> }   |
| To delete one or more RMON history entries:                   | <b>clear rmon history</b> { <i>index-list</i>   <b>to-defaults</b> } |
| To delete an RMON alarm entry:                                | <b>clear rmon alarm</b> <i>index</i>                                 |
| To delete an RMON event entry and any associated log entries: | <b>clear rmon event</b> <i>index</i>                                 |
| To delete an RMON channel entry:                              | <b>clear rmon channel</b> <i>index</i>                               |
| To delete an RMON filter entry:                               | <b>clear rmon filter</b> <i>index</i>                                |
| To delete an rmon capture entry:                              | <b>clear rmon capture</b> <i>index</i>                               |

Table 18-4 describes how to display RMON information and statistics.

**Table 18-4 Displaying RMON Information and Statistics**

| Task                                                                   | Command                                                                 |
|------------------------------------------------------------------------|-------------------------------------------------------------------------|
| To display RMON statistics for one or more ports:                      | <b>show rmon stats</b> [ <i>port-string</i> ]                           |
| To display RMON history properties and statistics:                     | <b>show rmon history</b> [ <i>port-string</i> ]                         |
| To display RMON alarm entries:                                         | <b>show rmon alarm</b> [ <i>index</i> ]                                 |
| To display RMON event entry properties:                                | <b>show rmon event</b> [ <i>index</i> ]                                 |
| To display RMON channel entries for one or more ports:                 | <b>show rmon channel</b> [ <i>port-string</i> ]                         |
| To display one or more RMON filter entries                             | <b>show rmon filter</b> [ <i>index index</i>   <b>channel channel</b> ] |
| To display RMON capture entries and associated buffer control entries: | <b>show rmon capture</b> [ <i>index</i> ] [ <b>nodata</b> ]             |

## sFlow

sFlow is a method for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives visibility into network activity, enabling effective management and control of network resources.

An sFlow solution consists of an sFlow Agent, embedded in the network device such as a switch or router, and an sFlow Collector. The sFlow Agent uses sampling technology to capture traffic statistics from the device it is monitoring and immediately forwards the sampled traffic statistics to an sFlow Collector for analysis in sFlow datagrams.

The sFlow Agent uses two forms of sampling— statistical packet-based sampling of switched or routed Packet Flows, and time-based sampling of counters.

Version 5 of sFlow is described in detail in the document entitled “sFlow Version 5” available from sFlow.org (<http://www.sflow.org>).

## Using sFlow in Your Network

The advantages of using sFlow include:

- sFlow makes it possible to monitor ports of a switch, with no impact on the distributed switching performance. (See “[Overview](#)” on page 18-12 for more information.)
- sFlow requires very little memory or CPU usage. Samples are not aggregated into a flow-table on the switch — they are forwarded immediately over the network to the sFlow Collector.
- The system is tolerant to packet loss in the network. (The statistical model means loss is equivalent to a slight change in the sampling rate.)
- The sFlow Collector can receive data from multiple switches, providing a real-time synchronized view of the whole network.
- The sFlow Collector can analyze traffic patterns for whatever protocols are found in the packet headers (for example, TCP/IP, IPX, Ethernet, AppleTalk). There is no need for the layer 2 switch to decode and understand all protocols.

## Definitions

The following table describes some of the main sFlow terms and concepts.

**Table 18-5 sFlow Definitions**

| Term                 | Definition                                                                                                                                                                                                                                                       |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Source          | A Data Source refers to a location within a Network Device that can make traffic measurements. Possible Data Sources include interfaces and VLANs.                                                                                                               |
| Packet Flow          | A Packet Flow is defined as the path or trajectory that a packet takes through a Network Device (That is, the path that a packet takes as it is received on one interface, is subjected to a switching/routing decision, and is then sent on another interface). |
| Packet Flow Sampling | Packet Flow Sampling refers to the random selection of a fraction of the Packet Flows observed at a Data Source.                                                                                                                                                 |
| Sampling Rate        | The Sampling Rate specifies the ratio of packets observed at the Data Source to the samples generated.                                                                                                                                                           |
| Sampling Interval    | The time period between successive Counter Samples.                                                                                                                                                                                                              |
| sFlow Instance       | An sFlow Instance refers to a measurement process associated with a Data Source.                                                                                                                                                                                 |
| sFlow Agent          | The sFlow Agent provides an interface for configuring the sFlow Instances within a device.                                                                                                                                                                       |
| sFlow Collector      | An sFlow Collector receives sFlow Datagrams from one or more sFlow Agents. The sFlow Collector may also configure sFlow Instances using the configuration mechanisms provided by the sFlow Agent.                                                                |
| sFlow Datagram       | An sFlow Datagram is a UDP datagram that contains the measurement data, and information about the measurement source and process.                                                                                                                                |

## sFlow Agent Functionality

Packet flow sampling and counter sampling are performed by sFlow Instances associated with individual Data Sources within the sFlow Agent. Packet flow sampling and counter sampling are designed as part of an integrated system. Both types of samples are combined in sFlow datagrams. Packet flow sampling will cause a steady, but random, stream of sFlow datagrams to be sent to the sFlow Collector. Counter samples may be taken opportunistically in order to fill these datagrams.

In order to perform packet flow sampling, an sFlow Sampler Instance is configured with a sampling rate. The packet flow sampling process results in the generation of packet flow records. In order to perform counter sampling, an sFlow Poller Instance is configured with a polling interval. The counter sampling process results in the generation of counter records. The sFlow Agent collects counter records and packet flow records and sends them in the form of sFlow datagrams to sFlow Collectors.

## Sampling Mechanisms

Two forms of sampling are performed by the sFlow Agent: statistical packet-based sampling of switched or routed packet flows, and time-based sampling of counters.

### Packet Flow Sampling

The packet flow sampling mechanism carried out by each sFlow Instance ensures that any packet observed at a Data Source has an equal chance of being sampled, irrespective of the packet flow(s) to which it belongs.

Packet flow sampling is accomplished as follows:

1. When a packet arrives on an interface, the Network Device makes a filtering decision to determine whether the packet should be dropped.
2. If the packet is not filtered (dropped), a destination interface is assigned by the switching/routing function.
3. At this point, a decision is made on whether or not to sample the packet. The mechanism involves a counter that is decremented with each packet. When the counter reaches zero a sample is taken.
4. When a sample is taken, the counter indicating how many packets to skip before taking the next sample is reset. The value of the counter is set to a random integer where the sequence of random integers used over time is the Sampling Rate.

Packet flow sampling results in the generation of Packet Flow Records. A Packet Flow Record contains information about the attributes of a packet flow, including:

- Information on the packet itself — a packet header, packet length, and packet encapsulation.
- Information about the path the packet took through the device, including information relating to the selection of the forwarding path.

### Counter Sampling

The primary objective of the counter sampling is to, in an efficient way, periodically export counters associated with Data Sources. A maximum sampling interval is assigned to each sFlow Instance associated with a Data Source.

Counter sampling is accomplished as follows:

1. The sFlow Agent keep a list of counter sources being sampled.

2. When a Packet Flow Sample is generated, the sFlow Agent examines the list of counter sources and adds counters to the sample datagram, least recently sampled first.

Counters are only added to the datagram if the sources are within a short period, 5 seconds say, of failing to meet the required sampling interval.

3. Periodically, say every second, the sFlow Agent examines the list of counter sources and sends any counters that need to be sent to meet the sampling interval requirement.

The set of counters is a fixed set defined in Section 5 of the document entitled “sFlow Version 5” available from sFlow.org (<http://www.sflow.org>).

## Sampling Implementation Notes

Although the switch hardware has the capability to sample packets on any port, to ensure that CPU utilization is not compromised, the number of sFlow samplers that can be configured per switch or stack of switches is limited to a maximum of 32. There is no limitation on the number of pollers that can be configured.

Under certain circumstances, the switch will drop packet samples that the sFlow implementation is not able to count and therefore cannot correctly report `sample_pool` and `drops` fields of flow samples sent to the sFlow Collector. Under heavy load, this sample loss could be significant and could therefore affect the accuracy of the sampling analysis.

## Configuring sFlow

### Overview

sFlow is disabled by default, and therefore must be manually enabled.

### Configuring Collectors

In order for an sFlow Collector to be assigned to receive sample datagrams from the sFlow Agent on the switch, an entry for that Collector must be configured in the switch's sFlow Receivers Table. An entry must contain an owner identity string, a non-zero timeout value, and the IP address of the Collector. Configure the identity string and timeout value with the **set sflow receiver owner** command and the IP address with the **set sflow receiver ip** command.

An entry without an owner identity string is considered unclaimed and cannot be assigned as a receiver to sampler or poller instances.

Once the timer set by the **set sflow receiver owner** command expires, the receiver/Collector and all the samplers and pollers associated with this Collector expire and are removed from the switch's configuration. In order to start sending sample data to the Collector again, the Collector must be reconfigured with a new timeout value and samplers and pollers must be configured again. Therefore, you should consider setting the timeout value to the largest value that is reasonable for your environment.

You can clear the IP address, maximum datagram size, or UDP port without deleting an entry from the sFlow Receivers Table with the **clear sflow receiver** command. If you clear the owner or timeout, the entire entry is cleared. If you enter only an entry index and none of the optional parameters, the entire entry is cleared.

Once an entry is cleared, all pollers and samplers associated with that receiver are also removed from the switch configuration.

## Configuring Poller and Sampler Instances

A **poller instance** performs counter sampling on the data source to which it is configured. You must first associate a receiver/Collector in the sFlow Receivers Table with the poller instance, before configuring the polling interval with the **set sflow port poller** command.

A **sampler instance** performs packet flow sampling on the data source to which it is configured. You must first associate a receiver/Collector in the sFlow Receivers Table with the sampler instance, before configuring the sampling rate or maximum number of bytes copied from sampled packets. A maximum of 32 sampler instances can be configured per switch or stack of switches.

When a receiver times out or is cleared from the sFlow Receivers Table, all poller and sampler instances associated with that receiver are also cleared from the switch's configuration.

## Configuring a Management Interface

The **set sflow interface** command allows you to configure the management interface used by the sFlow Agent when sending sampling datagrams to the sFlow Collector. Any of the interfaces, including VLAN routing interfaces, can be configured as the management interface.

An interface must have an IP address assigned to it before it can be set as the management interface. If no interface is specified, then the Host VLAN will be used as the management interface.

If a non-loopback interface is configured as the management interface, application packet egress is restricted to that interface if the server can be reached from that interface. Otherwise, the packets are transmitted over the first available route. Packets from the application server are received on the configured interface.

If a loopback interface is configured, and there are multiple paths to the application server, the outgoing interface (gateway) is determined based on the best route lookup. Packets from the application server are then received on the sending interface. If route redundancy is required, therefore, a loopback interface should be configured.

## Parameter Defaults

**Table 18-6 Default sFlow Parameters**

| Parameter        | Description                                                                                                                                                         | Default Value                    |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| maxdatagram      | The maximum number of data bytes that can be sent in a single sample datagram.                                                                                      | 1400 bytes                       |
| UDP port         | The UDP port on the receiver/Collector to which the sample datagrams should be sent.                                                                                | 6343                             |
| Polling interval | Poller instance polling interval                                                                                                                                    | 0 (Counter sampling is disabled) |
| maxheadersize    | The maximum number of bytes that should be copied from the sampler packet.                                                                                          | 128 bytes                        |
| Sampler rate     | The statistical sampling rate for sampling from this data source. The value of rate specifies the number of incoming packets from which one packet will be sampled. | 0 (Sampling is disabled)         |

## Procedure

[Procedure 18-2](#) on page 18-14 provides the steps and commands to configure sFlow.

### Procedure 18-2 Configuring sFlow

| Step | Task                                                                                                                                                                                                                           | Command(s)                                                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Configure the owner identity string and timeout value for an sFlow Collector in the switch's sFlow Receivers Table                                                                                                             | <code>set sflow receiver index owner owner-string timeout timeout</code>                                                                                                                          |
| 2.   | Configure the IP address of the sFlow Collector being configured.                                                                                                                                                              | <code>set sflow receiver index ip ipaddr</code>                                                                                                                                                   |
| 3.   | Optionally, set the maximum number of data bytes that can be sent in a single sample datagram.                                                                                                                                 | <code>set sflow receiver index maxdatagram bytes</code>                                                                                                                                           |
| 4.   | Optionally, configure the UDP port on the sFlow Controller to which the switch will send sample datagrams.                                                                                                                     | <code>set sflow receiver index port port</code>                                                                                                                                                   |
| 5.   | Configure a sampler instance on a port:<br>Associate the instance with a specific Collector<br><br>Set the sampling rate<br><br>Optionally, specify the maximum number of bytes that should be copied from the sampler packet. | <code>set sflow port port-string sampler index</code><br><br><code>set sflow port port-string sampler rate rate</code><br><br><code>set sflow port port-string sampler maxheadersize bytes</code> |
| 6.   | Configure a poller instance on a port:<br>Associate the instance with a specific Collector<br><br>Set the polling interval                                                                                                     | <code>set sflow port port-string poller index</code><br><br><code>set sflow port port-string poller interval seconds</code>                                                                       |
| 7.   | Optionally, specify the interface used for the source IP address of the sFlow Agent when sending sampling datagrams to the sFlow Collector.                                                                                    | <code>set sflow interface {loopback loop-ID   vlan vlan-ID}</code>                                                                                                                                |

The following example configures sFlow Collector number 1, accepting the default values for datagram size and UDP port. The example then configures packet sampling instances and counter poller instances on ports 1 through 12, assigning them to sFlow Collector 1.

```
C5(su)->set sflow receiver 1 owner enterasys timeout 180000
C5(su)->set sflow receiver 1 ip 192.168.16.91

C5(su)->set sflow port ge.1.1-12 sampler 1
C5(su)->set sflow port ge.1.1-12 sampler maxheadersize 256
C5(su)->set sflow port ge.1.1-12 sampler rate 2048

C5(su)->set sflow port ge.1.1-12 poller 1
C5(su)->set sflow port ge.1.1-12 poller interval 20
```

[Table 18-7](#) lists the commands to display sFlow information and statistics. Refer to the *CLI Reference* for your platform for command details.

**Table 18-7 Displaying sFlow Information**

| Task                                                                                                                                 | Command                                   |
|--------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| to display the contents of the sFlow Receivers Table, or to display information about a specific sFlow Collector listed in the table | <code>show sflow receivers [index]</code> |
| To display information about configured poller instances                                                                             | <code>show sflow pollers</code>           |
| To display information about configured sampler instances.                                                                           | <code>show sflow samplers</code>          |
| To display the interface used by the sFlow Agent when sending sampling datagrams to the sFlow Collector                              | <code>show sflow interface</code>         |
| To display information about the sFlow Agent.                                                                                        | <code>show sflow agent</code>             |

[Table 18-8](#) lists the commands to manage sFlow. Refer to the *CLI Reference* for your platform for command details.

**Table 18-8 Managing sFlow**

| Task                                                                                                                                                | Command                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| To delete a receiver/Collector from the sFlow Receivers Table, or to return certain parameters to their default values for the specified Collector. | <code>clear sflow receiver index [ip   maxdatagram   owner [timeout]   port]</code> |
| To change the poller interval or to remove poller instances.                                                                                        | <code>clear sflow port <i>port-string</i> poller [interval]</code>                  |
| To change the sampler rate or maximum header size, or to remove sampler instances.                                                                  | <code>clear sflow port <i>port-string</i> sampler [maxheadersize   rate]</code>     |
| To clear the management interface used by the sFlow Agent back to the default of the Host VLAN.                                                     | <code>clear sflow interface</code>                                                  |





## Configuring Multicast

This chapter describes the multicast features supported by the Enterasys fixed switches.

| For information about...                        | Refer to page... |
|-------------------------------------------------|------------------|
| <a href="#">Using Multicast in Your Network</a> | 19-1             |
| <a href="#">Configuring IGMP</a>                | 19-15            |
| <a href="#">Configuring DVMRP</a>               | 19-18            |
| <a href="#">Configuring PIM-SM</a>              | 19-21            |

### Using Multicast in Your Network

Multicast is a “one source to many destinations” method of simultaneously sending information over a network using the most efficient delivery strategy over each link. Only the end stations that explicitly indicate a need to receive a given multicast stream will receive it.

Applications that take advantage of multicast include video conferencing, streaming video, corporate communications, distance learning, and distribution of software, stock quotes, and news.

Multicast technology includes the following protocols:

- Internet Group Management Protocol (IGMP) for IPv4 on all supported Enterasys multicast devices
- Distance Vector Multicast Routing Protocol (DVMRP)
- Protocol Independent Multicast (PIM)

Unlike unicast and broadcast, multicast uses network infrastructure efficiently because only one copy of the source traffic is sent throughout the network, going only to interested receivers, minimizing the burden placed on the sender, network, and receiver. The routers in the network take care of replicating the packet, where necessary, to reach multiple receivers. If a router decides that there are no interested users downstream from itself, it prunes the stream back to the next router. Thus, unwanted streams are not sent to the pruned routers, saving bandwidth and preventing unwanted packets from being sent.

### Implementing Multicast

You can implement the IGMP, DVMRP, and PIM-SM multicast protocols on Enterasys devices using simple CLI commands as described in this document. A basic configuration process involves the following tasks:

1. Configuring the VLANs and IP interfaces on which you want to transmit multicast.

2. Enabling the multicast protocol(s) on configured interfaces.
  - For PIM, you must also configure a unicast routing protocol, such as OSPF.
  - For both DVMRP and PIM-SM for IPv4 to operate, IGMP must be enabled.

## Multicast Operation

Multicast allows a source to send a single copy of data using a single IP address from a well-defined range for an entire group of recipients (a multicast group). A source sends data to a multicast group by simply setting the destination IP address of the datagram to be the multicast group address. Sources do not need to register in any way before they can begin sending data to a group, and do not need to be members of the group themselves. Routers between the source and recipients use the group address to route the data, forwarding duplicate data packets only when the path to recipients diverges.

Hosts that wish to receive data from the multicast group join the group by sending a message to a multicast router on a local interface, using a multicast group membership discovery protocol, such as IGMP (IPv4). For more information, see “[Internet Group Management Protocol \(IGMP\)](#)” on page 19-2.

Multicast routers communicate among themselves using a multicast routing protocol, such as DVMRP or PIM-SM. These protocols calculate a multicast distribution tree of recipients to ensure that:

- Multicast traffic reaches all recipients that have joined the multicast group
- Multicast traffic does not reach networks that do not have any such recipients (unless the network is a transit network on the way to other recipients)
- The number of identical copies of the same data flowing over the same link is minimized.

For more information, see “[Protocol Independent Multicast \(PIM\)](#)” on page 19-11.

## Internet Group Management Protocol (IGMP)

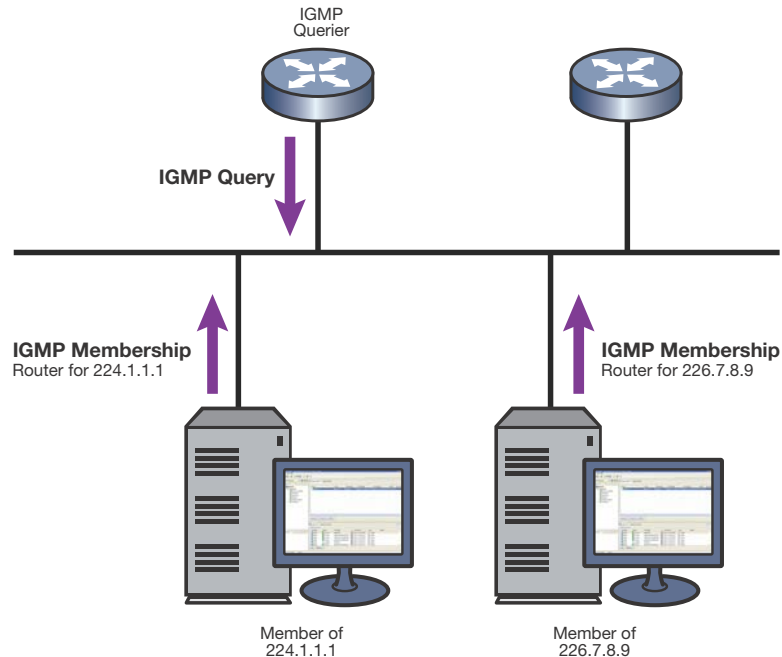
### Overview

Group membership management is fundamental to the multicasting process. An arbitrary group of receivers can express interest in receiving a particular multicast stream, regardless of the physical or geographical boundaries of its members.

The purpose of IP multicast group management is to optimize a switched network’s performance so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast switch devices instead of flooding to all ports in the subnet (VLAN).

IGMP uses three key components to control multicast membership:

- **Source** — A server that sends an IP multicast data stream with a particular multicast destination IP and MAC address. A server may not have direct IGMP involvement, as it often does not receive a multicast stream, but only sends a multicast stream.
- **Querier** — A device that periodically sends out queries in search of multicast hosts on a directly connected network. If multiple queriers are present on the LAN, the querier with the lowest IP address assumes the role.
- **Host** — A client end station that sends one of two IGMP messages to a querier:
  - Join message — Indicates the host wants to receive transmissions associated to a particular multicast group.
  - Leave message — Indicates the host wants to stop receiving the multicast transmissions.

**Figure 19-1 IGMP Querier Determining Group Membership**

As shown in [Figure 19-1](#), a multicast-enabled device can periodically ask its hosts if they want to receive multicast traffic. If there is more than one device on the LAN performing IP multicasting, one of these devices is elected querier and assumes the responsibility of querying the LAN for group members.

Based on the group membership information learned from IGMP, a device can determine which (if any) multicast traffic needs to be forwarded to each of its ports. At Layer 3, multicast switch devices use this information, along with a multicast routing protocol, to support IP multicasting across the Internet.

IGMP provides the final step in IP multicast delivery. It is only concerned with forwarding multicast traffic from the local switch device to group members on a directly attached subnetwork or LAN segment.

IGMP neither alters nor routes any IP multicast packets. Since IGMP is not concerned with the delivery of IP multicast packets across subnetworks, an external IP multicast device is needed if IP multicast packets have to be routed across different subnetworks.

## IGMP Support on Enterasys Devices

Enterasys devices implement IGMP version 2 (RFC 2236) and IGMP version 3 (RFC 3376), which includes interoperability with version 1 hosts. IGMP version 1 is defined in RFC 1112.

Depending on your Enterasys device, IGMP can be configured independently at the switch level (Layer 2) and at the router level (Layer 3).

Enterasys devices support IGMP as follows:

- Passively snooping on the IGMP query and IGMP report packets transferred between IP multicast switches and IP multicast host groups to learn IP multicast group members. Each Layer 2 device records which ports IGMP packets are received on, depending on the kind of IGMP message, so multicast data traffic is not flooded across every port on the VLAN when it is received by the switch.

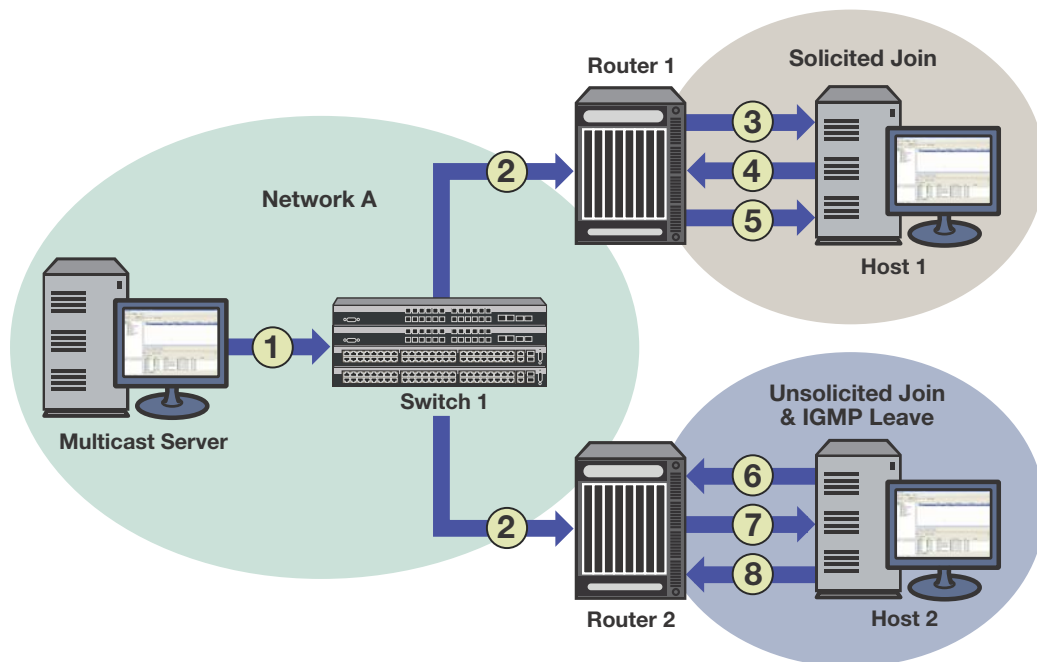
IGMP snooping is disabled by default on Enterasys devices. You can enable it using the **set igmpsnooping adminmode** command on Enterasys stackable and standalone devices as described in “[Configuring IGMP](#)” on page 19-15.

- Actively sending IGMP query messages to learn locations of multicast switches and member hosts in multicast groups within each VLAN.
- Configuration of static IGMP groups using the **set igmpsnooping add-static** on the fixed switches. Static IGMP configuration provides for specifying the IP address (group address) and VLAN of a non-IGMP capable device, forcing the sending of IGMP messages to the device. The static IG groups commands are described in “[Configuring IGMP](#)” on page 19-15.

### Example: Sending a Multicast Stream

[Figure 19-2](#) provides an example of IGMP processing on Enterasys devices when there are no directly attached hosts.

**Figure 19-2 Sending a Multicast Stream with No Directly Attached Hosts**



1. A single IP multicast server, with no directly attached hosts, sends a multicast stream into the network via Switch 1.
2. Because IGMP snooping is disabled, Switch 1 floods the multicast stream to all ports which are linked to Router 1 and Router 2.

Each router performs an IGMP forwarding check to see if there are any hosts that want to join the multicast group on its locally attached network. Each router drops multicast packets until a host joins the group using one of the following messages:

- **solicited join** (sent in response to an IGMP query produced by the router’s interface)

In [Figure 19-2](#), this type of exchange occurs between Router 1 and Host 1 when:

- (3) Router 1 sends a query to potential Host 1.
- (4) Host 1 responds with a join message.
- (5) Router 1 forwards the multicast stream.

- **unsolicited join** (sent as a request without receiving an IGMP query first)  
In [Figure 19-2](#), this type of exchange occurs between Router 2 and Host 2 when:
  - (6) Host 2 sends a join message to Router 2.
  - (7) Router 2 forwards the multicast stream to Host 2.
  - (8) When it no longer wants to receive the stream, Host 2 can do one of the following:
    - Send a leave message to Router 2.
    - Time out the IGMP entry by not responding to further queries from Router 2.

## Distance Vector Multicast Routing Protocol (DVMRP)

### Overview

DVMRP, which is used for routing multicasts within a single, autonomous system, is designed to be used as an interior gateway protocol (IGP) within a multicast domain. It is a distance-vector routing protocol that relies on IGMP functionality to provide connectionless datagram delivery to a group of hosts across a network.

DVMRP routes multicast traffic using a technique known as reverse path forwarding (RPF). When a router receives IP multicast packets, it first does an RPF check to determine if the packets are received on the correct interface. If so, the router forwards the packets out to the following:

- Local IGMP receivers for that group on interfaces for which the transmitting router is the designated forwarder
- Neighbor routers that have indicated their dependence on the transmitting router for forwarding multicast packets from that source (this is determined during DVMRP Route Exchange) and from which the transmitting router has not received any prune messages.

If not, the packets are discarded by the router. The transmitting router does not forward the packets back to the source.

If a router is attached to a set of VLANs that do not want to receive from a particular multicast group, the router can send a prune message back up the distribution tree to stop subsequent packets from traveling where there are no members. DVMRP periodically re-floods in order to reach any new hosts that want to receive from a particular group.

DVMRP routers dynamically discover their neighbors by sending neighbor probe messages periodically to an IP multicast group address that is reserved for all DVMRP routers.

Key features of DVMRP are the following:

- uses the well-known multicast IP address 224.0.0.4
- uses IGMP to exchange routing datagrams
- does not require an underlying Layer 3 routing protocol to provide a path to remote multicast destinations
- combines many of the features of the Routing Information Protocol (RIP) with the Truncated Reverse Path Broadcasting (TRPB) algorithm to route multicast packets between sources and receivers

### DVMRP Support on Enterasys Devices



**Note:** DVMRP is supported on Enterasys fixed switches on which advanced routing has been enabled. Refer to [“Licensing Advanced Features”](#) on page 4-8 for more information.

DVMRP routing is implemented on Enterasys devices as specified in RFC 1075 and *draft-ietf-idmr-dvmrp-v3-10.txt*.

Enterasys devices support the following DVMRP components:

- [Probe Messages](#) for neighbor discovery
- [Route Table](#) for maintaining routes to all DVRMP networks
- [Route Reports](#) for route exchange with adjacent devices
- [Mroute Table](#) for maintaining per-source-group multicast trees
- [Prune Messages](#) for terminating multicast delivery trees
- [Graft Messages](#) for re-adding pruned multicast delivery trees

### Probe Messages

Each DVMRP-enabled interface transmits multicast probe packets to inform other DVMRP routers that it is operational. Probe messages are sent every 10 seconds on every interface running DVMRP. These messages provide:

- **A mechanism for DVMRP devices to locate each other.** Probe messages contain a list of the neighbors detected for each enabled interface. If no neighbors are found, the network is considered to be a leaf network.
- **A mechanism for DVMRP devices to determine the capabilities of neighboring devices.** Probe messages contain flags about neighbors' DVMRP capabilities and version compliance.
- **A keep-alive function for quickly detecting neighbor loss.** If a probe message from an adjacent neighbor is not seen within 35 seconds, the neighbor is timed out.

### Route Table

Each DVMRP-enabled device builds a DVMRP route table to maintain routes to all networks involved in DVMRP routing. As shown in the following example output, the DVMRP route table contains destination and neighbor addresses, metric value (in brackets), expiration time (currently not supported in the firmware), up-time (in seconds), and generation IDs from Probe messages.

```
System(su)->router#show ip dvmrp route
flag characters used:

V Neighbor is verified.
P Neighbor supports pruning.
G Neighbor supports generation ID.
N Neighbor supports netmask in prunes and grafts.
S Neighbor supports SNMP.
M Neighbor supports mtrace.

10.5.10.0/255.255.255.0 [3] Uptime: 61103 , expires: 0
via neighbor: 10.5.60.2 version: 3
Generation ID gen id: 1331801871
10.5.20.0/255.255.255.0 [2] Uptime: 61103 , expires: 0
via neighbor: 10.5.60.2 version: 3
Generation ID gen id: 1331801871
10.5.30.0/255.255.255.0 [2] Uptime: 61103 , expires: 0
via neighbor: 10.5.60.2 version: 3
```

```

Generation ID gen id: 1331801871
10.5.40.0/255.255.255.0 [2] Uptime: 66704 , expires: 0
via neighbor: 10.5.50.1 version: 3
Generation ID gen id: 1331805217
10.5.50.0/255.255.255.0 [0] Uptime: 66704 , expires: 0
via neighbor: direct version: 3
10.5.51.0/255.255.255.0 [0] Uptime: 66714 , expires: 0
via neighbor: direct version: 3
10.5.52.0/255.255.255.0 [0] Uptime: 66716 , expires: 0
via neighbor: direct version: 3
10.5.60.0/255.255.255.0 [0] Uptime: 3615 , expires: 0
via neighbor: direct version: 3
10.5.70.0/255.255.255.0 [3] Uptime: 66705 , expires: 0
via neighbor: 10.5.50.1 version: 3
Generation ID gen id: 1331805217
192.168.200.0/255.255.255.0 [0] Uptime: 66721 , expires: 0
via neighbor: direct version: 3

```

## Route Reports

DVMRP-enabled devices send route report packets to adjacent DVMRP devices every 60 seconds. When a DVMRP device receives one, it checks to verify that the report is from a known neighbor before processing.

The first time a device sees its own address in a neighbor's probe packet, it sends a unicast copy of its entire routing table to the neighbor to reduce start-up time.

The route report packet contains data about all networks/routes of which the sending device is aware. This information is used to determine the reverse path back to a particular multicast source. Every DVMRP device keeps a separate metric associated with each route. This metric is the sum of all interface metrics between the device originating the report and the source network.

DVMRP devices accept route reports for aggregated source networks in accordance with classless inter-domain devices (CIDR). This means that, if a prune or graft is received on a downstream interface for which the source network is aggregated, then a prune or graft should be sent upstream (to the multicast source).

If a DVMRP device has a large number of DVMRP routes, it will spread route reports across the route update interval (60 seconds) to avoid bottlenecks in processing and route synchronization issues.

For the purpose of pruning, DVMRP needs to know which downstream routes depend on the device for receiving multicast streams. Using poison reverse, the upstream router maintains a table of the source network and all downstream devices that are dependent on the upstream device.

## Mroute Table

DVMRP-enabled devices use the mroute table to maintain a source-specific forwarding tree.

When a DVMRP device is initialized, it assumes the role of the designated forwarder for all of its locally attached networks. Before forwarding any packets, all devices use IGMP to learn which networks would like to receive particular multicast group streams. In the case of a shared network, the device with a lower interface metric (a configurable value), or the lower IP address will become the designated forwarder.

A DVMRP device forwards multicast packets first by determining the upstream interface, and then by building the downstream interface list. If a downstream router has no hosts for a multicast stream, it sends a prune message to the upstream router. If the upstream router's outbound list is now empty, it may send a prune message to its upstream router.

If a downstream device has pruned a multicast group that a host would like to now receive, the downstream device must send a DVMRP graft message to its upstream device. The DVMRP graft will traverse the source-specific multicast delivery tree to the device that is receiving this stream.

As shown in the following example output, the Mroute table displays the incoming interface IP address, the multicast group address, the uptime of the stream, the address of the upstream neighbor, and the upstream and downstream VLANs.

```
System(su)->router#show ip mroute

Active IP Multicast Sources
Flags: D - Dense, S - Sparse, C - Connected, L - Local,P - Pruned, R - RP-bit set,
F - Register flag, T - SPT-bit set,Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

Source Network : 192.168.111.10
Source Mask : 0.0.0.0
MultiCast Group : 239.1.8.9
Uptime : 6336
Upstream Neighbor: 0.0.0.0
Upstream Vlan : 111
Downstream Vlans : 8

Source Network : 192.168.111.10
Source Mask : 0.0.0.0
MultiCast Group : 239.1.7.105
Uptime : 6336
Upstream Neighbor: 0.0.0.0
Upstream Vlan : 111
Downstream Vlans : 8

Source Network : 192.168.111.10
Source Mask : 0.0.0.0
MultiCast Group : 239.1.8.169
Uptime : 6582
Upstream Neighbor: 0.0.0.0
Upstream Vlan : 111
Downstream Vlans : 8

Source Network : 192.168.111.10
Source Mask : 0.0.0.0
MultiCast Group : 239.1.4.173
Uptime : 6582
Upstream Neighbor: 0.0.0.0
Upstream Vlan : 111
Downstream Vlans : 8
```

In this example, the device is receiving multicast streams for groups 239.1.8.9, 239.1.7.105, 239.1.8.169, and 239.1.4.173 from IP address 192.168.111.10 on the incoming interface VLAN 8.

## Prune Messages

If a device receives a datagram that has no IGMP group members present, and all the downstream networks are leaf networks, the device sends a prune packet upstream to the source tree.

When sending a prune upstream, the device:



1. Decides if the upstream neighbor is capable of receiving prunes.
  - If it is not, then the sending device proceeds no further.
  - If it is, then the sending device proceeds as follows.
2. Stops any pending grafts awaiting acknowledgments.
3. Determines the prune lifetime.

This value should be the minimum of the default prune lifetime (randomized to prevent synchronization) and the remaining prune lifetimes of the downstream neighbors.

4. Forms and transmits the packet to the upstream neighbor for the source.

To ensure the prune is accepted, the DVMRP-enabled device sets a negative cache prune entry for three seconds. If the traffic has not stopped after three seconds, the device sends another prune and doubles the cache entry. This method is called exponential back-off. The more prunes that are dropped, the longer the back-off becomes.

After the prune lifetime expires (two hours), the prune transmission process is repeated.

When receiving a prune, the upstream device:

1. Decides if the sending neighbor is known.
  - If the neighbor is unknown, it discards the received prune.
  - If the neighbor is known, the receiving device proceeds as follows.
2. Ensures the prune message contains at least the correct amount of data.
3. Copies the source address, group address, and prune time-out value, and, if it is available in the packet, the netmask value to determine the route to which the prune applies.
4. Determines if there is active source information for the source network, multicast group (S,G) pair.
  - If there is not, then the device ignores the prune.
  - If there is, then the device proceeds as follows.
5. Verifies that the prune was received from a dependent neighbor for the source network.
  - If it was not, then the device discards the prune.
  - If it was, then the device proceeds as follows.
6. Determines if a prune is currently active from the same dependent neighbor for this S,G pair.
  - If not active, creates a state for the new prune and sets a timer for the prune lifetime
  - If active, resets the timer to the new time-out value.
7. Determines if all dependent downstream devices on the interface from which the prune was received have now sent prunes.
  - If they have not, removes the interface from all forwarding cache entries for this group instantiated using the route to which the prune applies.
  - If they have, determines if there are group members active on the interface and if this device is the designated forwarder for the network.

### Graft Messages

Leaf devices send graft messages when the following occur:

- A new local member joins a group that has been pruned upstream and this device is the designated forwarder for the source.

- A new dependent downstream device appears on a pruned branch.
- A dependent downstream device on a pruned branch restarts.
- A graft retransmission timer expires before a graft ACK is received.

Graft messages are sent upstream hop-by-hop until the multicast tree is reached. Since there is no way to tell whether a graft message was lost or the source has stopped sending, each graft message is acknowledged hop-by-hop.

When sending grafts, the downstream device does the following:

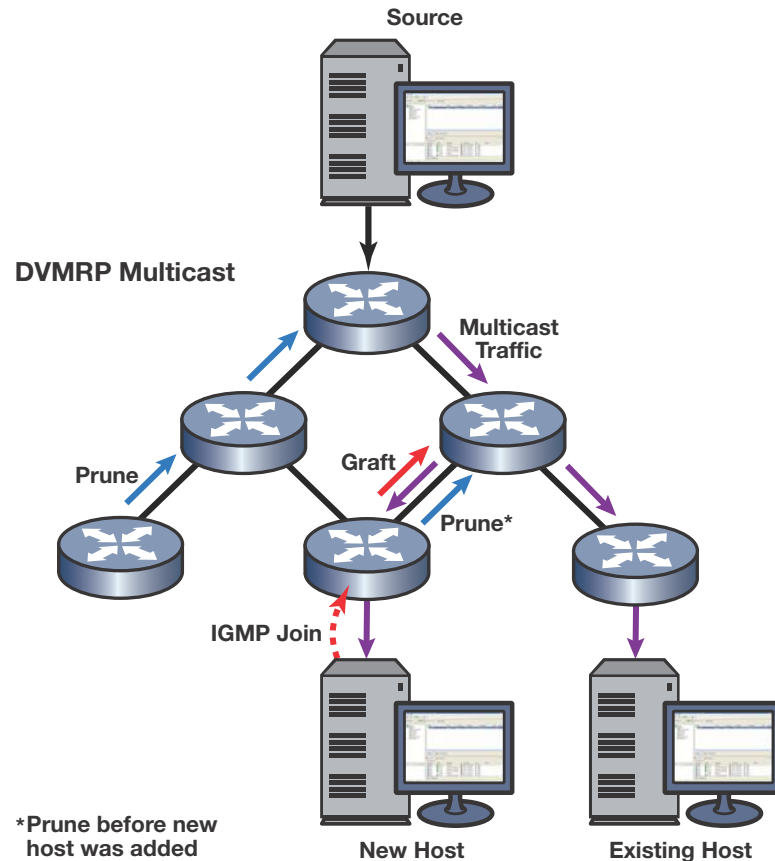
1. Verifies a prune exists for the source network and group.
2. Verifies that the upstream device is capable of receiving prunes (and therefore grafts).
3. Adds the graft to the retransmission timer list awaiting an acknowledgment.
4. Formulates and transmits the graft packet.

When receiving grafts, the upstream device does the following:

1. Verifies whether the neighbor is known.
  - If unknown, discards the received graft.
  - If known, proceeds as follows.
2. Ensures the graft message contains at least the correct amount of data.
3. Sends back a graft ACK to the sender.
4. If the sender was a downstream dependent neighbor from which a prune had previously been received:
  - Removes the prune state for this neighbor.
  - If necessary, updates any forwarding cache entries based on this (source, group) pair to include this downstream interface.

[Figure 19-3](#) on page 19-11 shows the DVMRP pruning and grafting process.

Figure 19-3 DVMRP Pruning and Grafting



## Protocol Independent Multicast (PIM)

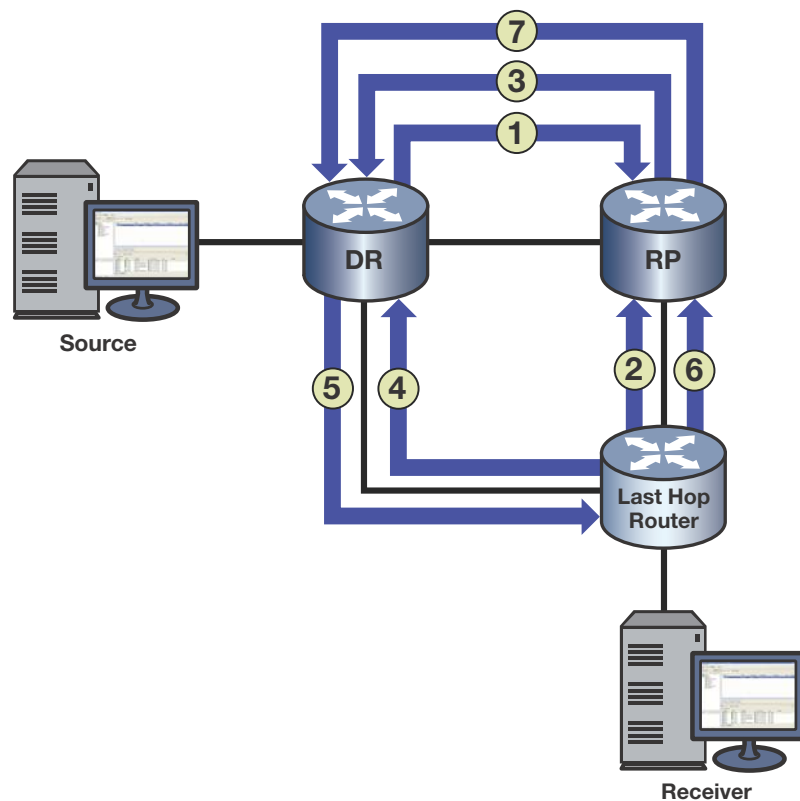
### Overview

PIM dynamically builds a distribution tree for forwarding multicast data on a network. It is designed for use where there may be many devices communicating at the same time, and any one of the devices could be the sender at any particular time. Scenarios for using PIM multicasting include desktop video conferencing and telephone conference calls.

PIM relies on IGMP technology to determine group memberships and uses existing unicast routes to perform reverse path forwarding (RPF) checks, which are, essentially, a route lookup on the source. Its routing engine then returns the best interface, regardless of how the routing table is constructed. In this sense, PIM is independent of any routing protocol. It can perform RPF checks using protocol-specific routes (for example, OSPF routes), static routes, or a combination of route types.

PIM, a shared-tree technology, designates a router as the rendezvous point (RP), which is the root of a shared tree for a particular group. All sources send packets to the group via the RP (that is, traffic flows from the sender to the RP, and from the RP to the receiver). By maintaining one RP-rooted tree instead of multiple source-rooted trees, bandwidth is conserved.

Figure 19-4 on page 19-12 illustrates the PIM traffic flow.

**Figure 19-4 PIM Traffic Flow**

1. The source's DR registers (that is, encapsulates) and sends multicast data from the source directly to the RP via a unicast routing protocol (number 1 in figure). The RP de-encapsulates each register message and sends the resulting multicast packet down the shared tree.
2. The last-hop router (that is, the receiver's DR) sends a multicast group (\*,G) join message upstream to the RP, indicating that the receiver wants to receive the multicast data (number 2 in figure). This builds the RP tree (RPT) between the last-hop router and the RP.
3. The RP sends an S,G join message to the source (number 3 in figure). It may send the join message immediately, or after the data rate exceeds a configured threshold. This allows the administrator to control how PIM-SM uses network resources.
4. The last-hop router joins the shortest path tree (SPT) and sends an S,G join message to the source. (number 4 in figure). This builds the SPT.
5. Native multicast packets (that is, non-registered packets) are sent from the source's DR to the receiver on its SPT (number 5 in figure), while registered multicast packets continue to be sent from the source's DR to the RP.
6. A prune message is sent from the last-hop router to the RP (number 6 in figure).
7. A prune message (*register-stop*) is sent from the RP to the source's DR (number 7 in figure). Once traffic is flowing down the SPT, the RPT is pruned for that given S,G.

When receivers go away, prunes are sent (S,G prune messages towards the source on the SPT, and \*,G prune messages towards the RP on the RPT). When new receivers appear, the process begins again.

## PIM Support on Enterasys Devices



**Note:** PIM is supported on Enterasys fixed switches on which advanced routing has been enabled. Refer to “[Licensing Advanced Features](#)” on page 4-8 for more information.

Enterasys devices support version 2 of the PIM protocol as described in RFC 4601 and *draft-ietf-pim-sm-v2-new-09*.

The PIM specifications define several modes or methods by which a PIM router can build the distribution tree. Enterasys stackable C3 and C5 and standalone G-Series platforms support sparse mode (PIM-SM).

The PIM specifications define several modes or methods by which a PIM router can build the distribution tree. Enterasys devices support sparse mode (PIM-SM), which uses only those routers that need to be included in forwarding multicast data. PIM-SM uses a host-initiated process to build and maintain the multicast distribution tree. Sparse mode routers use bandwidth more efficiently than other modes, but can require more processing time when working with large numbers of streams.

### Key Features

Key features of PIM-SM are the following:

- Uses IGMP to propagate group membership information
- Sends hello messages to determine neighbor presence and configuration
- Sends join/prune messages to determine the need to retain multicast route information for a particular group on an interface
- Sends assert messages to resolve conflicts that occur regarding inbound interfaces
- Uses routes in the Multicast Routing Information Base (MRIB) to perform its reverse path forwarding check

### PIM-SM Message Types

Enterasys PIM-SM-enabled devices use the following message types:

**Table 19-1 PIM-SM Message Types**

| Message Type  | Description                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hello         | These messages announce the sender’s presence to other PIM-SM devices. The hello packet includes options such as: <ul style="list-style-type: none"> <li>• Hold time — the length of time to keep the sender reachable</li> <li>• Designated router (DR) priority — used to designate which PIM-SM device will act on behalf of sources and receivers in the PIM-SM domain</li> </ul> |
| Register      | These messages are used by a source’s DR to encapsulate (register) multicast data, and send it to the rendezvous point (RP) — a PIM-SM router designated as the root of a shared tree.                                                                                                                                                                                                |
| Register-Stop | These messages are used by the RP to tell the source’s DR to stop registering traffic for a particular source.                                                                                                                                                                                                                                                                        |

**Table 19-1 PIM-SM Message Types (continued)**

| Message Type         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Join/Prune (J/P)     | <p>These messages contain information on group membership received from downstream routers.</p> <p>PIM-SM adopts RPF technology in the join/prune process. When a multicast packet arrives, the router first judges the correctness of the arriving interfaces:</p> <ul style="list-style-type: none"> <li>• If the packet is a source address/multicast group (S,G) entry (on the shortest path tree (SPT)), then the correct interface is the reverse path forwarding (RPF) interface towards the source.</li> <li>• If the packet is not an S,G entry (on the RP tree (RPT)), then the correct interface is the RPF interface towards the RP.</li> </ul> <p>A router directly connected to the hosts is often referred to as a leaf router or DR. The leaf router is responsible for sending the prune messages to the RP, informing it to stop sending multicast packets associated with a specific multicast group. When the RP receives the prune message, it will no longer forward the multicast traffic out the interface on which it received the prune message.</p> |
| Assert               | <p>These messages indicate that the device received a data packet on its outbound (receiving) interface for the group. They report the metric or distance to the source or RP to help the device identify the most direct path to the root of the tree. If multiple routers claim to have the most direct path to the source or RP, each device sends its own assert message and the router with the best metric wins. The other device will then remove that link from its outbound interface list for the group.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Bootstrap            | <p>These messages are sent by the PIM-SM router that has been elected as the bootstrap router (BSR) to inform all PIM-SM routes of the RP/group mappings.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Candidate RP message | <p>These messages are sent by the configured candidate RP routers to the BSR to inform the BSR of its RP/group candidacy.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## PIM Terms and Definitions

Table 19-2 lists terms and definitions used in PIM configuration.

**Table 19-2 PIM Terms and Definitions**

| Term                                       | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bootstrap Router (BSR)                     | <p>A PIM router responsible for collecting, within a PIM domain, the set of potential rendezvous points (RPs) and distributing the RP set information to all PIM routers within the domain. The BSR is dynamically elected from the set of candidate BSRs.</p> <p>RP set information includes group-to-RP mappings.</p>                                                                                                                                       |
| Candidate Bootstrap Router (Candidate-BSR) | <p>A small number of routers within a PIM domain are configured as candidate BSRs, and each C-BSR is given a BSR priority. All C-BSRs multicast bootstrap messages (BSMs) containing their priority to the ALL-PIM-ROUTERS group. When a C-BSR receives a bootstrap message from a C-BSR with a higher priority, it stops sending. This continues until only one C-BSR remains sending bootstrap messages, and it becomes the elected BSR for the domain.</p> |

**Table 19-2 PIM Terms and Definitions (continued)**

| Term                                      | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rendezvous Point (RP)                     | <p>The root of a group-specific distribution tree whose branches extend to all nodes in the PIM domain that want to receive traffic sent to the group.</p> <p>RPs provide a place for receivers and senders to meet. Senders use RPs to announce their existence, and receivers use RPs to learn about new senders of a group.</p> <p>The RP router, for the group, is selected by using the hash algorithm defined in RFC 2362.</p>                                                                                                                                                                                                                                                                                                                                                      |
| Candidate Rendezvous Point (Candidate-RP) | <p>PIM routers configured to participate as RPs for some or all groups.</p> <p>C-RPs send C-RP Advertisement messages to the BSR. The messages contain the list of group prefixes for which the C-RP is willing to be the RP. Once the PIM-SM routers receive the BSR's message, the routers use a common hashing algorithm to hash the C-RP address, group, and mask together to identify which router will be the RP for a given group.</p> <p>A C-RP router must also learn which PIM-SM router is the BSR. Each designated candidate-BSR (C-BSR) asserts itself as the BSR, then defers once it receives a preferable BSR message. Eventually, all C-RPs send their messages to a single BSR, which communicates the <i>Candidate RP-set</i> to all PIM-SM routers in the domain.</p> |
| Static RP                                 | <p>If a BSR is not used to distribute RP set information, RP-to-group mappings are configured statically on each router.</p> <p>Static RP configuration and use of bootstrap routers are mutually exclusive. You should not configure both in a PIM-SM domain because such configuration could result in inconsistent RP sets. Statically configured RP set information will take precedence over RP set information learned from a BSR.</p>                                                                                                                                                                                                                                                                                                                                              |
| Designated Router (DR)                    | <p>A designated router is elected from all the PIM routers on a shared network. DRs are responsible for encapsulating multicast data from local sources into PIM-SM register messages and for unicasting them to the RP. The router with the highest priority wins the DR election. In the case of a tie, the router with the highest IP address wins.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                |
| PIM Domain                                | <p>A contiguous set of routers that implement PIM and are configured to operate within a common boundary defined by PIM multicast border routers.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| PIM Multicast Border Router (PMBR)        | <p>A router that connects a PIM domain to other multicast routing domains.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| sparse mode                               | <p>PIM sparse mode (SM) uses a host-initiated process to build and maintain the multicast distribution tree, using only those routers that need to be included in forwarding multicast data. Sparse mode routers use bandwidth more efficiently than other modes, but can require more processing time when working with large numbers of streams</p>                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Configuring IGMP

On the fixed switch stackable and standalone devices, IGMP can be configured independently at the switch level (Layer 2) for IGMP snooping. On fixed switch devices that support basic routing, IGMP can also be configured at the router level (Layer 3) for determining host membership on directly attached subnets. At Layer 2, IGMP can be enabled for VLANs, regardless of whether it is enabled on routed interfaces. If, however, IGMP is enabled on a routed interface, and the routed interface is a routed VLAN, then IGMP must also be enabled at the switch level.

[Table 19-3](#) on page 19-16 lists the Layer 2 IGMP configuration commands for fixed switch devices.

**Table 19-3 Layer 2 IGMP Configuration Commands**

| Task                                                                               | Command                                                                                      |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Enable or disable IGMP on the system.                                              | <b>set igmpsnooping adminmode</b> {enable   disable}                                         |
| Enable or disable IGMP on one or all ports.                                        | <b>set igmpsnooping interfacemode</b> <i>port-string</i> {enable   disable}                  |
| Configure the IGMP group membership interval time for the system.                  | <b>set igmpsnooping groupmembershipinterval</b> <i>time</i>                                  |
| Configure the IGMP query maximum response time for the system.                     | <b>set igmpsnooping maxresponse</b> <i>time</i>                                              |
| Configure the IGMP multicast router expiration time for the system.                | <b>set igmpsnooping mcretexpire</b> <i>time</i>                                              |
| Create a new static IGMP entry or add one or more new ports to an existing entry.  | <b>set igmpsnooping add-static</b> <i>group vlan-list</i> [modify] [ <i>port-string</i> ]    |
| Delete a static IGMP entry or remove one or more new ports from an existing entry. | <b>set igmpsnooping remove-static</b> <i>group vlan-list</i> [modify] [ <i>port-string</i> ] |
| Clear all IGMP snooping entries.                                                   | <b>clear igmpsnooping</b>                                                                    |

Table 19-4 lists the Layer 3 IGMP configuration commands for fixed switch devices that support basic routing.

**Table 19-4 Layer 3 IGMP Configuration Commands**

| Task                                                                                                                                                                                            | Command                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Enable IGMP on the router. Use the <b>no</b> command to disable IGMP on the router.                                                                                                             | <b>ip igmp</b><br><b>no ip igmp</b>                                                             |
| Enable IGMP on an interface. Use the <b>no</b> command to disable IGMP on an interface.                                                                                                         | <b>ip igmp enable</b><br><b>no ip igmp enable</b>                                               |
| Set the version of IGMP running on the router. Use the <b>no</b> command to reset IGMP to the default version of 2 (IGMPv2).                                                                    | <b>ip igmp version</b> <i>version</i><br><b>no ip igmp</b>                                      |
| Set the IGMP query interval on a routing interface. Use the <b>no</b> command to reset the IGMP query interval to the default value of 125 seconds.                                             | <b>ip igmp query-interval</b> <i>time</i><br><b>no ip igmp query-interval</b>                   |
| Set the maximum response time interval advertised in IGMPv2 queries. Use the <b>no</b> command to reset the IGMP maximum response time to the default value of 100 (one tenth of a second).     | <b>ip igmp query-max-response-time</b> <i>time</i><br><b>no ip igmp query-max-response-time</b> |
| Set the interval between general IGMP queries sent on startup. Use the <b>no</b> command to reset the IGMP startup query interval to the default value of 31 seconds.                           | <b>ip igmp startup-query-interval</b> <i>time</i><br><b>no ip igmp startup-query-interval</b>   |
| Set the number of IGMP queries sent out on startup, separated by the <b>startup-query-interval</b> . Use the <b>no</b> command to reset the IGMP startup query count to the default value of 2. | <b>ip igmp startup-query-count</b> <i>count</i><br><b>no ip igmp startup-query-count</b>        |



**Table 19-4 Layer 3 IGMP Configuration Commands**

| Task                                                                                                                                                                                                                        | Command                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Set the maximum response time being inserted into group-specific queries sent in response to leave group messages. Use the <b>no</b> command to reset the IGMP last member query interval to the default value of 1 second. | <b>ip igmp last-member-query-interval</b> <i>time</i><br><b>no ip igmp last-member-query-interval</b> |
| Set the number of group-specific queries sent before assuming there are no local members. Use the <b>no</b> command to reset the IGMP last member query count to the default value of 2.                                    | <b>ip igmp last-member-query-count</b> <i>count</i><br><b>no ip igmp last-member-query-count</b>      |
| Configure the robustness tuning for expected packet loss on an IGMP routing interface. Use the <b>no</b> command to reset the IGMP robustness value to the default of 2.                                                    | <b>ip igmp robustness</b> <i>robustness</i><br><b>no ip igmp robustness</b>                           |

## Basic IGMP Configuration

[Procedure 19-1](#) describes the basic steps to configure Layer 2 IGMP snooping on Enterasys stackable and standalone devices. This procedure assumes that the VLANs on which IGMP will run have been configured and enabled with IP interfaces.

### Procedure 19-1 Basic IGMP Snooping Configuration

| Step | Task                                                   | Command                                                                |
|------|--------------------------------------------------------|------------------------------------------------------------------------|
| 1.   | In switch mode, enable IGMP globally.                  | <b>set igmpsnooping adminmode enable</b>                               |
| 2.   | In switch mode, enable IGMP on each of the VLAN ports. | <b>set igmpsnooping interfacemode</b> <i>port-string</i> <b>enable</b> |

[Procedure 19-2](#) describes the basic steps to configure Layer 3 IGMP querying on fixed switch platforms that support basic routing. This procedure assumes that the VLANs on which IGMP will run have been configured and enabled with IP interfaces.

### Procedure 19-2 Basic IGMP Configuration in Router Mode

| Step | Task                                                                                                                                              | Command               |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| 1.   | In router configuration mode, enable IGMP globally.                                                                                               | <b>ip igmp</b>        |
| 2.   | In router configuration mode, enable IGMP on each VLAN interface that will be required to determine host membership on directly attached subnets. | <b>ip igmp enable</b> |

For more information on IGMP CLI commands, refer to your device's *CLI Reference* as applicable.

## Example IGMP Configuration on Layer 3

```
System(su)->router
System(su)->router>enable
System(su)->router#configure
 Enter configuration commands:
System(su)->router(Config)#ip igmp
System(su)->router(Config)#interface vlan 1
System(su)->router(Config-if(Vlan 1))#ip igmp enable
```

```

System(su)->router(Config-if(Vlan 1))#exit
System(su)->router(Config)#interface vlan 2
System(su)->router(Config-if(Vlan 2))#ip igmp enable
System(su)->router(Config-if(Vlan 2))#exit

```

## IGMP Display Commands

[Table 19-5](#) lists Layer 2 IGMP show commands for Enterasys stackable and standalone devices.

**Table 19-5 Layer 2 IGMP Show Commands**

| Task                                                            | Command                                                        |
|-----------------------------------------------------------------|----------------------------------------------------------------|
| Display IGMP snooping information.                              | <b>show igmpsnooping</b>                                       |
| Display static IGMP ports for one or more VLANs or IGMP groups. | <b>show igmpsnooping static</b> <i>vlan-list</i> [group group] |
| Display multicast forwarding database (MFDB) information.       | <b>show igmpsnooping mfdb</b>                                  |

[Table 19-6](#) lists Layer 3 IGMP show commands for fixed switches that support basic routing.

**Table 19-6 Layer 3 IGMP Show Commands**

| Task                                                                                | Command                                              |
|-------------------------------------------------------------------------------------|------------------------------------------------------|
| Display IGMP information regarding multicast group membership.                      | <b>show ip igmp groups</b>                           |
| Display multicast-related information about a specific interface or all interfaces. | <b>show ip igmp interface</b> [vlan <i>vlan-id</i> ] |

## Configuring DVMRP

DVMRP is an advanced routing feature that must be enabled with a license key.

### DVMRP Configuration Commands

[Table 19-7](#) lists the DVMRP configuration commands for fixed switch devices that support and have enabled advanced routing features.

**Table 19-7 DVMRP Configuration Commands**

| Task                                                                                      | Command                                             |
|-------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Enable the DVMRP process. Use the <b>no</b> command to disable the DVMRP process.         | <b>ip dvmrp</b><br><b>no ip dvmrp</b>               |
| Enable DVMRP on an interface. Use the <b>no</b> command to disable DVMRP on an interface. | <b>ip dvmrp enable</b><br><b>no ip dvmrp enable</b> |
| Configure the metric associated with a set of destinations for DVMRP reports.             | <b>ip dvmrp metric</b> <i>metric</i>                |

## Basic DVMRP Configuration

By default, DVMRP is disabled globally and on each interface. Basic DVMRP configuration includes the following steps:

1. Creating and enabling VLANs.
2. Enabling IGMP globally on the device and on the VLANs.
3. Enabling DVMRP globally on the device and on the VLANs.

[Procedure 19-3](#) describes the basic steps to configure DVMRP on fixed switches with advanced routing enabled. [Procedure 19-3](#) assumes VLANs have been configured and enabled with IP interfaces.

### Procedure 19-3 Basic DVMRP Configuration

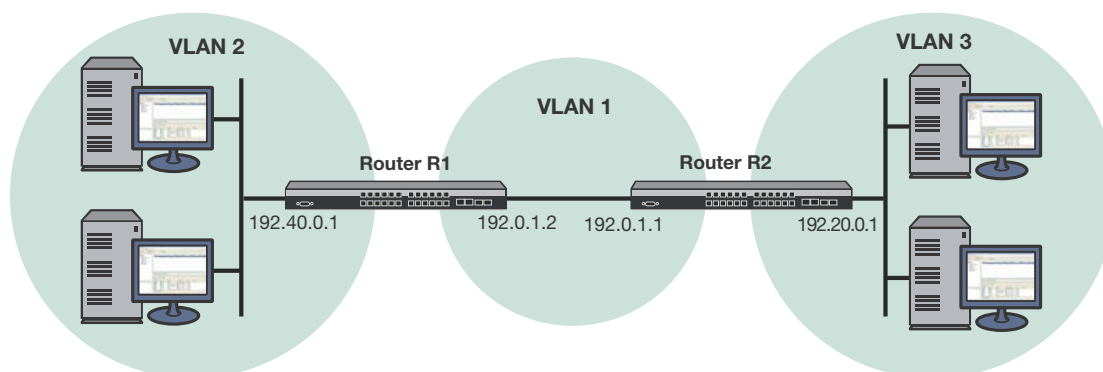
| Step | Task                                                                                        | Command                |
|------|---------------------------------------------------------------------------------------------|------------------------|
| 1.   | In router configuration mode, enable IGMP globally.                                         | <b>ip igmp</b>         |
| 2.   | In router configuration mode, enable DVMRP globally.                                        | <b>ip dvmrp</b>        |
| 3.   | In router configuration mode, enable IGMP on each VLAN interface on which DVMRP will run.   | <b>ip igmp enable</b>  |
| 4.   | In router configuration mode, enable DVMRP for each VLAN interface on which DVMRP will run. | <b>ip dvmrp enable</b> |

### Example DVMRP Configuration

[Figure 19-5](#) on page 19-19 illustrates the DVMRP configuration of two Enterasys devices shown in the example below. This example assumes the following:

- VLANs have been configured and enabled with IP interfaces
- IGMP has been enabled on the VLANs

**Figure 19-5 DVMRP Configuration on Two Routers**



### Router R1 Configuration

For the VLAN 1 interface, which provides connection to Router R2, an IP address is assigned and DVMRP is enabled. For the VLAN 2 interface, which provides connection to the host network, an IP address is assigned and DVMRP is enabled.

```
System1 (su) ->router
System1 (su) ->router>enable
```

```
System1(su)->router#configure
 Enter configuration commands:
System1(su)->router(Config)#ip igmp
System1(su)->router(Config)#ip dvmrp
System1(su)->router(Config)#interface vlan 1
System1(su)->router(Config-if(Vlan 1))#ip address 192.0.1.2 255.255.255.0
System1(su)->router(Config-if(Vlan 1))#ip igmp enable
System1(su)->router(Config-if(Vlan 1))#ip dvmrp enable
System1(su)->router(Config-if(Vlan 1))#no shutdown
System1(su)->router(Config-if(Vlan 1))#exit
System1(su)->router(Config)#interface vlan 2
System1(su)->router(Config-if(Vlan 2))#ip address 192.40.0.1 255.255.255.0
System1(su)->router(Config-if(Vlan 2))#ip igmp enable
System1(su)->router(Config-if(Vlan 2))#ip dvmrp enable
System1(su)->router(Config-if(Vlan 2))#no shutdown
System1(su)->router(Config-if(Vlan 2))#exit
```

### Router R2 Configuration

For the VLAN 1 interface, which provides connection to the Router R1, an IP address is assigned and DVMRP is enabled. For the VLAN 3 interface which provides connection to the host network, an IP address is assigned and DVMRP is enabled.

```
System2(su)->router
System2(su)->router>enable
System2(su)->router#configure
 Enter configuration commands:
System2(su)->router(Config)#ip igmp
System2(su)->router(Config)#ip dvmrp
System2(su)->router(Config)#interface vlan 1
System2(su)->router(Config-if(Vlan 1))#ip address 192.0.1.1 255.255.255.0
System2(su)->router(Config-if(Vlan 1))#ip igmp enable
System2(su)->router(Config-if(Vlan 1))#ip dvmrp enable
System2(su)->router(Config-if(Vlan 1))#no shutdown
System2(su)->router(Config-if(Vlan 1))#exit
System2(su)->router(Config)#interface vlan 3
System2(su)->router(Config-if(Vlan 3))#ip address 192.20.0.1 255.255.255.0
System2(su)->router(Config-if(Vlan 3))#ip igmp enable
System2(su)->router(Config-if(Vlan 3))#ip dvmrp enable
System2(su)->router(Config-if(Vlan 3))#no shutdown
System2(su)->router(Config-if(Vlan 3))#exit
```

## Displaying DVMRP Information

[Table 19-8](#) lists the DVMRP show commands for the fixed switches that support and have enabled advanced routing.

**Table 19-8 DVMRP Show Commands**

| Task                                                                             | Command                                                                                                     |
|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Display DVMRP routing information, neighbor information, or DVMRP enable status. | <b>show ip dvmrp</b> [ <i>route</i>   <i>neighbor</i>   <i>status</i> ]                                     |
| Display the IP multicast routing table.                                          | <b>show ip mroute</b> [ <i>unicast-source-address</i>   <i>multicast-group-address</i> ] [ <i>summary</i> ] |

Refer to the device's *CLI Reference Guide*, as applicable, for an example of each command's output.

## Configuring PIM-SM

PIM-SM is an advanced routing feature that must be enabled with a license key.

### Design Considerations

Enterasys Networks recommends that administrators consider the following recommendations before configuring the fixed switch platforms for a PIM-SM environment.

- A fixed switch device **cannot** be configured as a Candidate-RP or a Candidate-BSR.
- A fixed switch device **should not** be the first hop router for a multicast stream. In other words, the multicast stream **should not** originate on a fixed switch device.
- A fixed switch device **should not** be positioned in the core of a PIM-SM topology, and **should only** be positioned at the edge in a PIM-SM topology. In other words, the fixed switch device **should only** be used to deliver multicast streams to end clients.

### PIM-SM Configuration Commands

[Table 19-9](#) lists the PIM-SM set commands for stackable and standalone devices that support and have enabled advanced routing.

**Table 19-9 PIM-SM Set Commands**

| Task                                                                                                                                                                                                              | Command                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Set the administrative mode of PIM-SM multicast routing across the router to enabled. By default, PIM-SM is globally disabled. Use the <b>no</b> command to disable PIM (across the entire stack, if applicable). | <b>ip pimsm</b><br><b>no ip pimsm</b>                                                                                                   |
| Create a manual RP IP address for the PIM-SM router. Use the <b>no</b> command to remove a previously configured RP.                                                                                              | <b>ip pimsm staticrp</b> <i>ipaddress groupaddress groupmask</i><br><b>no ip pimsm staticrp</b> <i>ipaddress groupaddress groupmask</i> |
| Enable PIM-SM multicast routing on a routing interface. By default, PIM is disabled on all IP interfaces. Use the <b>no</b> command to disable PIM on the specific interface.                                     | <b>ip pimsm enable</b><br><b>no ip pimsm enable</b>                                                                                     |
| Configure the transmission frequency of hello messages, in seconds, between PIM-enabled neighbors. Use the <b>no</b> command to reset the hello interval to the default, 30 seconds.                              | <b>ip pimsm query-interval</b> <i>seconds</i><br><b>no ip pimsm query-interval</b>                                                      |

## Basic PIM-SM Configuration

By default, PIM-SM is disabled globally on Enterasys fixed switches and attached interfaces.

Basic PIM-SM configuration includes the following steps:

1. Creating and enabling VLANs with IP interfaces.
2. Configuring the underlying unicast routing protocol (for example, OSPF).
3. Enabling IGMP on the device and on the VLANs.
4. Configuring PIM-SM on the device and on the VLANs.

[Procedure 19-4](#) assumes the following:

- VLANs have been configured and enabled with IP interfaces.
- The unicast routing protocol has been configured.
- IGMP has been enabled on the devices and VLANs that will be connected with hosts. For information on enabling IGMP, see “[Configuring IGMP](#)” on page 19-15.

[Procedure 19-4](#) describes the basic steps to configure PIM-SM on stackable C3 and C5 devices and standalone G-Series devices.

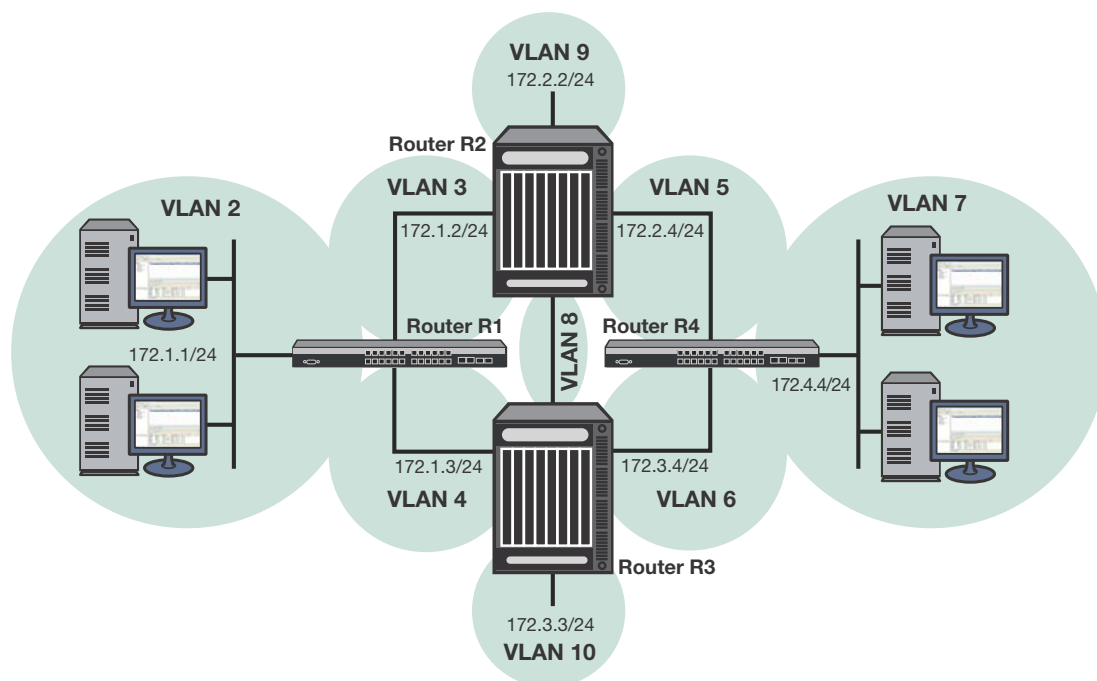
### Procedure 19-4 Basic PIM-SM Configuration

| Step | Task                                                                                                 | Command(s)                                                       |
|------|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| 1.   | In global configuration mode, enable PIM-SM on the device.                                           | <b>ip pimsm</b>                                                  |
| 2.   | In global configuration mode, if desired, create a manual RP IP address for the PIM-SM router.       | <b>ip pimsm staticrp</b> <i>ipaddress groupaddress groupmask</i> |
| 3.   | In interface configuration mode, enable PIM-SM on the device's VLAN interfaces that will run PIM-SM. | <b>ip pimsm enable</b>                                           |

### Example Configuration

[Figure 19-6](#) illustrates a PIM-SM configuration where two fixed switches are located at the edge of the PIM-SM topology. They are used to deliver multicast streams to end users only. The following configuration example does not include configuring Routers R2 and R3, which could be S-Series switches. Refer to the *S-Series Configuration Guide* for more information.

Figure 19-6 PIM-SM Configuration



### Routers R1 and R4 Configuration

On Router R1, at the switch level, IGMP snooping is enabled globally and on the ports connected to hosts. At router level (Level 3), the IGMP querier function is enabled on the device, and IGMP is enabled on VLAN 2, which connects to hosts. IGMP is used to determine host group membership on directly attached subnets. PIM-SM is enabled globally and on all interfaces. The underlying unicast routing protocol is OSPF.

The configuration on Router R4 would be the same, but would use different VLANs, IP addresses, and router ID.

```
R1(su)->set igmpsnooping adminmode enable
R1(su)->set igmpsnooping interfacemode ge.1.1-10 enable

R1(su)->router
R1(su)->router>enable
R1(su)->router#configure
 Enter configuration commands:
R1(su)->router(Config)#ip igmp
R1(su)->router(Config)#ip pimsm

R1(su)->router(Config)#interface vlan 2
R1(su)->router(Config-if(Vlan 2))#ip address 172.1.1.1 255.255.255.0
R1(su)->router(Config-if(Vlan 2))#ip igmp enable
R1(su)->router(Config-if(Vlan 2))#ip ospf enable
R1(su)->router(Config-if(Vlan 2))#ip pimsm enable
R1(su)->router(Config-if(Vlan 2))#no shutdown
R1(su)->router(Config-if(Vlan 2))#exit
```

```

R1(su)->router(Config)#interface vlan 3
R1(su)->router(Config-if(Vlan 3))#ip address 172.1.2.1 255.255.255.0
R1(su)->router(Config-if(Vlan 3))#ip igmp enable
R1(su)->router(Config-if(Vlan 3))#ip ospf enable
R1(su)->router(Config-if(Vlan 3))#ip pimsm enable
R1(su)->router(Config-if(Vlan 3))#no shutdown
R1(su)->router(Config-if(Vlan 3))#exit

R1(su)->router(Config)#interface vlan 4
R1(su)->router(Config-if(Vlan 4))#ip address 172.1.3.1 255.255.255.0
R1(su)->router(Config-if(Vlan 4))#ip igmp enable
R1(su)->router(Config-if(Vlan 4))#ip ospf enable
R1(su)->router(Config-if(Vlan 4))#ip pimsm enable
R1(su)->router(Config-if(Vlan 4))#no shutdown
R1(su)->router(Config-if(Vlan 4))#exit

R1(su)->router(Config)#router id 1.1.1.1
R1(su)->router(Config)#router ospf 1

```

## PIM-SM Display Commands

[Table 19-10](#) lists the PIM show commands for stackable C3 and C5 devices and standalone G-Series devices.

**Table 19-10 PIM-SM Show Commands**

| Task                                                                                                                                                                  | Command                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Display system-wide PIM-SM routing information.                                                                                                                       | <b>show ip pimsm</b>                                                                                        |
| Display the table containing objects specific to a PIM domain.                                                                                                        | <b>show ip pimsm componenttable</b>                                                                         |
| Display PIM-SM status of the router interfaces. With the <b>stats</b> parameter, this command displays statistical information for PIM-SM on the specified interface. | <b>show ip pimsm interface</b> {vlan <i>vlan-id</i>   <b>stats</b> { <i>vlan-id</i>   <b>all</b> }}         |
| Display the router's PIM neighbors.                                                                                                                                   | <b>show ip pimsm neighbor</b> [ <i>vlan-id</i> ]                                                            |
| Display the PIM information for candidate RPs for all IP multicast groups or for a specific group address.                                                            | <b>show ip pimsm rp</b> { <i>group-address group-mask</i>   <b>all</b>   <b>candidate</b> }                 |
| Display the RP that will be selected from the set of active RP routers.                                                                                               | <b>show ip pimsm rphash</b> <i>group-address</i>                                                            |
| Display the PIM-SM static RP information.                                                                                                                             | <b>show ip pimsm staticrp</b>                                                                               |
| Display the IP multicast routing table.                                                                                                                               | <b>show ip mroute</b> [ <i>unicast-source-address</i>   <i>multicast-group-address</i> ] [ <b>summary</b> ] |



## IP Configuration

This chapter provides general IPv4 routing configuration information.

| For information about...                        | Refer to page... |
|-------------------------------------------------|------------------|
| <a href="#">Enabling the Switch for Routing</a> | 20-1             |
| <a href="#">Routing Interfaces</a>              | 20-3             |
| <a href="#">IP Static Routes</a>                | 20-4             |
| <a href="#">Testing Network Connectivity</a>    | 20-5             |
| <a href="#">The ARP Table</a>                   | 20-6             |
| <a href="#">IP Broadcast Settings</a>           | 20-7             |
| <a href="#">Configuring ICMP Redirects</a>      | 20-10            |
| <a href="#">Terms and Definitions</a>           | 20-10            |

For information about

- Configuring RIP or IRDP protocols, refer to [Chapter 21, IPv4 Basic Routing Protocols](#)
- Configuring OSPF, refer to [Chapter 22, Configuring OSPFv2](#)
- Configuring DVMRP or PIM-SM, refer to [Chapter 19, Configuring Multicast](#)
- Configuring VRRP, refer to [Chapter 23, Configuring VRRP](#).
- IPv6 routing, refer to [Chapter 25, Configuring and Managing IPv6](#).

## Enabling the Switch for Routing

Startup and general configuration of the fixed switch must occur from the switch CLI. Once startup and general switch settings are complete, IP configuration and other router-specific commands can be executed when the switch is in router mode.

This chapter describes the various router modes and how to navigate them, how to configure a routing interface, how to configure static routes and IP broadcast settings, and how to manage the ARP table.

## Router Configuration Modes

The fixed switch CLI provides different modes of router operation for issuing a subset of commands from each mode. [Table 20-1](#) describes these modes of operation.

**Table 20-1 Router CLI Configuration Modes**

| Use this mode...             | To...                                                                                                                                                | Access method...                                                                                                              | Resulting Prompt...                                                        |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Privileged EXEC Mode         | Show configuration parameters and statistics<br><br>Restart the OSPF process (advanced feature)<br><br>Debug network issues with ping and traceroute | From the switch CLI:<br>Type <b>router</b> , then<br>Type <b>enable</b> .                                                     | C5(su)->router><br>C5(su)->router#                                         |
| Global Configuration Mode    | Set system-wide router parameters.                                                                                                                   | Type <b>configure</b> from Privileged EXEC mode.                                                                              | C5(su)->router (Config)#                                                   |
| Interface Configuration Mode | Configure router interfaces.                                                                                                                         | Type <b>interface vlan</b> or <b>loopback</b> and the interface's id from Global Configuration mode.                          | C5(su)->router(Config-if (Vlan 1))#<br>C5(su)->router(Config-if (Lpbk 1))# |
| Router Configuration Mode    | Set IP protocol parameters.                                                                                                                          | Type <b>router</b> and the protocol <i>name</i> (and, for OSPF, the instance ID) from Global or Interface Configuration mode. | C5(su)->router(Config-router)#                                             |



**Note:** To jump to a lower configuration mode, type **exit** at the command prompt. To revert back to switch CLI, type **exit** from Privileged EXEC router mode.

## Entering Router Configuration Modes

[Procedure 20-1](#) shows the tasks to enter router protocol configuration mode and router interface mode.

**Procedure 20-1 Entering Router Configuration Mode**

| Step | Task                                                                                            | Command(s)                                                                |
|------|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| 1.   | From switch mode, enable router mode.                                                           | <b>router</b>                                                             |
| 2.   | Enable router Privileged EXEC mode.                                                             | <b>enable</b>                                                             |
| 3.   | Enable global router configuration mode.                                                        | <b>configure</b>                                                          |
| 4.   | Enable router configuration mode to set the routing protocol parameters.                        | <b>router</b> <i>protocol-name</i>                                        |
| 5.   | When finished configuring the routing protocol parameters, return to global configuration mode. | <b>exit</b>                                                               |
| 6.   | Enable interface configuration mode using the routing VLAN or loopback id.                      | <b>interface</b> { <i>vlan vlan-id</i>   <b>loopback</b> <i>loop-id</i> } |
| 7.   | Assign an IP address to the routing interface.                                                  | <b>ip address</b> { <i>ip-address ip-mask</i> }                           |
| 8.   | Enable the interface for IP routing.                                                            | <b>no shutdown</b>                                                        |
| 9.   | When finished configuring the interface parameters, return to global configuration mode.        | <b>exit</b>                                                               |

## Example

The following example shows how to enable RIP on the switch, then configure VLAN 1 with IP address 192.168.63.1 255.255.255.0 as a routing interface and enable RIP on the interface.

```
C5(su)->router
C5(su)->router>enable
C5(su)->router#configure
 Enter configuration commands:
C5(su)->router(Config)#router rip
C5(su)->router(Config-router)#exit
C5(su)->router(Config)#interface vlan 1
C5(su)->router(Config-if(Vlan 1))#ip address 192.168.63.1 255.255.255.0
C5(su)->router(Config-if(Vlan 1))#no shutdown
C5(su)->router(Config-if(Vlan 1))#ip rip enable
C5(su)->router(Config-if(Vlan 1))#exit
C5(su)->router(Config)#
```

## Routing Interfaces

Routing interfaces are created using the **interface** command in router global configuration mode. The **interface** command enables router interface configuration mode from global configuration mode, and, if the interface has not previously been created, creates a new routing interface.

VLANs must be created from the switch CLI before they can be configured for IP routing. For details on creating VLANs and configuring them for IP, refer to [Chapter 9, Configuring VLANs](#).

Each VLAN interface must be configured for routing separately using the **interface** command. To end configuration on one interface before configuring another, type **exit** at the command prompt. Enabling interface configuration mode is required for completing interface-specific configuration tasks.

A loopback interface is always expected to be up. This interface can provide the source address for sent packets and can receive both local and remote packets. The loopback interface is typically used by routing protocols, but it can also be used for management or network services such as RADIUS, SNMP, Syslog, SNTP, or sFlow. By default, if RADIUS is configured with no host IP address on the device, it will use the loopback interface 0 IP address (if it has been configured) as its source for the NAS-IP attribute. (Administrators can assign where to source management or network service IP packets via the **set interface** commands.)

Fixed switch platforms support different numbers of primary and secondary IP routing interfaces. Refer to the Release Notes for your platform for the number of interfaces supported. Each interface can be configured for the RIP (and/or OSPF, on platforms that support advanced routing features) routing protocols.

By default, IP routing is enabled when interfaces are configured for it. Use the **no ip routing** command at router global configuration mode to disable routing on the switch.

## IPv4 Interface Addresses

A single primary IP address must be configured on each routing interface. Secondary IP addresses can optionally be configured. The first network IP address assigned to an interface is the primary address. To configure a secondary network IP address on an interface, the address must be explicitly configured as secondary — otherwise, you will overwrite the current primary.

Use the **ip address** command in interface configuration command mode to assign IP networks as primary or secondary to a routing interface.

[Procedure 20-2](#) describes how to configure the routing interface.

**Procedure 20-2 Configuring the Routing Interface**

| Step | Task                                                                                                                                                 | Command(s)                                                            |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| 1.   | Enter router interface configuration command mode for the specified interface from global configuration command mode.                                | <b>interface</b> {vlan <i>vlan-id</i>   loopback <i>loopback-id</i> } |
| 2.   | Set the primary, and optionally the secondary, IPv4 address for this interface, in interface configuration command mode.                             | <b>ip address</b> <i>ip-address ip-mask</i> [ <b>secondary</b> ]      |
| 3.   | Enable this interface for IP routing and allow the interface to automatically be enabled at device startup, in interface configuration command mode. | <b>no shutdown</b>                                                    |

The following example configures a primary and secondary IP address on VLAN 100, then displays the VLAN 100 interface configuration:

```
C5(su)->router
C5(su)->router>enable
C5(su)->router#configure
 Enter configuration commands:
C5(su)->router(Config)#interface vlan 100
C5(su)->router(Config-if(Vlan 100))#ip address 192.168.63.1 255.255.255.0
C5(su)->router(Config-if(Vlan 100))#ip address 192.168.65.1 255.255.255.0
secondary
C5(su)->router(Config-if(Vlan 1))#no shutdown
C5(su)->router(Config-if(Vlan 1))#exit

C5(su)->router(Config)#show interface vlan 100

Vlan 100 is Administratively DOWN
Vlan 100 is Operationally DOWN
Internet Address is 192.168.63.1 , Subnet Mask is 255.255.255.0
Internet Address is 192.168.64.1 , Subnet Mask is 255.255.255.0 Secondary
Mac Address is: 001F.4554.F689
The name of this device is Vlan 100
The MTU is 1500 bytes
The bandwidth is 0 Mb/s
Encapsulation type Ethernet
ARP Timeout: 14400 seconds
```

The **no ip address** command removes the specified IPv4 address configuration for this interface.

## IP Static Routes

Static routes are configured in router global configuration mode using the **ip route** command. IP static routes are configured by specifying the destination IPv4 prefix and mask for the route and the next hop router (gateway) IP address.

An administrative distance can be optionally configured that is used for route selection preference. The lower the numeric distance value, the greater the preference for the route.

Static routes can be removed from the routing table with the **no ip route** command.

Use the **show ip route** command to display IP routes known by the switch, both learned and static.

## Configuring Static Routes

Procedure 20-3 lists the commands to configure a static route.

### Procedure 20-3 Configuring Static Routes

| Step | Task                                                          | Command(s)                                                                         |
|------|---------------------------------------------------------------|------------------------------------------------------------------------------------|
| 1.   | In global configuration mode, configure an IPv4 static route. | <b>ip route</b> <i>dest-prefix dest-prefix-mask forwarding-rtr-addr [distance]</i> |
| 2.   | Optionally, remove a static route.                            | <b>no ip route</b> <i>dest-prefix dest-prefix-mask forwarding-rtr-addr</i>         |
| 3.   | Display the routing table, including static routes            | <b>show ip route</b>                                                               |

The following example configures a static route in routing mode and then displays the IP routing table.

```
C5(su)->router(Config)#ip route 9.9.9.248 255.255.255.248 61.168.4.254
C5(su)->router(Config)#show ip route
```

Codes: C - connected, S - static, R - RIP, O - OSPF, IA - OSPF interarea  
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
 E1 - OSPF external type 1, E2 - OSPF external type 2  
 E - EGP, i - IS-IS, L1 - IS-IS level-1, LS - IS-IS level-2  
 \* - candidate default, U - per user static route

```
E1 2.2.1.0/24 [110/31] via 61.168.4.254, Vlan 1600
E2 3.3.3.0/24 [110/20] via 61.168.4.254, Vlan 1600
S 9.9.9.248/29 [99/0] via 61.168.4.254, Vlan 1600
E2 11.11.11.240/28 [110/14] via 61.168.4.254, Vlan 1600
E2 12.12.12.252/30 [110/9] via 61.201.161.198, Vlan 3041
C 30.1.1.0/24 [0/1] directly connected, Vlan 300
C 30.1.2.0/24 [0/1] directly connected, Vlan 301
C 30.1.3.0/24 [0/1] directly connected, Vlan 302
E2 61.0.0.1/32 [110/20] via 61.33.9.8, Vlan 3398
S 61.1.128.0/17 [1/0] via 61.168.4.254, Vlan 1600
S 61.2.0.0/15 [1/0] via 61.33.9.8, Vlan 3398
N2 61.5.1.1/32 [110/20] via 61.201.1.30, Vlan 3210
C 61.15.0.0/21 [0/1] directly connected, Vlan 115
E2 61.19.0.0/30 [110/9] via 61.201.161.198, Vlan 3041
O 61.21.21.0/30 [110/11] via 61.33.9.8, Vlan 3398
O 61.24.24.0/24 [110/20] via 61.201.161.198, Vlan 3041
E2 61.31.0.0/16 [110/20] via 61.33.9.8, Vlan 3398
C 61.33.9.0/28 [0/1] directly connected, Vlan 3398
E2 61.35.22.0/24 [110/20] via 61.201.161.198, Vlan 3041
E2 61.35.23.0/24 [110/20] via 61.168.4.254, Vlan 1600
O 61.50.0.0/29 [110/20] via 61.201.161.198, Vlan 3041
O 61.51.0.0/29 [110/11] via 61.33.9.8, Vlan 3398
IA 61.79.0.0/16 [110/31] via 61.168.4.254, Vlan 1600
```

## Testing Network Connectivity

Use the **ping** command to test routing network connectivity by sending IP ping requests to a specific destination. The **ping** command is available in both switch and routing command modes.

This example shows output from a successful **ping** to IP address 182.127.63.23:

```
C5(su)->router#ping 182.127.63.23
182.127.63.23 is alive
```

Use the **tracert** command to display a hop-by-hop path through an IP network from the device to a specific destination host. Three ICMP probes will be transmitted for each hop between the source and the traceroute destination. The **tracert** command is available in both switch and routing command modes.

This example shows how to use **tracert** to display a round trip path to host 192.141.90.183.

```
C5(su)->router#tracert 192.141.90.183
Traceroute to 192.141.90.183, 30 hops max, 40 byte packets
 1 10.1.56.1 0.000 ms 0.000 ms 0.000 ms
 2 10.1.48.254 10.000 ms 0.000 ms 0.000 ms
 3 10.1.0.2 0.000 ms 0.000 ms 0.000 ms
 4 192.141.89.17 0.000 ms 0.000 ms 10.000 ms
 5 192.141.100.13 0.000 ms 10.000 ms 0.000 ms
 6 192.141.100.6 0.000 ms 0.000 ms 10.000 ms
 7 192.141.90.183 0.000 ms 0.000 ms 0.000 ms
```

## The ARP Table

Address Resolution Protocol (ARP) is the method for finding a MAC hardware address when only the IP address is known. The fixed switch firmware allows you to configure Address Resolution Protocol (ARP) table entries and parameters. ARP is used to associate IP addresses with MAC addresses. Once determined, the IP address and MAC association is stored in an ARP cache for rapid retrieval. An IP datagram is then encapsulated into a link-layer frame and sent over the network.

ARP table entries can be temporary (dynamic) or permanent. A temporary ARP entry has a timeout interval associated with it. The ARP entry expires at the end of the timeout interval.

You can configure an ARP entry in routing mode or in switch mode. If you set a static route in router configuration mode, the IP address specified for the static ARP entry must fall within one of the subnets or networks defined on the routed interfaces of the system. The system can then match the IP address of the static ARP entry with the appropriate routed interface and associate it with the correct VLAN.

Refer to the Router Capacities table in the Release Notes for your fixed switch product for a listing of the number of static ARP entries supported by the product.

- In routing mode, use
  - the **arp** command to configure a permanent static ARP entry. A multicast MAC address can be used in a static ARP entry.
  - the **no arp** command to remove a static ARP entry.
  - the **arp timeout** command to set the duration in seconds for dynamically learned entries to remain in the ARP table before expiring. The default value is 14,400 seconds.
  - the **show ip arp** command to display ARP table entries.
  - the **clear arp-cache** command to clear all non-static (dynamic) ARP entries from the ARP table.

If you don't have routing configured, you can set a static ARP entry using the switch mode command line.

- In switch mode, use
  - the **set arp** command to add a mapping entry to the switch ARP table.

- the **clear arp** command to delete a specific entry or all entries from the switch ARP table.
- the **show arp** command to display the link level ARP table.

## Proxy ARP

This variation of the ARP protocol allows the router to send an ARP response on behalf of an end node to the requesting host. Proxy ARP can be used to resolve routing issues on end stations that are unable to route in the subnetted environment. The fixed switch will answer to ARP requests on behalf of targeted end stations on neighboring networks.

Proxy ARP is disabled by default and can be enabled per interface with the **ip proxy-arp** command in router interface configuration mode.

## ARP Configuration

[Procedure 20-4](#) on page 20-7 lists the commands used to configure the ARP table in router configuration mode.

### Procedure 20-4 Configuring the ARP Table

| Step | Task                                                                                                                               | Command(s)                                                                                             |
|------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| 1.   | In router global configuration mode, add static entries to the ARP table.                                                          | <b>arp</b> <i>ip-address mac-address</i>                                                               |
| 2.   | Optionally, in global configuration mode, change the duration that dynamic ARP entries will stay in the ARP table before expiring. | <b>arp timeout</b> <i>seconds</i>                                                                      |
| 3.   | Optionally, in router interface configuration mode, enable Proxy ARP on an interface.                                              | <b>ip proxy-arp</b>                                                                                    |
| 4.   | In any router mode, display the ARP table.                                                                                         | <b>show ip arp</b> [ <i>ip-address</i> ]   [ <b>vlan</b> <i>vlan-id</i> ]   [ <i>output-modifier</i> ] |
| 5.   | Optionally, clear the ARP cache.                                                                                                   | <b>clear arp cache</b>                                                                                 |

Refer to the CLI Reference for your platform for details about using the commands listed above.

The following example sets a static ARP entry in routing configuration mode, then displays the ARP table.

```
C5(su)->router(Config)#arp 134.141.235.165 0002.1664.a5b3
C5(su)->router(Config)#show ip arp
Protocol Address Age (min) Hardware Addr Interface

Internet 134.141.235.251 0 0003.4712.7a99 Vlan1
Internet 134.141.235.165 - 0002.1664.a5b3 Vlan1
Internet 134.141.235.167 4 00d0.cf00.4b74 Vlan2
```

## IP Broadcast Settings

### Directed Broadcast

Directed broadcast is an efficient mechanism for communicating with multiple hosts on a network while only transmitting a single datagram. A directed broadcast is a packet sent to all hosts on a

specific network or subnet. The directed broadcast address includes the network or subnet fields, with the binary bits of the host portion of the address set to one. For example, for a network with the address 192.168.0.0/16, the directed broadcast address would be 192.168.255.255. For a subnet with the address 192.168.12.0/24, the directed broadcast address would be 192.168.12.255.

In order to minimize broadcast DoS attacks, forwarding of directed broadcasts is disabled by default on the fixed switches, as recommended by RFC 2644.

If the ability to send directed broadcasts to a network is required, you should enable directed broadcasts only on the one interface that will be transmitting the datagrams. For example, if a switch has five routed interfaces for the 10, 20, 30, 40, and 50 networks, enabling directed broadcast only on the 30 network interface will allow anyone from any of the other networks (10, 20, 40, 50) to send directed broadcast to the 30 network.

Use the **ip directed-broadcast** command in router interface configuration mode to enable IP directed broadcasts on an interface.

## UDP Broadcast Forwarding

Typically, broadcast packets from one interface are not forwarded (routed) to another interface. However, some applications use UDP broadcasts to detect the availability of services, and some protocols, such as BOOTP/DHCP, require broadcast forwarding to provide services to clients on other subnets.

Configuring UDP broadcast forwarding on the fixed switch device involves enabling it for one or more protocols with the **ip forward-protocol** command, and configuring an IP helper address on the individual router interfaces with the **ip helper-address** command. For all protocols specified with the **ip forward-protocol** command except DHCP/BOOTP, the system forward broadcast UDP traffic as a unicast packet to the specified IP addresses. Refer to “[DHCP and BOOTP Relay](#)” on page 20-9 for more information about DHCP/BOOTP processing.

If a certain service exists inside the device, and there is no need to forward the request to remote networks, the **no** form of the **ip forward-protocol** command should be used to disable the forwarding for the specific port. Such requests will not be automatically blocked from being forwarded just because a service for them exists in the switch.

By default, UDP broadcast forwarding is enabled, with no port specified.

If *port* is not specified, the following defaults are used:

**Table 20-2 UDP Broadcast Forwarding Port Default**

| Port Number | Protocol                              |
|-------------|---------------------------------------|
| 0           | Reserved                              |
| 7           | Echo                                  |
| 9           | Discard                               |
| 37          | Time Service                          |
| 42          | EN-116 Name Service                   |
| 49          | TACACS Service                        |
| 53          | Domain Naming System                  |
| 69          | Trivial File Transfer Protocol (TFTP) |
| 137         | NetBIOS Name Server                   |
| 138         | NetBIOS Datagram Server               |



**Table 20-2 UDP Broadcast Forwarding Port Default (continued)**

| Port Number | Protocol               |
|-------------|------------------------|
| 4011        | Alternate Service Boot |

The **no** form of the **ip forward-protocol** command removes a UDP port or protocol, disabling forwarding.

## DHCP and BOOTP Relay

DHCP/BOOTP relay functionality is applied with the help of UDP broadcast forwarding. A typical situation occurs when a host requests an IP address with no DHCP server located on that segment. A routing device can forward the DHCP request to a server located on another network if:

- UDP broadcast forwarding is enabled
- The address of the DHCP server is configured as a helper address on the receiving interface

The DHCP/BOOTP relay agent function will detect the DHCP request and make the necessary changes to the packet, including:

- Replacing the destination IP address with the address of the DHCP server,
- Replacing the source IP address with its own address (that is, the IP address of the local routed interface), and
- Within the BOOTP part of the packet, changing the Relay Agent IP address from 0.0.0.0 to the address of the local routed interface.

The last change to the BOOTP packet “tells” the DHCP server that it needs to assign an IP address that is in the same subnet as the Relay Agent IP. When the response comes from the server, the DHCP/BOOTP relay agent sends it to the host.

Use the **ip helper-address** command in conjunction with the **ip forward-protocol** command to configure DHCP/BOOTP relay functionality to the specified server(s). Up to 6 IP helper addresses may be configured per interface.

## IP Broadcast Configuration

[Procedure 20-5](#) describes how to configure IP broadcast.

### Procedure 20-5 Configuring IP Broadcast

| Step | Task                                                                                                                                                                                                                                         | Command(s)                            |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| 1.   | In interface configuration command mode, enable IP directed broadcasts on an interface.                                                                                                                                                      | <b>ip directed-broadcast</b>          |
| 2.   | In interface configuration command mode, enable UDP broadcast forwarding and specify the destination port number that controls the forwarding protocol. Refer to <a href="#">Table 20-2</a> on page 20-8 for a list of default port numbers. | <b>ip forward-protocol udp [port]</b> |
| 3.   | In interface configuration command mode, optionally, enable DHCP/BOOTP relay and the forwarding of local UDP broadcasts, specifying a new destination address.                                                                               | <b>ip helper-address address</b>      |

This example shows how to enable IP directed broadcasts on VLAN 1 and have all client DHCP requests for users in VLAN 1 to be forwarded to the remote DHCP server with IP address 192.168.1.28

```
C5(su)->router(Config)#interface vlan 1
C5(su)->router(Config-if(Vlan 1))#ip directed-broadcast
C5(su)->router(Config-if(Vlan 1))#ip forward-protocol udp
C5(su)->router(Config-if(Vlan 1))#ip helper-address 192.168.1.28
```

## Configuring ICMP Redirects

You can disable or enable sending ICMP redirect packets to the switch CPU for processing, at a global level and at an interface level. By default, sending ICMP redirects is enabled globally and on all interfaces. Disabling sending ICMP redirects can reduce CPU usage in certain deployments.



**Note:** On the A4 platforms, you can only enable or disable ICMP redirects at an interface level, not at a global device level.

Use the **ip icmp redirect enable** command to enable or disable sending ICMP redirects to the CPU for processing. The **no** form of the command disables sending ICMP redirects to the CPU.

Use the **show ip icmp redirect** command to display the status of sending ICMP redirects.

This example disables sending ICMP redirects on the interface VLAN 5 and then displays the ICMP redirect status for VLAN 5

```
C5(su)->router#configure
C5(su)->router(Config)#interface vlan 5
C5(su)->Router1(Config-if(Vlan 5))# no ip icmp redirect enable
C5(su)->Router1(Config-if(Vlan 5))#exit

C5(su)->router(Config)#show ip icmp redirect interface vlan 5
Vlan Id Admin Status

5 Disabled
```

## Terms and Definitions

[Table 20-3](#) lists terms and definitions used in this IP routing configuration discussion.

**Table 20-3 IP Routing Terms and Definitions**

| Term                              | Definition                                                                                                                                                                  |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Address Resolution Protocol (ARP) | A protocol providing a method for finding a MAC hardware address when only the IP address is known.                                                                         |
| ARP proxy                         | Provides for the ability of a device on a given network to answer the ARP queries for a network address that is not on that network.                                        |
| broadcast forwarding              | Provides for the ability for rout UDP broadcasts in order to provide services to clients on a different subnet than the one originating the broadcast.                      |
| directed broadcast                | The ability to address a destination host such that the arriving packet will be broadcasted to the network as if it was a normal broadcast generated by the receiving host. |
| IP address                        | An address used by the IP protocol to identify a routing interface or routing device.                                                                                       |
| IP address helper                 | The ability to specify the IP address the UDP forwarded packet should be sent to.                                                                                           |

**Table 20-3 IP Routing Terms and Definitions (continued)**

| Term              | Definition                                                                                                                                                                    |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| relay agent       | A DHCPv6 application that provides a means for relaying DHCPv6 requests between a subnet to which no DHCP server is connected to other subnets on which servers are attached. |
| routing interface | A VLAN or loopback interface configured for IP routing.                                                                                                                       |
| static route      | An administratively configured IP route consisting of the destination and next-hop IP addresses from the IP router the route is configured on.                                |



---

## IPv4 Basic Routing Protocols

This chapter describes how to configure the Routing Information Protocol (RIP) and the ICMP Router Discovery Protocol (IRDP).

| For information about...         | Refer to page... |
|----------------------------------|------------------|
| <a href="#">Configuring RIP</a>  | 21-1             |
| <a href="#">Configuring IRDP</a> | 21-5             |

### Configuring RIP

#### Using RIP in Your Network

The fixed switches support Routing Information Protocol (RIP) Version 1 and 2. RIP is a distance-vector routing protocol for use in small networks — it is not intended for complex networks. RIP is described in RFC 2453. A router, running RIP broadcasts, updates at set intervals. Each update contains paired values where each pair consists of an IP network address and an integer distance to that network. RIP uses a hop count metric to measure the distance to a destination and is not appropriate for situations where routes need to be chosen based on real-time parameters such as a measured delay, reliability, or load.

The fixed switch devices implement plain text and MD5 authentication methods for RIP.

#### RIP Configuration Overview

Enabling RIP on the device starts the RIP process which then begins populating its routing table and sending and receiving routing updates. Use the **router rip** command in configuration command mode to both enable RIP on the device and enter RIP router configuration mode.

Refer to [Table 21-2](#) on page 21-3 for a list of default RIP parameter values.

#### RIP Router Configuration

Once in router configuration mode, you can configure the administrative distance for RIP routes with the **distance** command. If several routes (coming from different protocols) are presented to the switch, the protocol with the lowest administrative distance will be chosen for route installation. You can change the default RIP administrative distance value of 120 with the **distance** command, resetting RIP's route preference in relation to other routes as shown in [Table 21-1](#) on page 21-2 below.

**Table 21-1 Routing Protocol Route Preferences**

| Route Source                                                        | Default Distance |
|---------------------------------------------------------------------|------------------|
| Connected                                                           | 0                |
| Static                                                              | 1                |
| OSPF (Requires support for advanced routing features on the switch) | 110              |
| RIP                                                                 | 120              |

Also in router configuration mode, you can disable automatic route summarization with the **no auto-summary** command. By default, RIP version 2 supports automatic route summarization, which summarizes sub-prefixes to the classful network boundary when crossing network boundaries. Disabling automatic route summarization enables CIDR, allowing RIP to advertise all subnets and host routing information on the fixed switch device. To verify which routes are summarized for an interface, use the **show ip route** command. The reverse of the command (**auto-summary**) re-enables automatic route summarization. By default, RIP auto-summarization affects both RIPv1 and RIPv2 routes.



**Note:** The **no auto-summary** command is necessary for enabling CIDR for RIP on the fixed switch devices.

Other parameters that you can set in router configuration mode include:

- Split horizon, which prevents a network from being advertised out the same interface it was received on. This function is disabled by default.  
Use the **split-horizon poison** command to enable or disable split horizon poison-reverse mode for RIP packets. The **no** form of the command disables split horizon poison reverse.
- Passive interface, which prevents RIP from transmitting update packets on an interface. Use the **passive-interface** command to configure a routing VLAN interface as passive, or the **no** form of the command to disable passive interface. Configuring an interface as passive does not prevent RIP from monitoring updates on the interface.
- Use the **receive-interface** command to allow RIP to receive update packets on a routing VLAN interface. The **no** form of the command denies the reception of RIP updates. By default, receiving is enabled on all routing interfaces. This command does not affect the sending of RIP updates on the specified interface.
- You can allow routing information discovered through non-RIP protocols to be distributed in RIP update messages. Use the **redistribute** command to configure the protocols that can be redistributed. The **no** form of the **redistribute** command clears redistribution parameters.

## RIP Interface Configuration

Separately from configuring the router parameters, you must enable RIP on individual routing interfaces using the **ip rip enable** command in interface configuration mode. Other optional parameters that can be configured in interface configuration mode include:

- The RIP version to use for RIP update packets sent out an interface. You can specify version 1 (the default), version 2, or R1 compatible. R1 compatible specifies that packets be sent as version 2 packets, but transmits these as broadcast packets rather than multicast packets so that systems which only understand RIP version 1 can receive them.
- The RIP version or versions for RIP update packets accepted on the interface. You can specify version 1 (the default), version 2, both versions 1 and 2, or none, meaning that no RIP routes will be processed on the interface.

- Configure a RIP authentication key for use on the interface. Authentication can be either clear text or encrypted MD5.

## RIP Configuration Example

Table 21-2 lists the default RIP configuration values.

Procedure 21-1 lists the basic steps to configure RIP and the commands used.

**Table 21-2 RIP Default Values**

| Parameter                     | Description                                                                                                                                                                                                                                           | Default Value                           |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| RIP process                   | The RIP router process on the switch                                                                                                                                                                                                                  | disabled globally and on all interfaces |
| distance                      | The administrative distance that specifies the preference for RIP routing over other types on the switch                                                                                                                                              | 120                                     |
| automatic route summarization | Summarizes subprefixes to the classful network boundary when crossing network boundaries.<br><br>Disabling automatic route summarization enables CIDR, allowing RIP to advertise all subnets and host routing information on the fixed switch device. | enabled for V1 and V2                   |
| split horizon poison reverse  | Prevents a network from being advertised out the same interface it was received on.                                                                                                                                                                   | disabled                                |
| passive interface             | Prevents RIP from transmitting update packets on an interface.                                                                                                                                                                                        | disabled on all interfaces              |
| receive interface             | Allows RIP to receive update packets on an interface.                                                                                                                                                                                                 | enabled on all interfaces               |
| redistribution                | Allows routing information received from non-RIP protocols to be distributed in RIP update messages                                                                                                                                                   | disabled                                |
| send version                  | RIP version to use for RIP update packets sent out an interface.                                                                                                                                                                                      | version 1                               |
| receive version               | RIP version or versions for RIP update packets accepted on the interface.                                                                                                                                                                             | version 1                               |
| authentication                | Whether RIP uses authentication on an interface                                                                                                                                                                                                       | disabled                                |

Refer to the CLI Reference for your fixed switch platform for details about the commands listed in the following procedure.

### Procedure 21-1 Basic RIP Configuration

| Step | Task                                                                           | Command(s)                   |
|------|--------------------------------------------------------------------------------|------------------------------|
| 1.   | Enable RIP and enter router configuration mode.                                | <code>router rip</code>      |
| 2.   | In router configuration mode, optionally configure an administrative distance. | <code>distance weight</code> |

**Procedure 21-1 Basic RIP Configuration (continued)**

| Step | Task                                                                                                                                                                                                                                                             | Command(s)                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| 3.   | In router configuration mode, optionally disable automatic route summarization (necessary for enabling CIDR).                                                                                                                                                    | <code>no auto-summary</code>                                                                            |
| 4.   | In router configuration mode, optionally enable split horizon poison reverse.                                                                                                                                                                                    | <code>split-horizon poison</code>                                                                       |
| 5.   | In router configuration mode, optionally enable route redistribution of non-RIP protocol routes.<br><b>Note:</b> OSPF is an advanced routing feature that requires an advanced feature license and is only available on platforms that support advanced routing. | <code>redistribute {connected   ospf process-id   static} [metric metric value] [subnets]</code>        |
| 6.   | In router configuration mode, optionally configure an interface to not send RIP updates.                                                                                                                                                                         | <code>passive-interface vlan vlan-id</code>                                                             |
| 7.   | In router configuration mode, optionally configure an interface to not receive RIP updated packets.                                                                                                                                                              | <code>no receive-interface vlan vlan-id</code>                                                          |
| 8.   | In interface configuration mode, enable RIP on the interface.                                                                                                                                                                                                    | <code>ip rip enable</code>                                                                              |
| 9.   | In interface configuration mode, optionally configure the RIP version used to send RIP update packets.                                                                                                                                                           | <code>ip rip send version {1   2   r1compatible}</code>                                                 |
| 10.  | In interface configuration mode, optionally configure the RIP version for RIP update packets accepted on an interface.                                                                                                                                           | <code>ip rip receive version {1   2   1 2   none}</code>                                                |
| 11.  | In interface configuration mode, optionally configure authentication.<br><br>To configure a clear text authentication password to be used on the interface:<br><br>To configure MD5 authentication:                                                              | <code>ip rip authentication-key name</code><br><br><code>ip rip message-digest-key keyid md5 key</code> |

The following code example enables RIP on the router, disables automatic route summarization, then enables RIP on VLANs 5 and 10 and configures MD5 authentication. This example assumes that VLANs 5 and 10 have already been configured for routing.

```
C5(su)->router#configure
C5(su)->router(Config)#router rip
C5(su)->router(Config-router)# no auto-summary
C5(su)->router(Config-router)#exit
C5(su)->router(Config)#interface vlan 5
C5(su)->router(Config-if(Vlan 5))#ip rip enable
C5(su)->router(Config-if(Vlan 5))#ip rip message-digest-key 5 md5 password
C5(su)->router(Config-if(Vlan 5))#exit
C5(su)->router(Config)#interface vlan 10
C5(su)->router(Config-if(Vlan 10))#ip rip enable
C5(su)->router(Config-if(Vlan 10))#ip rip message-digest-key 10 md5 mypassword
C5(su)->router(Config-if(Vlan 10))#exit
C5(su)->router(Config)#
```



# Configuring IRDP

## Using IRDP in Your Network

The ICMP Router Discovery Protocol (IRDP), described in RFC 1256, enables a host on multicast or broadcast networks to determine the address of a router it can use as a default gateway. Routing interfaces that are enabled for IRDP periodically send out ICMP Router Advertisement messages announcing the IP address of that interface. Hosts on the link discover the addresses of their neighboring routers by listening for advertisements. Hosts on startup also may send out ICMP Router Solicitation messages to ask for immediate advertisements.

IRDP is disabled by default on fixed switch platforms.

## IRDP Configuration Overview

When you configure a routing VLAN interface to participate in IRDP, the only required step is to enable IRDP on the interface. You can keep the default values defined for the IRDP parameters, or change them:

- Maximum and minimum advertisement intervals — set the maximum and minimum intervals in seconds between IRDP advertisements sent by the routing interface. The default values set the advertising rate to once every 7 to 10 minutes.
- Advertisement lifetime or holdtime — sets the maximum length of time in seconds that the IP address sent in the IRDP advertisement should be considered valid.
- Router preference level — sets the preference level for the advertised router address. Hosts use this value when choosing a default router address, choosing the router address with the highest preference. You can use this value to encourage or discourage use of a particular router as a default router.
- Advertisement address — sets the IP destination address used in the advertisements sent by the interface. The only permissible values are the all-systems multicast address, 224.0.0.1, or the limited-broadcast address, 255.255.255.255.

## IRDP Configuration Example

[Table 21-3](#) lists the default IRDP configuration values.

[Procedure 21-2](#) on page 21-6 lists the basic steps to configure IRDP and the commands used.

**Table 21-3 IRDP Default Values**

| Parameter                      | Description                                                                                                                           | Default Value                                                         |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| IRDP process                   | The IRDP router process on the routing interfaces.                                                                                    | disabled on all interfaces                                            |
| maximum advertisement interval | The maximum time allowed between sending multicast router advertisements from the interface.<br>Can range between 4 and 1800 seconds. | 600 seconds                                                           |
| minimum advertisement interval | The minimum time allowed between sending multicast router advertisements from the interface.<br>Can be no less than 3 seconds.        | three-fourths of the maximum advertisement interval.<br>(450 seconds) |

**Table 21-3 IRDP Default Values (continued)**

| Parameter              | Description                                                                                                                   | Default Value                                                     |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| advertisement holdtime | The length of time this advertised address should be considered valid.<br>Can be no less than the max advertisement interval. | three times the maximum advertisement interval.<br>(1800 seconds) |
| preference level       | The preference value for this advertised address.                                                                             | 0                                                                 |
| advertisement address  | IP destination address for advertisements.                                                                                    | 224.0.0.1<br>(all-systems multicast address)                      |

Refer to the CLI Reference for your fixed switch platform for details about the commands listed in the following procedure. All commands are entered in router interface configuration mode.

**Procedure 21-2 Basic IRDP Configuration**

| Step | Task                                                                                                                                                                                                                                                                                                                             | Command(s)                                      |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| 1.   | Enable IRDP on the interface                                                                                                                                                                                                                                                                                                     | <code>ip irdp enable</code>                     |
| 2.   | Optionally, change the maximum advertisement interval. Valid values range from 4 to 1800 seconds.<br>Use the no form of the command to return to the default value.                                                                                                                                                              | <code>ip irdp maxadvertinterval interval</code> |
| 3.   | Optionally, change the minimum advertisement interval. Valid values range from 3 to 1800 seconds.<br>Use the no form of the command to return to the default value.                                                                                                                                                              | <code>ip irdp minadvertinterval interval</code> |
| 4.   | Optionally, change the valid lifetime of the IP address in the advertisement. Valid values range from 0 to 9000 seconds.<br>Use the no form of the command to return to the default value.                                                                                                                                       | <code>ip irdp holdtime holdtime</code>          |
| 5.   | Optionally, change the preference level for this interface. Valid values range from -2147483648 to 2147483648.<br>Setting preference to the minimum value indicates that the address should not be used by neighboring hosts as a default router address.<br>Use the no form of the command to return to the default value of 0. | <code>ip irdp preference preference</code>      |
| 6.   | Optionally, change the advertisement address to 255.255.255.255.<br>The default of 224.0.0.1 should be used if the router supports IP multicast on the interface.<br>Use the no form of the command to return to the default value.                                                                                              | <code>ip irdp broadcast</code>                  |
| 7.   | Display IRDP information.                                                                                                                                                                                                                                                                                                        | <code>show ip irdp [vlan vlan-id]</code>        |

The following code example enables IRDP on VLAN 10, leaving all default values, and then shows the IRDP configuration on that VLAN. This example assumes that VLAN 10 has already been configured for routing.

```
C5(su)->router#configure
C5(su)->router(Config)#interface vlan 10
C5(su)->router(Config-if(Vlan 10))#ip irdp enable
C5(su)->router(Config-if(Vlan 10))#exit
C5(su)->router(Config)#show ip irdp vlan 10
Interface vlan 10 has router discovery enabled
Advertisements will occur between 450 and 600 seconds
Advertisements are sent with multicasts
Advertisements are valid for 1800 seconds
Default preference will be 0
```



## Configuring OSPFv2

This chapter gives a brief overview of OSPFv2 and then presents several configuration scenarios. OSPFv2 is available only on those fixed switch platforms that support advanced routing and on which an advanced feature license has been enabled.



**Note:** OSPF is an advanced routing feature that must be enabled with a license key. If you have purchased an advanced license key, you must activate your license as described in the chapter entitled “Activating Licensed Features” in order to enable the OSPF command set. If you wish to purchase an advanced routing license, contact Enterasys Networks Sales.

| For information about...                          | Refer to page... |
|---------------------------------------------------|------------------|
| <a href="#">OSPF Overview</a>                     | 22-1             |
| <a href="#">Basic OSPF Topology Configuration</a> | 22-3             |
| <a href="#">Configuring OSPF Areas</a>            | 22-8             |
| <a href="#">Configuring OSPF Interfaces</a>       | 22-15            |
| <a href="#">Default Settings</a>                  | 22-16            |
| <a href="#">Configuration Procedures</a>          | 22-17            |

### OSPF Overview

The Open Shortest Path First (OSPF) routing protocol is considered a TCP/IP internet routing Interior Gateway Protocol (IGP). OSPF distributes routing information between routers belonging to a single Autonomous System (AS). The OSPF protocol gathers link state information from available neighboring routers and constructs a topology map of the network. It then determines the shortest path for each route using a “shortest path first” algorithm.

The advantages associated with a link-state routing protocol are:

- Rapid convergence
- Reduced routing updates traffic over traditional distance-vector protocols
- Hierarchical segmentation
- Route summarization and aggregation, which are needed to handle large and complicated networks

This OSPF implementation supports RFC 2328 *OSPF Version 2*.



**Note:** The fixed switch firmware also provides a command to implement RFC 1583 compatibility. RFC 1583 used a method to calculate metrics for summary routes that is different from the method specified in RFC 2328. In order to avoid the problem of sub-optimal routing in networks where not all routers have been upgraded to RFC 2328 implementations, you can make OSPF compatible with RFC 1583 with the router mode command **1583compatibility**.

The OSPF protocol is designed expressly for the TCP/IP internet environment. It provides for the authentication of routing updates, and utilizes IP multicast when sending and receiving the updates.

OSPF routes IP packets based solely on the destination IP address found in the IP packet header. IP packets are not encapsulated in any further protocol headers as they transit the Autonomous System (AS). OSPF is a dynamic routing protocol in that it quickly detects topological changes in the AS, such as router interface failures, and calculates new loop-free routes after a period of convergence. This period of convergence is short and involves a minimum of routing traffic.

In a link-state routing protocol, each router maintains a database describing the AS's topology. This database is referred to as the link-state database. Each participating router has an identical database. Each individual piece of this database is a particular router's local state made up of such information as the router's usable interfaces and reachable neighbors. The router distributes its local state throughout the AS by flooding.

## OSPF Areas

OSPF allows sets of networks to be grouped together. Such a grouping is called an area. The topology of an area is hidden from the rest of the AS. This information hiding enables a significant reduction in routing traffic. Also, routing within the area is determined only by the area's own topology, lending the area protection against bad routing data.

Areas are labeled with 32-bit identifiers that typically are written in the dotted decimal notation of an IPv4 address, although this notation is not required. Area IDs are NOT IP addresses, however, and may duplicate any IPv4 address without conflict.

OSPF area types include:

- Backbone Area

The backbone area (area 0, or 0.0.0.0) is the core of the OSPF network. All other areas must be connected to it. Inter-area routing is carried out by routers connected to the backbone area and to their own areas.

- Stub Area

A stub area does not receive route advertisements external to the AS, and routing from within the area is based entirely on a default route.

- Not-So-Stubby Area (NSSA)

A not-so-stubby area is an extension of the stub area type that allows the injection of external routes in a limited way. A NSSA can import AS external routes and send them to other areas, but cannot receive AS external routes from other areas.

- Transit Area

A transit area is used to pass network traffic from one adjacent area to another. The transit area does not originate the traffic nor is it the destination of the traffic.

An area is a generalization of an IP subnetted network. OSPF enables the flexible configuration of IP subnets. Each route distributed by OSPF has a destination and mask. Two different subnets of the same IP network number may have different masks providing a different range of addresses for that subnet. This is commonly referred to as Variable Length Subnet Masking (VLSM). A packet is routed to the longest or most specific match. Host routes are considered to be subnets whose masks are "all ones" (0xffffffff).



**Note:** Refer to the Release Notes for your fixed switch platform for the number of areas supported by your device.

## OSPF Router Types

OSPF router type is an attribute of an OSPF process. A Fixed Switch device uses one OSPF router process that can be any number between 1 and 65535. OSPF defines four router types:

- Area border router (ABR)

An ABR is a router that connects one or more areas to the backbone area, and is a member of every area to which it is connected. An ABR keeps a separate copy of the link-state database for each area to which it is connected.

- Autonomous system boundary router (ASBR)

An ASBR is a router that is connected to more than one routing protocol and exchanges routing information with routers running other protocols. An ASBR distributes routes received from external autonomous systems through its own autonomous system.

- Internal router (IR)

An internal router has all its interfaces in a single area.

- Backbone router (BR)

Backbone routers are located in the backbone area and can be ABRs or IRs.

Each router has an identifier that uniquely identifies that router in the AS. The router ID is written in dotted decimal format. If the router ID is not explicitly configured, the highest configured loopback IP address, if one exists, is used, or the highest routing VLAN IP address is used.

## Designated Router

A designated router (really an interface on a physical router device) is elected by all OSPF routers on a particular network segment, based on highest priority. Each network that has at least two attached routers has a designated router.

The purpose of the designated router (DR) is to reduce network traffic by being the source for routing updates. Other routers on the network send their updates to the DR (and the backup designated router or BDR). The DR keeps a complete topology map of the network and sends the updates it receives from the other routers out to the other routers on the network via multicast. This reduces the amount of network traffic because the routers do not have to update each other and can get all their updates from the DR only.

The backup designated router (BDR), as the name indicates, is the backup to the DR and becomes the DR if the current DR fails. The BDR is also elected by the other routers on the network based on OSPF priority.

A designated router is different from an OSPF router type, which is an attribute of an OSPF process. A DR is an interface on a physical router, and the election of a DR is based on the priority assigned to the OSPF process, and if necessary, the highest router ID.

## Authentication

OSPF v2 supports optional authentication between routers. When configured, only trusted routers can participate in the AS's routing. The fixed switch platforms support either simple or MD5 authentication schemes. Separate authentication schemes can be configured for each IP subnet.

## Basic OSPF Topology Configuration

[Figure 22-1](#) on page 22-4 provides an overview of a basic OSPF topology. This topology displays two areas: a backbone area which must exist in any OSPF topology and a directly connected area

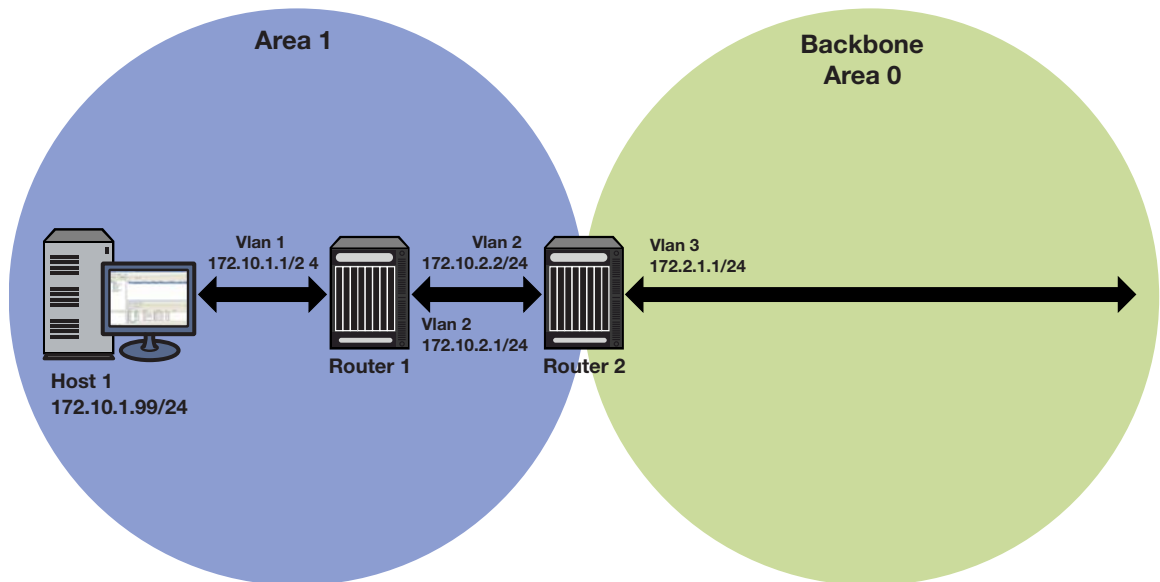
1. See “[Configuring OSPF Areas](#)” on page 22-8 for additional discussion of OSPF area configuration. This basic configuration requires the configuration of four interfaces and associated IP addresses. Also configured are two loopback interfaces, to use for the router IDs.

## Configuring the Router ID

OSPF initially assigns all routers a router ID based on the highest loopback IP address of the interfaces configured for IP routing. If there is no loopback interface configured then it will be the highest VLAN IP address configured. This unique value, which is included in the hello packet transmitted in Link State Advertisements (LSA), identifies one router to another and helps establish adjacencies among OSPF routers. When you specify an interface as the router ID, this value supersedes the default ID.

### Example

**Figure 22-1 Basic OSPF Topology**



The following code example configures the basic OSPF topology as displayed in [Figure 22-1](#) above.

#### Router 1 CLI Input

```
Router 1(su)->router(Config)#interface vlan 1
Router 1(su)->router(Config-if(Vlan 1))#ip address 172.10.1.1 255.255.255.0
Router 1(su)->router(Config-if(Vlan 1))#ip ospf areaid 0.0.0.1
Router 1(su)->router(Config-if(Vlan 1))#ip ospf enable
Router 1(su)->router(Config-if(Vlan 1))#no shutdown
Router 1(su)->router(Config-if(Vlan 1))#exit

Router 1(su)->router(Config)#interface vlan 2
Router 1(su)->router(Config-if(Vlan 2))#ip address 172.10.2.1 255.255.255.0
Router 1(su)->router(Config-if(Vlan 2))#ip ospf areaid 0.0.0.1
Router 1(su)->router(Config-if(Vlan 2))#ip ospf enable
```



```
Router 1(su)->router(Config-if(Vlan 2))#no shutdown
Router 1(su)->router(Config-if(Vlan 2))#exit
```

```
Router 1(su)->router(Config)#interface loopback 0
Router 1(su)->router(Config-if(Lpbk 0))#ip address 10.10.10.10 255.255.255.255
Router 1(su)->router(Config-if(Lpbk 0))#no shutdown
Router 1(su)->router(Config-if(Lpbk 0))#exit
```

```
Router 1(su)->router(Config)#router id 10.10.10.10
Router 1(su)->router(Config)#router ospf 1
Router 1(su)->router(Config-router)#
```

## Router 2 CLI Input

```
Router 2(su)->router(Config)#interface vlan 2
Router 2(su)->router(Config-if(Vlan 2))#ip address 172.10.2.2 255.255.255.0
Router 2(su)->router(Config-if(Vlan 2))#ip ospf areaid 0.0.0.1
Router 2(su)->router(Config-if(Vlan 2))#ip ospf enable
Router 2(su)->router(Config-if(Vlan 2))#no shutdown
Router 2(su)->router(Config-if(Vlan 2))#exit
```

```
Router 2(su)->router(Config)#interface vlan 3
Router 2(su)->router(Config-if(Vlan 3))#ip address 172.2.1.1 255.255.255.0
Router 2(su)->router(Config-if(Vlan 3))#ip ospf areaid 0.0.0.0
Router 2(su)->router(Config-if(Vlan 3))#ip ospf enable
Router 2(su)->router(Config-if(Vlan 3))#no shutdown
Router 2(su)->router(Config-if(Vlan 3))#exit
```

```
Router 2(su)->router(Config)#interface loopback 0
Router 2(su)->router(Config-if(Lpbk 0))#ip address 20.20.20.20 255.255.255.255
Router 2(su)->router(Config-if(Lpbk 0))#no shutdown
Router 2(su)->router(Config-if(Lpbk 0))#exit
```

```
Router 2(su)->router(Config)#router id 20.20.20.20
Router 2(su)->router(Config)#router ospf 1
Router 2(su)->router(Config-router)#
```

## Configuring the Designated Router

In the process of implementing OSPF, a large number of multi-access links to routers across the network may cause too many adjacencies to form. To avoid this problem, a Designated Router (DR) is elected per multi-access network to build adjacencies to all other routers on that network. A Backup Designated Router (BDR) is also elected in case the Designated Router (DR) fails, in which case the BDR will become the DR.



**Note:** A DR is required only for multi-access networks. Point-to-Point links do not need a DR because only a single adjacency is required.

To elect a DR from a host of candidates on the network, each router multicasts a hello packet and examines the priority of hello packets received from other routers. The router with the highest priority is elected the DR, and the router with the next highest priority is elected the BDR. Any router with a priority of 0 will opt out of the DR election process.

If DR candidates all share non-zero priorities, OSPF applies the router ID as a tie-breaker where the highest ID is chosen DR and the next highest ID is chosen BDR.

## Configuring Router Priority

When two routers attached to a network both attempt to become the designated router, the one with the highest router priority takes precedence. A router whose router priority is set to 0 is ineligible to become the designated router on the attached network. Router priority is specified per router interface and is advertised in hello packets sent out by the interface.

Use the **ip ospf priority** command in interface configuration command mode to specify the router priority that will be included in LSAs going out this interface.

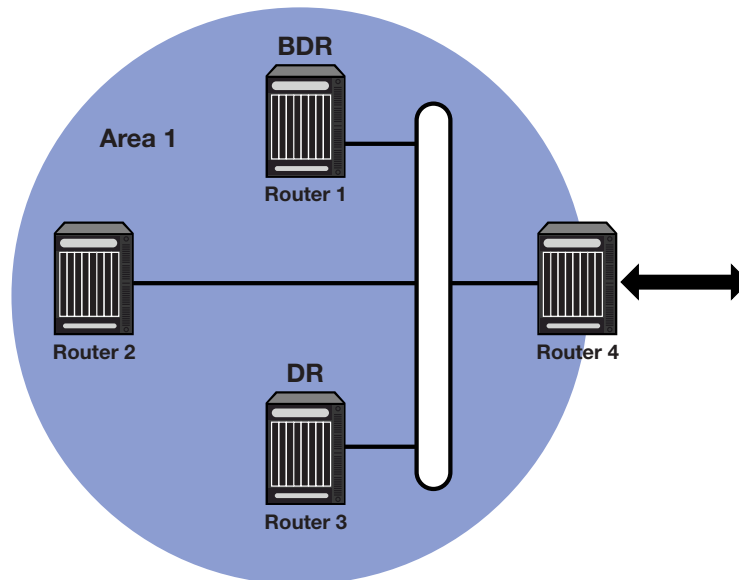
## Example

Figure 22-2 displays a designated router topology example. The code example below Figure 22-2 will configure the four displayed routers with the following priorities:

- Router 1 = 25
- Router 2 = 10
- Router 3 = 30
- Router 4 = 0

Router 4 will not take part in the election process at all. Router 3 has the highest priority and therefore will be elected DR. Router 1 has the second highest priority and will be elected BDR.

**Figure 22-2 OSPF Designated Router Topology**



### Router 1 CLI Input

```
Router 1(su)->router(Config)#interface vlan 1
Router 1(su)->router(Config-if(Vlan 1))#ip ospf priority 25
```

```
Router 1(su)->router(Config-if(Vlan 1))#ip ospf areaid 0.0.0.1
Router 1(su)->router(Config-if(Vlan 1))#ip ospf enable
Router 1(su)->router(Config-if(Vlan 1))#exit
```

### Router 2 CLI Input

```
Router 2(su)->router(Config)#interface vlan 1
Router 2(su)->router(Config-if(Vlan 1))#ip ospf priority 10
Router 2(su)->router(Config-if(Vlan 1))#ip ospf areaid 0.0.0.1
Router 2(su)->router(Config-if(Vlan 1))#ip ospf enable
Router 2(su)->router(Config-if(Vlan 1))#exit
```

### Router 3 CLI Input

```
Router 3(su)->router(Config)#interface vlan 1
Router 3(su)->router(Config-if(Vlan 1))#ip ospf priority 30
Router 3(su)->router(Config-if(Vlan 1))#ip ospf areaid 0.0.0.1
Router 3(su)->router(Config-if(Vlan 1))#ip ospf enable
Router 3(su)->router(Config-if(Vlan 1))#exit
```

### Router 4 CLI Input

```
Router 4(su)->router(Config)#interface vlan 1
Router 4(su)->router(Config-if(Vlan 1))#ip ospf priority 0
Router 4(su)->router(Config-if(Vlan 1))#ip ospf areaid 0.0.0.1
Router 4(su)->router(Config-if(Vlan 1))#ip ospf enable
Router 4(su)->router(Config-if(Vlan 1))#exit
```

## Configuring the Administrative Distance for OSPF Routes

If several routes coming from different protocols are presented to the fixed switch device, the protocol with the lowest administrative distance will be chosen for route installation. By default, OSPF administrative distance is set to 110. The **distance ospf** command in router configuration mode can be used to change this value, resetting OSPF's route preference in relation to other routes as shown in the table below.

| Route Source | Default Distance                                                             |
|--------------|------------------------------------------------------------------------------|
| Connected    | 0                                                                            |
| Static       | 1                                                                            |
| OSPF         | Intra-area - 8; Inter-area - 10; External type 1 - 13; External type 2 - 150 |
| RIP          | 15                                                                           |

## Configuring SPF Timers

In router configuration mode, use the **timers spf** command to fine-tune the operation of OSPF in the network. You can change two timers with this command:

- The SPF delay, which is the delay in seconds between the receipt of an update and execution of the shortest path first (SPF) calculation. The default delay is 5 seconds.
- The SPF hold time, which is the minimum amount of time, in seconds, between two consecutive SPF calculations. The default value is 10 seconds, and valid values can range from

0 to 4294967295. A value of 0 means that two consecutive SPF calculations are performed one immediately after the other. +

## Configuring OSPF Areas

OSPF allows collections of contiguous networks and hosts to be grouped together. Such a group, together with the routers having interfaces to any one of the included networks, is called an area. Each area has its own link-state database.

The topology of an area is invisible from the outside of the area, and routers internal to a given area know nothing of the detailed topology external to the area. This isolation of area detail enables the protocol to reduce routing traffic, as compared to treating the entire Autonomous System as a single link-state domain.

A router has a separate link-state database for each area it is connected to. Routers connected to multiple areas are called Area Border Routers (ABR). Two routers belonging to the same area have, for that area, identical area link-state databases.

An autonomous system can have one or more areas. An AS with multiple areas must define one of the areas as the backbone with an area ID of 0. All non-backbone areas in a multiple area AS must either be contiguous to the backbone or connected using a virtual-link. The backbone is responsible for distributing routing information between non-backbone areas. The backbone must be contiguous, although it need not be physically contiguous. Backbone connectivity can be established and maintained with virtual links.

Virtual links can be configured between any two backbone routers that have an interface to a common non-backbone area. Such virtual links belong to the backbone. The protocol treats two routers joined by a virtual link as if they were connected by an unnumbered point-to-point backbone network.

See RFC 2328 *OSPF Version 2* for further details on inter-area connectivity.

An Area ID can be any value from 0 - 4294967295, but is converted into the 32-bit dotted-quad format (area 50 would be displayed as 0.0.0.50; area 3546 would be displayed as 0.0.13.218).

## Configuring Area Range

An area range is a form of address summarization that defines a range of addresses to be used by the backbone ABRs when they communicate routes to other areas. Area range is a critical tool that pares the route tables and update traffic, as well as reduces network recalculation by the Dijkstra algorithm. Area range configuration summarizes by aggregating an areas' internal networks to advertise a single network. Backbone routers see only one update, representing an entire range of subnets. Area ranges can be configured for purposes of network advertisement as well as summarization of subnets that should not be advertised.

Use the **area range** command in router configuration command mode to configure an area network summarization.

### Example

The following code example configures summarization for the topology shown in [Figure 22-3](#) on page 22-9.

#### Area 1

```
ABR1(su)->router(Config)#router ospf 1
ABR1(su)->router(Config-router)#area 0.0.0.1 range 10.2.0.0 255.255.0.0
```

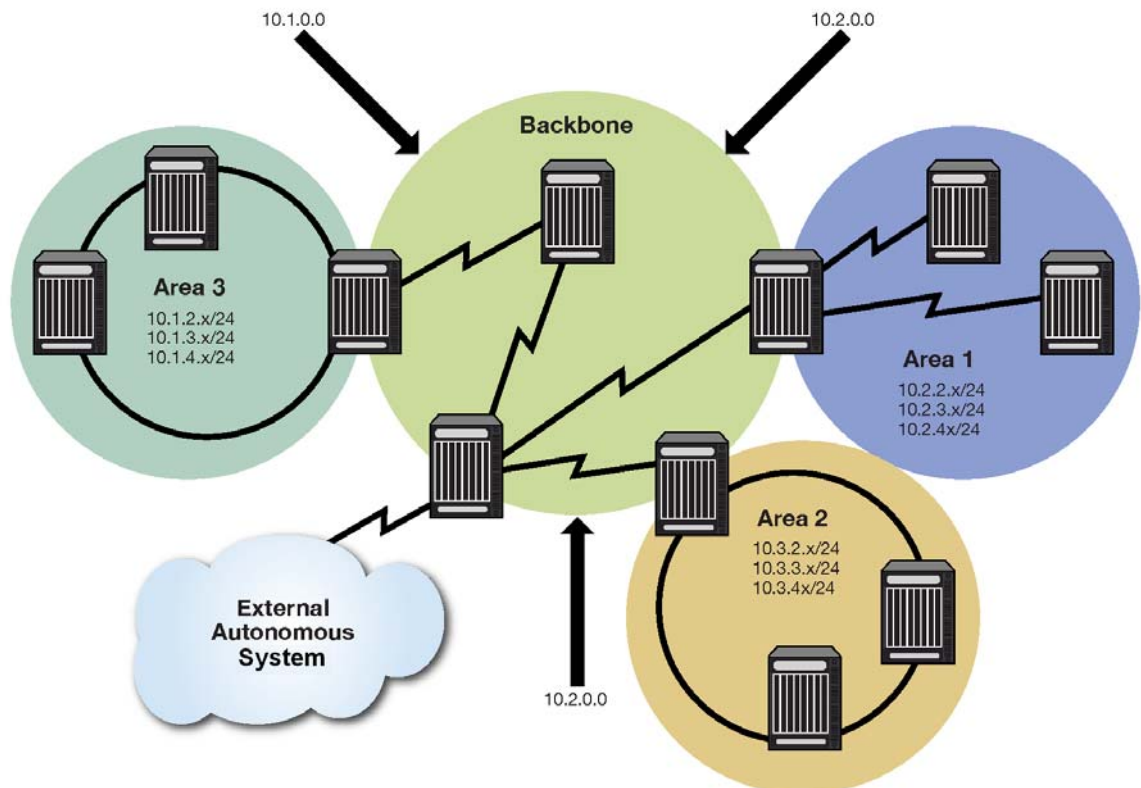
## Area 2

```
ABR2(su)->router(Config)#router ospf 1
ABR2(su)->router(Config-router)#area 0.0.0.2 range 10.3.0.0 255.255.0.0
ABR2(su)->router(Config-router)#area 0.0.0.2 range 10.3.2.0 255.255.255.0 no-advertise
```

## Area 3

```
ABR3(su)->router(Config)#router ospf 1
ABR3(su)->router(Config-router)#area 0.0.0.3 range 10.1.0.0 255.255.0.0
```

**Figure 22-3 OSPF Summarization Topology**



## Configuring a Stub Area

A stub area is a non-transit area. In other words, an area that does not originate or propagate external routes. AS-external-LSAs are not flooded into the stub area; routing to AS external networks is based on a single per-area default route. This reduces the link-state-database size and memory requirements for routers within stub areas.

Handy for reducing routing table size, a stub area is a “dead-end” in which there is no other way to enter or exit except through an Area Border Router (ABR). No ASE (Autonomous System External) or NSSA routes are permitted in a stub area. Each router in a stub area must specify that they are members of the stub area. When specifying that the ABR is a member of the stub area, the ABR will inject a default route into the area.

Routing to external designations from stub areas is based on a default route injected by a stub area’s ABR. A default route is automatically created by the stub area’s ABR. This default route is

injected into the stub area to enable other stub routers within the stub area to reach any external routes that are no longer inserted into the stub area.

A stub area can be configured such that the ABR is prevented from sending type 3 summary LSAs into the stub area using the **no-summary** option. In this case, all destinations outside of the stub area are represented by means of a default route.

There are a couple of restrictions on the use of stub areas. Virtual-links cannot be configured through stub areas, and AS boundary routers cannot be placed internal to stub areas.

Use the **area stub** command in router configuration command mode to configure an area as a stub.

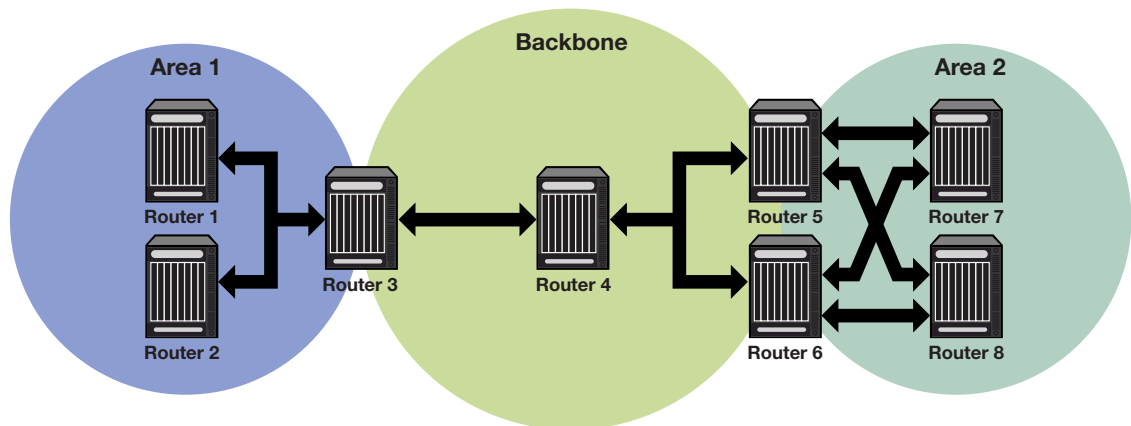
## Stub Area Default Route Cost

A cost value can be set for the default route that is sent into a stub area by an ABR. Configuration of the stub area default route cost is restricted to the ABR attached to this stub area.

Use the **area default cost** command in router configuration command mode on the ABR attached to this stub area to configure the stub area default route cost.

## Example

Figure 22-4 OSPF Stub Area Topology



Using the topology shown in [Figure 22-4](#), the following code example configures every router in Areas 1 and 2 for a stub area (Routers 1, 2, and 3 for Area 1 and Routers 5, 6, 7, and 8 for Area 2). Additionally, ABR routers 3, 5, and 6 are also configured with a default-cost to be assigned to the stub area. Router 5 has a lower metric cost when compared to Router 6, so Router 5 will be the preferred router for packets to access the area, with Router 6 employed as a backup in case Router 5 fails. Router 3 is configured to prevent it from sending LSAs into the stub area.

### Router 1

```
Router 1(su)->router(Config)#router ospf 1
Router 1(su)->router(Config-router)#area 0.0.0.1 stub
```

### Router 2

```
Router 2(su)->router(Config)#router ospf 1
Router 2(su)->router(Config-router)#area 0.0.0.1 stub
```

### Router 3

```
Router 3(su)->router(Config)#router ospf 1
```

```
Router 3(su)->router(Config-router)#area 0.0.0.1 stub no-summary
Router 3(su)->router(Config-router)#area 0.0.0.1 default-cost 15
```

### Router 5

```
Router 5(su)->router(Config)#router ospf 1
Router 5(su)->router(Config-router)#area 0.0.0.2 stub
Router 5(su)->router(Config-router)#area 0.0.0.2 default-cost 15
```

### Router 6

```
Router 6(su)->router(Config)#router ospf 1
Router 6(su)->router(Config-router)#area 0.0.0.2 stub
Router 6(su)->router(Config-router)#area 0.0.0.2 default-cost 20
```

### Router 7

```
Router 7(su)->router(Config)#router ospf 1
Router 7(su)->router(Config-router)#area 0.0.0.2 stub
```

### Router 8

```
Router 8(su)->router(Config)#router ospf 1
Router 8(su)->router(Config-router)#area 0.0.0.2 stub
```

## Configuring a Not So Stubby Area (NSSA)

A Not So Stubby Area (NSSA) is a hybrid area using an Autonomous System Border Router (ASBR) to connect two disparate organizations. External routes are advertised as Type 7 LSAs and are converted to Type 5 LSAs before flooding to the backbone by the NSSA's ABR. Also, summary routes are allowed into the NSSA while external routes from other networks are still filtered from insertion into the NSSA.

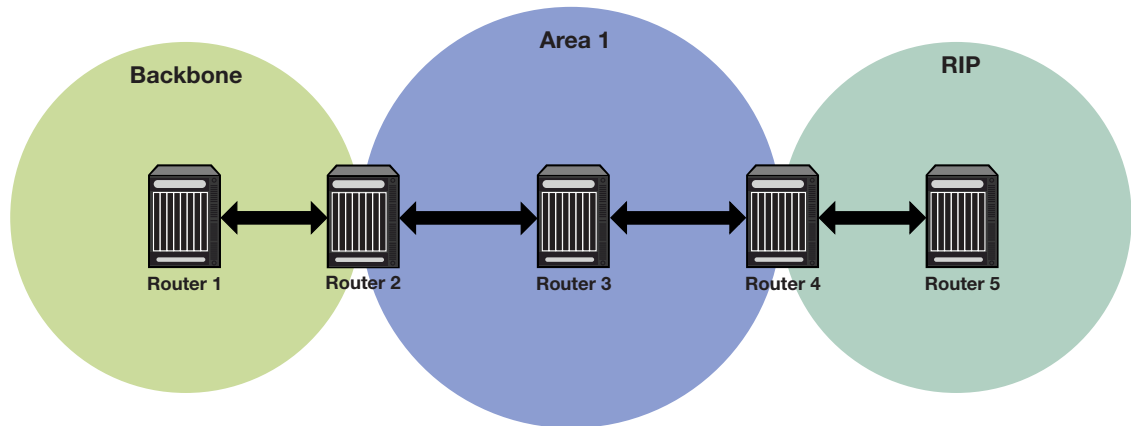
External routes that are not imported into an NSSA can be represented by a default route. If the router is an ABR and has the highest router ID of all ABRs in the area, it will translate Type 7 LSAs into Type 5 LSAs.

When a translating ABR loses a translator election, it will stop translating, and after a number of seconds, it will flush any Type 5 LSAs resulting from aggregation. Any Type 5 LSAs resulting from direct translation of Type 7 LSAs will be allowed to age out. An ABR will always originate a default route into any attached NSSAs.

Use the **area nssa** command to configure an area as a Not-So-Stubby-Area.

## Example

Figure 22-5 OSPF NSSA Topology



Using the topology shown in [Figure 22-5](#), the following code examples will configure Router 2 as the ABR between Area 1 and the backbone area 0. Router 4 is configured as an ASBR connected to a RIP autonomous system. Router 2 will translate Type 7 LSAs from the connected domain to Type 5 routes into the backbone.

Router 4 will be configured to redistribute connected and RIP routes.

### Router 2 (ABR)

```
Router 2(su)->router(Config)#router id 2.2.2.2
Router 2(su)->router(Config)#router ospf 1
Router 2(su)->router(Config-router)#area 0.0.0.1 nssa default-information-originate
```

### Router 3 (IR)

```
Router 3(su)->router(Config)#router id 3.3.3.3
Router 3(su)->router(Config)#router ospf 1
Router 3(su)->router(Config-router)#area 0.0.0.1 nssa
```

### Router 4(ASBR)

```
Router 4(su)->router(Config)#router id 4.4.4.4
Router 4(su)->router(Config)#router ospf 1
Router 4(su)->router(Config-router)#redistribute connected
Router 4(su)->router(Config-router)#redistribute rip
```

## Configuring Area Virtual-Links

The backbone area 0 cannot be disconnected from any other areas in the AS. Disconnected areas will become unreachable. To establish and maintain backbone connectivity, virtual-links can be configured through non-backbone areas for the purpose of connecting a disconnected area with the backbone through a backbone connected area. The two endpoints of a virtual link are ABRs, both of which belong to the backbone connected area (also referred to as the transit area); one of which belongs to the area disconnected from the backbone. Virtual links cannot be configured through stub areas.



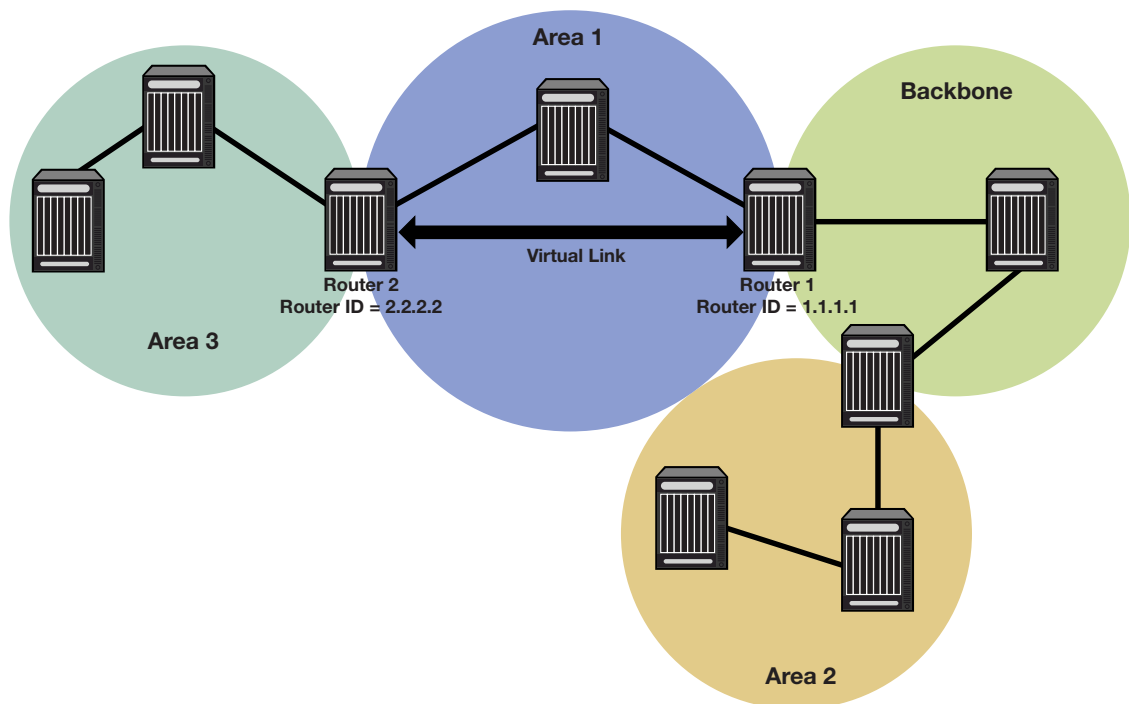
The virtual-link is treated as if it were an unnumbered point-to-point network belonging to the backbone and joining the two ABRs. The cost of a virtual link is not configured. It is auto configured with the cost of the intra-area path between the two ABRs that make up the virtual-link.

Use the **area virtual-link** command in OSPF router configuration command mode, providing the transit area ID and the ABRs router ID, to configure an area virtual-link.

Figure 22-6 on page 22-13 displays a typical virtual-link topology. Area 3 does not share an ABR with the backbone area, and is therefore disconnected from the backbone. Area 3 shares an ABR (router 2) with area 1. Area 1 has a second ABR (router 1) that it shares with the backbone. Area 1 is the transit area because it contains an ABR that it shares with the disconnected area and a second ABR that it shares with the backbone. By configuring an area virtual-link between router 2 and router 1, Area 3 will gain connectivity with the backbone and be able to learn routes for this AS.

## Example

Figure 22-6 Virtual Link Topology



The following code example presents the configuration required to configure the virtual-link displayed in Figure 22-6:

### Router 1

```
Router 1(su)->router(Config)#router id 1.1.1.1
Router 1(su)->router(Config)#router ospf 1
Router 2(su)->router(Config-router)#area 0.0.0.1 virtual-link 2.2.2.2
```

### Router 2

```
Router 2(su)->router(Config)#router id 2.2.2.2
Router 2(su)->router(Config)#router ospf 1
Router 2(su)->router(Config-router)#area 0.0.0.1 virtual-link 1.1.1.1
```

## Configuring Area Virtual-Link Authentication

An area virtual-link can be configured for simple authentication. Neighbor virtual link routers must have the same password.

Use the **area virtual-link authentication-key** command in OSPF router configuration command mode to configure simple authentication on this area virtual-link. The key is an alphanumeric string of up to 8 characters.

## Configuring Area Virtual-Link Timers

The following timers can be configured for an area virtual-link:

- Dead-interval using the **area virtual-link dead-interval** command.  
The dead interval specifies the number of seconds that a router must wait to receive a hello packet before declaring the neighbor as “dead” and removing it from the OSPF neighbor list. This value must be the same for all virtual links attached to a certain subnet. The value can range from **1** to **8192**.
- Hello-interval using the **area virtual-link hello-interval** command.  
The hello interval specifies the number of seconds between hello packets on the virtual link. This value must be the same for all virtual links attached to a network. The value can range from 1 to 8192.
- Retransmit-interval using the **area virtual-link retransmit-interval** command.  
The retransmit interval specifies the number of seconds between successive retransmissions of the same LSAs. Valid values are greater than the expected amount of time required for the update packet to reach and return from the interface, and range from **1** to **8192**. Default is 5 seconds.
- Transmit-delay using the **area virtual-link transmit-delay** command.  
The transmit delay specifies the estimated number of seconds before a link state update packet on the interface should be transmitted. Valid values range from **1** to **8192**. Default is 1 second.

See “[Configuring OSPF Interface Timers](#)” on page 22-16 for an OSPF timers discussion.



**Note:** RFC 2328 specifies that the retransmit-interval should be greater than the expected round-trip delay between the two routers. Since this may be hard to estimate for a virtual link, it is better to err on the side of making it too large.

## Configuring Route Redistribution

Redistribution permits the importation of other routing protocols into OSPF such as RIP, as well as static and directly connected routes. See “[Configuring a Not So Stubby Area \(NSSA\)](#)” on page 22-11 for an example of redistribution of connected and RIP routes by an ASBR in an NSSA context.

Use the **redistribute** command in OSPF router configuration command mode to permit the redistributions of OSPF, RIP, static, or connected routes by this router.

## Configuring Passive Interfaces

Passive interfaces explicitly allows the network to be advertised, but prevents it from forming neighbor relationships on that interface. Passive interfaces are included in the OSPF route table.

They do not send or receive hello packets. OSPF adjacencies can not be formed on a passive interface.

Use the **passive-interface** command in router configuration command mode to configure an interface as passive or to set passive as the default mode of operation for all interfaces.

## Configuring OSPF Interfaces

OSPF is disabled by default and must be enabled on routing interfaces with the **ip ospf enable** command in interface configuration mode. When OSPF is enabled on an interface, the OSPF area defaults to 0.0.0.0. Use the **ip ospf areaid** command to configure a different area ID for the interface.

### Configuring Interface Cost

Each interface has an outbound cost associated with it. The lower the cost, the more likely the interface will be used to forward data traffic. Should several equal-cost routes to a destination exist, traffic is distributed equally among them.

The default interface cost is 10. Use the **ip ospf cost** command in interface configuration command mode to specify a non-default outbound cost on an interface.

### Configuring Interface Priority

Each interface has a priority value that is communicated between routers by means of hello messages and is used in the election of the Designated Router. See “[Designated Router](#)” on page 22-3 for more information.

The default value of 1 is assigned to an interface when it is enabled for OSPF. Use the **ip ospf priority** command in interface configuration mode to set a non-default priority on an interface.

### Configuring Authentication

Authentication helps ensure that routing information is processed only from trusted routers. On the fixed switches, OSPF authentication is configured at the interface level.

Two authentication schemes are available:

- Simple, using the **ip ospf authentication-key** command
- MD5, using the **ip ospf message digest key md5** command

A single scheme must be configured for each network. The use of different schemes enables some interfaces to use much stricter authentication than others. When you wish to bar routers from exchanging OSPF packets, use simple authentication. The interfaces that the packets will be sent on still must be trusted because the authentication key will be placed in the packets and is visible to anyone on the network. All neighboring routers on the same network must have the same password configured to be able to form adjacencies and exchange OSPF information.

If you do not trust other routers on your network, use MD5 authentication. The system works by using shared secret keys. Because keys are used to sign the packets with an MD5 checksum through a one-way hash function, they cannot be forged or tampered with. Also, because the keys are not included in the packet, snooping the key is impossible. Network users can still snoop the contents of packets, though, because packets are not encrypted.

## Configuring OSPF Interface Timers

The following OSPF timers are configured at the interface level in interface configuration mode:

- Hello Interval
- Dead Interval
- Retransmit Interval
- Transmit Delay

Use the hello interval (**ip ospf hello-interval**) and dead interval (**ip ospf dead-interval**) timers to ensure efficient adjacency between OSPF neighbors. The hello interval is the period between transmissions of hello packet advertisements. The dead interval is the period that can elapse without receiving a router's hello packets before its neighbors will declare it down.

In order to ensure that flooding is reliable, LSAs are retransmitted until they are acknowledged. The period between retransmissions is the retransmit interval (**ip ospf retransmit-interval**). If this interval is set too low for an interface, needless retransmissions will take place. If the value is set too high, the speed of the flooding, during the period of lost packets, may be affected.

The transmit delay is an estimation of the number of seconds it takes to transmit a link state update packet over this interface. This value should take into account transmission and propagation delays. Configure this timer with the **ip ospf transmit-delay** command.

These OSPF timers can also be configured for an area virtual-link. See "[Configuring Area Virtual-Links](#)" on page 22-12. Also refer to "[Configuring SPF Timers](#)" on page 22-7 for a description of the router level timers that you can configure.

## Default Settings

[Table 22-1](#) lists OSPF parameters and their default values.

**Table 22-1 Default OSPF Parameters**

| Parameter          | Description                                                                                                                               | Default Value                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| OSPF process       | Status of the protocol, whether enabled or disabled.                                                                                      | Disabled globally and per interface                 |
| router ID          | Provides for the identification of one router to another and helps establish adjacencies among OSPF routers.                              | highest IP address of configured routing interfaces |
| interface cost     | An outbound interface value used in determining which routing interface should forward when more than one routing interface is available. | 10                                                  |
| interface priority | A value placed on the interface that helps in determining which router will be elected designated router.                                 | 1                                                   |
| SPF delay timer    | Specifies the amount of time between receiving an OSPF update and the start of an SPF calculation.                                        | 5 seconds                                           |
| SFP hold time      | Specifies the minimum amount of time, in seconds, between two consecutive OSPF calculations.                                              | 10 seconds                                          |

**Table 22-1 Default OSPF Parameters (continued)**

| Parameter           | Description                                                                                                                                     | Default Value                                                                                                                                     |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| retransmit interval | A timer that determines the retransmission of LSAs in order to ensure reliable flooding.                                                        | 5 seconds                                                                                                                                         |
| transmit delay      | Specifies the number of seconds it takes to transmit a link state update packet over this interface.                                            | 1 second                                                                                                                                          |
| hello interval      | The period between transmissions of hello packet advertisements.                                                                                | 10 seconds                                                                                                                                        |
| dead interval       | The period that can elapse without receiving a router's hello packets before its neighbors will declare it down.                                | 40 seconds                                                                                                                                        |
| distance            | Specifies the administrative distance for OSPF routes. The available protocol with the lowest administrative distance is chosen for this route. | connected = 0<br>static = 1<br>OSPF Intra-area = 8<br>OSPF Inter-area = 10<br>OSPF External Type 1 = 13<br>OSPF External Type 2 = 150<br>RIP = 15 |

## Configuration Procedures

### Basic OSPF Router Configuration

[Procedure 22-1](#) describes the basic OSPF router tasks.

#### Procedure 22-1 Basic OSPF Router Configuration

| Step | Task                                                                                                                                                                    | Command(s)                                                                                                    |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| 1.   | In global configuration mode, configure the router ID.                                                                                                                  | <code>router id ip-address</code>                                                                             |
| 2.   | Specify the OSPF process id and enable router configuration mode. Only one OSPF process, numbered between 1 and 65535, can be configured on the Fixed Switch platforms. | <code>router ospf process-id</code>                                                                           |
| 3.   | Optionally, change SPF timers                                                                                                                                           | <code>timers spf spf-delay spf-hold</code>                                                                    |
| 4.   | Optionally, change the administrative distance for OSPF routes.                                                                                                         | <code>distance ospf {external   inter-area   intra-area} weight</code>                                        |
| 5.   | Optionally, enable passive OSPF on an interface or set passive OSPF as the default mode on all interfaces.                                                              | <code>passive-interface {default   vlan vlan-id}</code>                                                       |
| 6.   | Optionally, allow routing information discovered through non-OSPF protocols to be distributed in OSPF messages.                                                         | <code>redistribute {connected   rip   static} [metric metric value] [metric-type type-value] [subnets]</code> |
| 7.   | If necessary, enable RFC 1583 compatibility                                                                                                                             | <code>1583compatibility</code>                                                                                |

## OSPF Interface Configuration

[Procedure 22-2](#) on page 22-18 describes the OSPF interface configuration tasks. All OSPF interface configuration commands are executed in router interface configuration mode.

### Procedure 22-2 OSPF Interface Configuration

| Step | Task                                                                                                                                                         | Command(s)                                                                                                                                                                                   |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | In interface configuration mode, configure an IP address for all routing interfaces in the AS. See <a href="#">Procedure 20-2</a> on page 20-4.              | <code>ip address ip-address ip-mask [secondary]</code>                                                                                                                                       |
| 2.   | Enable OSPF in the interface.                                                                                                                                | <code>ip ospf enable</code>                                                                                                                                                                  |
| 3.   | Configure the area in which the interface is located. By default, the interface's area id is set to the backbone, 0.0.0.0.                                   | <code>ip ospf areaid area-id</code>                                                                                                                                                          |
| 4.   | Set the interface's priority, which is used to determine the designated router on the network segment. By default, the priority is set to 1.                 | <code>ip ospf priority number</code>                                                                                                                                                         |
| 5.   | Optionally, set the cost of sending an OSPF packet on the interface. By default, the cost is set to 10.                                                      | <code>ip ospf cost cost</code>                                                                                                                                                               |
| 6.   | Optionally, adjust the OSPF timers on the interface.                                                                                                         | <code>ip ospf retransmit-interval seconds</code><br><code>ip ospf transmit-delay seconds</code><br><code>ip ospf hello-interval seconds</code><br><code>ip ospf dead-interval seconds</code> |
| 7.   | Optionally, configure OSPF authentication on the interface.<br><br>Refer to <a href="#">"Configuring Authentication"</a> on page 22-15 for more information. | <code>ip ospf authentication-key password</code><br>or<br><code>ip ospf message-digest-key keyid md5 key</code>                                                                              |

## OSPF Area Configuration

[Procedure 22-3](#) describes the OSPF area configuration tasks. All OSPF area configuration commands are executed in router configuration mode.

### Procedure 22-3 OSPF Area Configuration

| Step | Task                                                                                                                                                                                                            | Command(s)                                                                    |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| 1.   | Configure route summarization to be used by Area Border Routers (ABRs) when they communicate routes to other areas.<br><br>Refer to <a href="#">"Configuring Area Range"</a> on page 22-8 for more information. | <code>area area-id range ip-address ip-mask [advertise   no-advertise]</code> |
| 2.   | Configure an OSPF area as a stub area.<br><br>Refer to <a href="#">"Configuring a Stub Area"</a> on page 22-9 for more information.                                                                             | <code>area area-id stub [no-summary]</code>                                   |
| 3.   | Configure an OSPF area as a not-so-stubby area (NSSA).<br><br>Refer to <a href="#">"Configuring a Not So Stubby Area (NSSA)"</a> on page 22-11 for more information.                                            | <code>area area-id nssa [default-information-originate]</code>                |

**Procedure 22-3 OSPF Area Configuration (continued)**

| Step | Task                                                                                                                                          | Command(s)                                                                                                                                                                                                                                                                                                                                                                              |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.   | On ABRs connected to stub areas and NSSAs, configure the cost value for the default route sent into stub areas and NSSAs.                     | <code>area area-id default-cost cost</code>                                                                                                                                                                                                                                                                                                                                             |
| 5.   | If necessary, configure an OSPF virtual link. Refer to “ <a href="#">Configuring Area Virtual-Links</a> ” on page 22-12 for more information. | <code>area area-id virtual-link router-id</code>                                                                                                                                                                                                                                                                                                                                        |
| 6.   | Optionally, configure authentication and/or timer values for the virtual link.                                                                | <code>area area-id virtual-link router-id authentication-key key</code><br><code>area area-id virtual-link router-id dead-interval seconds</code><br><code>area area-id virtual-link router-id hello-interval seconds</code><br><code>area area-id virtual-link router-id retransmit-interval seconds</code><br><code>area area-id virtual-link router-id transmit-delay seconds</code> |

## Managing and Displaying OSPF Configuration and Statistics

Refer to the *CLI Reference* for your platform for explanations of the output of the commands listed in [Table 22-2](#). Show commands can be executed in any router mode.

**Table 22-2 OSPF Management Tasks.**

| Task                                                                                                                   | Command(s)                                                              |
|------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Reset the OSPF process, which will require adjacencies to be reestablished and routes to be reconverged.               | <code>clear ip ospf process process-id</code>                           |
| Display OSPF information.                                                                                              | <code>show ip ospf</code>                                               |
| Display the OSPF link state database.                                                                                  | <code>show ip ospf database</code>                                      |
| Display OSPF interface related information, including network type, priority, cost, hello interval, and dead interval. | <code>show ip ospf interface [vlan vlan-id]</code>                      |
| Display the state of communication between an OSPF router and its neighbor routers.                                    | <code>show ip ospf neighbor [detail] [ip-address] [vlan vlan-id]</code> |
| Display information about the virtual links configured on a router.                                                    | <code>show ip ospf virtual-links</code>                                 |
| Display information about an area.                                                                                     | <code>show ip ospf area area-id</code>                                  |





## Configuring VRRP

This chapter describes the Virtual Router Redundancy Protocol (VRRP) feature and its configuration. VRRP is available only on those fixed switch platforms that support advanced routing and on which an advanced feature license has been enabled.



**Note:** VRRP is an advanced routing feature that must be enabled with a license key. If you have purchased an advanced license key, you must activate your license as described in the chapter entitled “Activating Licensed Features” in order to enable the VRRP command set. If you wish to purchase an advanced routing license, contact Enterasys Networks Sales.

| For information about...              | Refer to page... |
|---------------------------------------|------------------|
| <a href="#">VRRP Overview</a>         | 23-1             |
| <a href="#">Configuring VRRP</a>      | 23-3             |
| <a href="#">Terms and Definitions</a> | 23-8             |

### VRRP Overview

Virtual Router Redundancy Protocol (VRRP) is an election protocol capable of dynamically assigning responsibility for a virtual router to one of the VRRP routers on a LAN. A virtual router is an abstract object managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a Virtual Router Identifier (VRID) and a set of associated IP addresses across a common LAN that define virtual router members. A VRRP router is a router with the VRRP protocol running on it. A VRRP router may participate in and back up one or more virtual routers.

VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a single subnet. The elected VRRP router is called the master. The router master controls the IP addresses associated with a virtual router. The master forwards packets sent to these IP addresses. The VRRP election process provides dynamic fail over of forwarding responsibility to another VRRP router should the current master become unavailable. This allows any of the virtual router IP addresses on the LAN to be used as the default first hop router by end-hosts. In this way, VRRP provides a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

Statically configured default routes can represent a single point of failure that can result in a catastrophic event, isolating all end-hosts that are unable to detect any alternate available path. VRRP is designed to eliminate the single point of failure inherent in the static default routed environment.

VRRP is defined in RFC 5798. [Figure 23-1](#) on page 23-2 illustrates a basic VRRP topology.

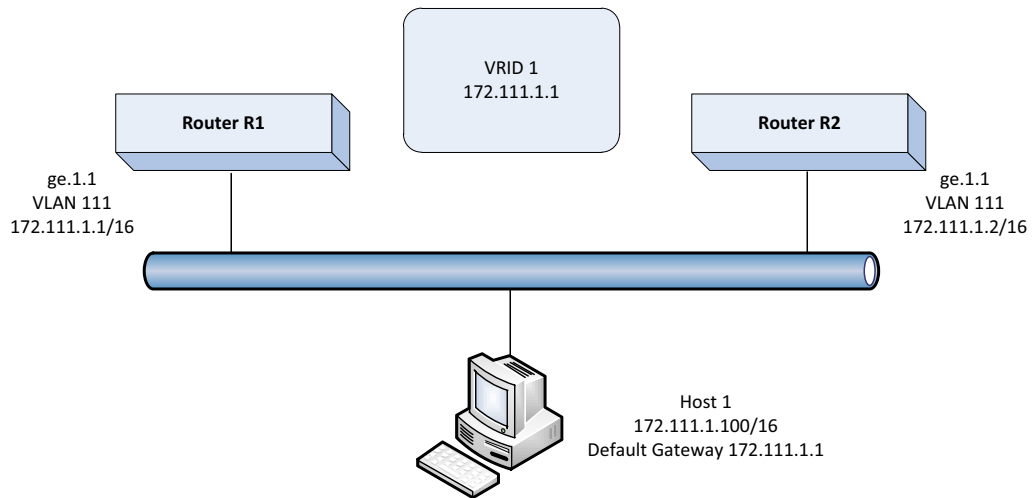
**Figure 23-1 Basic VRRP Topology**

Figure 23-1 shows a basic VRRP topology with a single virtual router. Routers R1 and R2 are both configured with one virtual router (VRID 1). Router R1 serves as the master and Router R2 serves as the backup. The hosts are configured to use 172.111.1.1/16 as the default route.

If Router R1 should become unavailable, Router R2 would take over virtual router VRID 1 and its associated IP addresses. Packets sent to 172.111.1.1/16 would go to Router R2. When Router R1 comes up again, it would take over as master, and Router R2 would revert to backup.

## VRRP Virtual Router Creation

Each virtual router has its own instance. Create a VRRP virtual router instance using the **create** command in router configuration command mode specifying the VRID for this instance. The virtual router instance must be created before any other VRRP settings can be configured.

Refer to the Release Notes for your fixed switch product to determine the maximum number of VRRP instances that can be created.

## VRRP Master Election

After the virtual router instance has been created, assign the IP addresses associated with this virtual router using the **address** command. You must specify the VLAN on which to configure the virtual router address, the virtual router ID (VRID), the virtual router IP address, and whether the router owns the IP address as one of its interface. A virtual router IP address can be either an address configured on the routing interface or an address that falls within the range of any networks configured on this routing interface.

If the virtual router IP address is the same as the routing interface (VLAN) address owned by a VRRP router, then the router owning the address becomes the master. The master sends an advertisement to all other VRRP routers declaring its status and assumes responsibility for forwarding packets associated with its VRID.

If the virtual router IP address is not owned by any of the VRRP routers, then the routers compare their priorities and the higher priority owner becomes the master. VRRP router priority is set using the **priority** command in router configuration command mode. If priority values are the same, then the VRRP router with the highest IP address is selected master.

VRRP advertisements are sent by the master router to other routers participating in the VRRP master selection process, informing them of its configured values. Once the master is selected,

then advertisements are sent every advertising interval to let other VRRP routers in this VRID know the router is still acting as master of the VRID. All routers with the same VRID should be configured with the same advertisement interval. Use the **advertise-interval** command to change the advertise-interval for this VRID.

## Enabling Master Preemption

By default, a router is enabled to preempt a lower priority master for the configured virtual router. If the router owns the virtual router IP address, it can not be preempted and always preempts other routers regardless of the priority setting or this preemption setting. Use the **preempt** command to enable or disable master preemption on this VRRP router.

## Enabling ICMP Replies

You can enable the virtual router master to respond to an ICMP echo even if it does not “own” the virtual IP address with the **master-icmp-reply** command. Without this function, the virtual router can only respond to an ICMP echo when the virtual IP address matches the real IP address of the interface. Therefore, when the backup router takes over, there would be no device that would answer the ICMP echo for that virtual IP (because only the primary was configured with the matching real IP). With **master-icmp-reply** enabled, management stations that use “ping” to poll devices will be able to “see” that the virtual router is available when the backup router assumes the role of master.

## Configuring VRRP Authentication

A version 2 VRRP VRID can be configured for a simple clear text authentication password. Use the **ip vrrp authentication-key** command in interface configuration command mode, specifying the password.

## Enabling the VRRP Virtual Router

All other VRRP options must be set before enabling a VRRP virtual router on the routing interface. Once enabled, you can not make any configuration changes to VRRP without first disabling VRRP, using the **no enable** command.

Use the **enable** command in router configuration command mode, specifying the VLAN on which to enable VRRP and the VRID of the virtual router to be enabled.

## Configuring VRRP

This section provides details for the configuration of VRRP on the fixed switch products.

[Table 23-1](#) lists VRRP parameters and their default values.

**Table 23-1 Default VRRP Parameters**

| Parameter         | Description                                                                                                                          | Default Value |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------|---------------|
| master-icmp-reply | Enables the master of this virtual router to respond to an ICMP echo, even if the device is not the owner of the virtual IP address. | disabled      |

**Table 23-1 Default VRRP Parameters (continued)**

| Parameter          | Description                                                                                                                | Default Value |
|--------------------|----------------------------------------------------------------------------------------------------------------------------|---------------|
| advertise-interval | Specifies the interval between the advertisement the master sends to other routers participating in the selection process. | 1 second      |
| priority           | Specifies the router priority for the master election for this virtual router.                                             | 100           |
| VRRP preemption    | Specifies whether higher priority backup VRRP routers can preempt a lower priority master VRRP router and become master.   | enabled       |

[Procedure 23-1](#) describes how to configure VRRP. The procedure assumes that the VLAN routing interface has been created and configured for routing.

### Procedure 23-1 Configuring VRRP

| Step | Task                                                                                                   | Command(s)                                                                          |
|------|--------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| 1.   | In global configuration mode, enable VRRP configuration mode.                                          | <code>router vrrp</code>                                                            |
| 2.   | In VRRP configuration mode, create a virtual router instance associated with a routing VLAN interface. | <code>create vlan <i>vlan-id</i> <i>vrid</i></code>                                 |
| 3.   | Configure the virtual router IP address.                                                               | <code>address vlan <i>vlan-id</i> <i>vrid</i> <i>ip-address</i> <i>owner</i></code> |
| 4.   | Optionally, change the VRRP router priority for this virtual router.                                   | <code>priority vlan <i>vlan-id</i> <i>vrid</i> <i>priority-value</i></code>         |
| 5.   | Optionally, change the advertise interval for this virtual router.                                     | <code>advertise-interval vlan <i>vlan-id</i> <i>vrid</i> <i>interval</i></code>     |
| 6.   | Optionally change the master preemption setting for this VRRP router. Default is enabled.              | <code>preempt <i>vlan-id</i> <i>vrid</i></code>                                     |
| 7.   | Optionally, enable ICMP replies for non-owner masters.                                                 | <code>master-icmp-reply vlan <i>vlan-id</i> <i>vrid</i></code>                      |
| 8.   | Optionally, in interface configuration mode, configure a VRRP authentication key on an interface.      | <code>ip vrrp authentication-key <i>name</i></code>                                 |
| 9.   | In router configuration mode, enable VRRP on the interface.                                            | <code>enable vlan <i>vlan-id</i> <i>vrid</i></code>                                 |
| 10.  | Display VRRP information.                                                                              | <code>show ip vrrp</code>                                                           |

## Configuration Examples

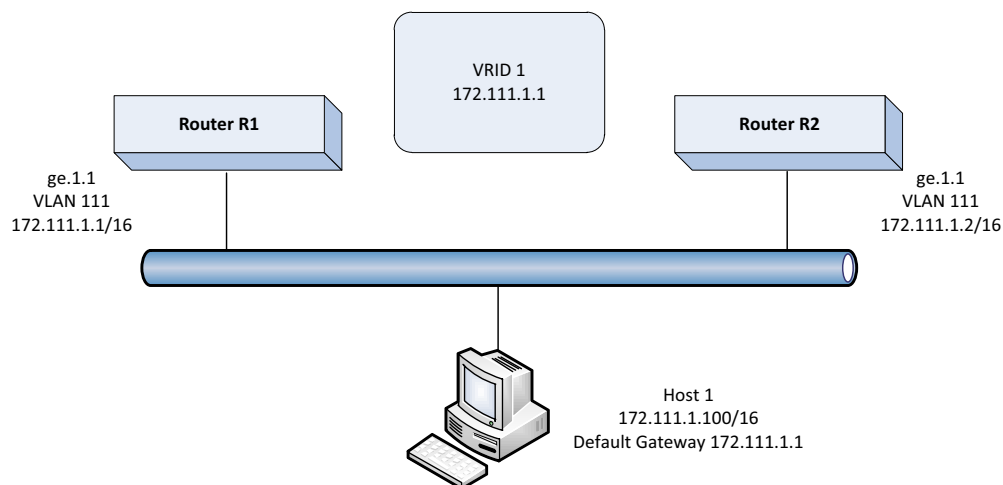
### Basic VRRP Configuration

[Figure 23-2](#) shows a basic VRRP configuration with a single virtual router. Routers R1 and R2 are both configured with one virtual router (VRID 1). Router R1 serves as the master because the VRRP router owns the IP address for this virtual router. Router R2 serves as the backup. The hosts are configured to use 172.111.1.1/16 as the default route.

The master advertise-interval is changed to 2 seconds for VRID 1.

If Router R1 should become unavailable, Router R2 would take over virtual router VRID 1 and its associated IP addresses. Packets sent to 172.111.1.1/16 would go to Router R2. When Router R1 comes up again, it would take over as master, and Router R2 would revert to backup.

**Figure 23-2 Basic Configuration Example**



### Router 1

```
Router 1(su)->router(Config)#interface vlan 111
Router 1(su)->router(Config-if(Vlan 111))#ip address 172.111.1.1 255.255.255.0
Router 1(su)->router(Config-if(Vlan 111))#no shutdown
Router 1(su)->router(Config-if(Vlan 111))#exit
```

```
Router 1(su)->router(Config)#router vrrp
Router 1(su)->router(Config-router)#create vlan 111 1
Router 1(su)->router(Config-router)#address vlan 111 1 172.111.1.1 1
Router 1(su)->router(Config-router)#advertise-interval vlan 111 1 2
Router 1(su)->router(Config-router)#enable vlan 111 1
Router 1(su)->router(Config-router)#exit
```

### Router 2

```
Router 2(su)->router(Config)#interface vlan 111
Router 2(su)->router(Config-if(Vlan 111))#ip address 172.111.1.2 255.255.255.0
Router 2(su)->router(Config-if(Vlan 111))#no shutdown
Router 2(su)->router(Config-if(Vlan 111))#exit
```

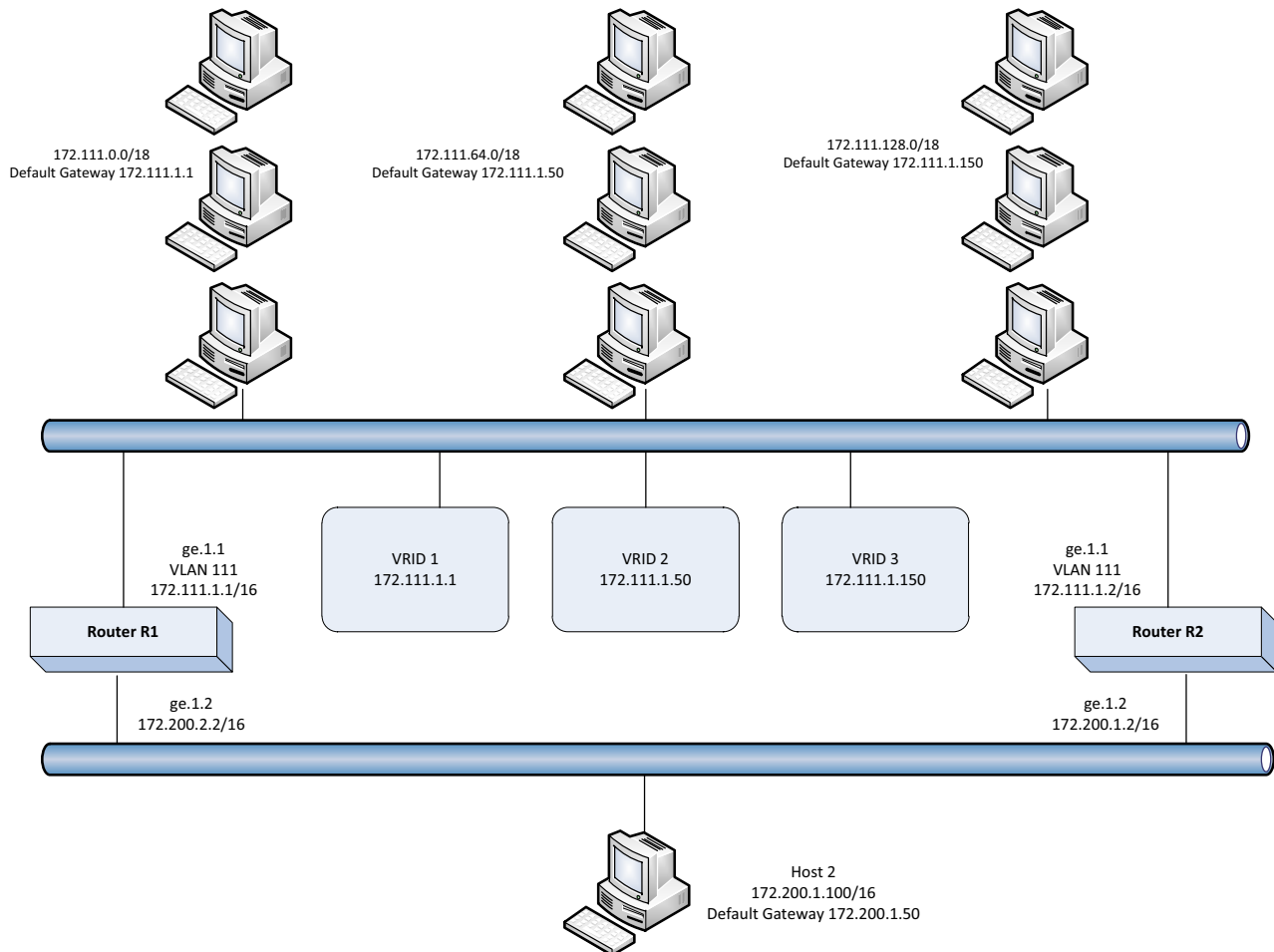
```
Router 2(su)->router(Config)#router vrrp
Router 2(su)->router(Config-router)#create vlan 111 1
Router 2(su)->router(Config-router)#address vlan 111 1 172.111.1.1 0
Router 2(su)->router(Config-router)#advertise-interval vlan 111 1 2
Router 2(su)->router(Config-router)#master-icmp-reply vlan 111 1
Router 2(su)->router(Config-router)#enable vlan 111 1
```

```
Router 2(su)->router(Config-router)#exit
```

## Multiple Backup VRRP Configuration

Figure 23-3 shows a multi-backup sample configuration.

Figure 23-3 Multi-Backup VRRP Configuration Example



Three VRRP instances are configured on VLAN 111 for both fixed switch devices — on Router R1’s interface, 172.111.1.1, and Router R2’s interface, 172.111.1.2. Each virtual router is given a different virtual IP address that is used as a default gateway by a subset of hosts that reside on the LAN segment. Because interfaces on Router R1 and Router R2 for VLAN 111 are configured as belonging to VRID 1, 2, and 3, VRRP will support resiliency between these interfaces if one interface fails.

To load balance traffic generated from the hosts on the 172.111.0.0/16 network, the hosts are partitioned into being configured with default gateways matching the virtual IP address of the VRRP virtual routers, and the VRRP Master for each VRRP instance is configured for distribution across Router R1 and Router R2. It is known that Router R1’s interface, 172.111.1.1, will become Master for VRID 1 because it is the IP address owner for the virtual router. This interface is also configured to be Master for VRID 3 by raising its VRRP priority in VRRP instance 3 to 200. Therefore, Router R1’s interface 172.111.1.1 will be Master for VRID 1 and VRID 3 handling traffic on this LAN segment sourced from subnets 172.111.0.0/18 and 172.111.128.0/18. Router R2’s interface is configured to be the Master for VRID 2 by raising its VRRP priority in VRRP instance

2. Therefore, Router R2's interface 172.111.1.2 will be Master for VRID 2 handling traffic on this LAN segment sourced from subnets 172.111.64.0/18.

In this configuration, an interface on VLAN 111 for Router R1 or Router R2, or VRID 1, 2, or 3 fails, the interface on the other router will take over for forwarding outside the local LAN segment.

### Router R1

```
Router 1(su)->router(Config)#interface vlan 111
Router 1(su)->router(Config-if(Vlan 111))#ip address 172.111.1.1 255.255.255.0
Router 1(su)->router(Config-if(Vlan 111))#no shutdown
Router 1(su)->router(Config-if(Vlan 111))#exit
```

```
Router 1(su)->router(Config)#router vrrp
Router 1(su)->router(Config-router)#create vlan 111 1
Router 1(su)->router(Config-router)#address vlan 111 1 172.111.1.1 1
Router 1(su)->router(Config-router)#enable vlan 111 1
```

```
Router 1(su)->router(Config-router)#create vlan 111 2
Router 1(su)->router(Config-router)#address vlan 111 2 172.111.1.50 0
Router 1(su)->router(Config-router)#master-icmp-reply vlan 111 2
Router 1(su)->router(Config-router)#enable vlan 111 2
```

```
Router 1(su)->router(Config-router)#create vlan 111 3
Router 1(su)->router(Config-router)#address vlan 111 3 172.111.1.150 0
Router 1(su)->router(Config-router)#master-icmp-reply vlan 111 3
Router 1(su)->router(Config-router)#priority vlan 111 3 200
Router 1(su)->router(Config-router)#enable vlan 111 3
```

```
Router 1(su)->router(Config-router)#exit
```

### Router R2

```
Router 2(su)->router(Config)#interface vlan 111
Router 2(su)->router(Config-if(Vlan 111))#ip address 172.111.1.2 255.255.255.0
Router 2(su)->router(Config-if(Vlan 111))#no shutdown
Router 2(su)->router(Config-if(Vlan 111))#exit
```

```
Router 2(su)->router(Config)#router vrrp
Router 2(su)->router(Config-router)#create vlan 111 1
Router 2(su)->router(Config-router)#address vlan 111 1 172.111.1.1 0
Router 2(su)->router(Config-router)#master-icmp-reply vlan 111 1
Router 2(su)->router(Config-router)#enable vlan 111 1
```

```
Router 2(su)->router(Config-router)#create vlan 111 2
Router 2(su)->router(Config-router)#address vlan 111 2 172.111.1.50 0
Router 2(su)->router(Config-router)#priority vlan 111 2 200
Router 2(su)->router(Config-router)#master-icmp-reply vlan 111 2
Router 2(su)->router(Config-router)#enable vlan 111 2
```

```

Router 2(su)->router(Config-router)#create vlan 111 3
Router 2(su)->router(Config-router)#address vlan 111 3 172.111.1.150 0
Router 2(su)->router(Config-router)#master-icmp-reply vlan 111 3
Router 2(su)->router(Config-router)#enable vlan 111 3

Router 2(su)->router(Config-router)#exit

```

## Terms and Definitions

[Table 23-2](#) lists terms and definitions used in this VRRP configuration discussion.

**Table 23-2 VRRP Configuration Terms and Definitions**

| Term             | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup           | The set of VRRP routers available to assume forwarding responsibility for a virtual router should the current Master fail.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| IP Address owner | The VRRP router that has the virtual router's IP address(es) as real interface address(es). This is the router that, when up, will respond to packets addressed to one of these IP addresses for ICMP pings, TCP connections, etc.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Master           | The VRRP router that is assuming the responsibility of forwarding packets sent to the IP address(es) associated with the virtual router, and answering ARP requests for these IP addresses.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Priority         | <p>The priority field specifies the sending VRRP router's priority for the virtual router. Higher values equal higher priority. This field is an 8 bit unsigned integer field. The priority value for the VRRP router that owns the IP address(es) associated with the virtual router MUST be 255 (decimal).</p> <p>VRRP routers backing up a virtual router MUST use priority values between 1-254 (decimal). The default priority value for VRRP routers backing up a virtual router is 100 (decimal). The priority value zero (0) has special meaning indicating that the current Master has stopped participating in VRRP. This is used to trigger Backup routers to quickly transition to Master without having to wait for the current Master to timeout.</p> |
| Virtual Router   | An abstract object managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a Virtual Router Identifier and a set of associated IP address(es) across a common LAN. A VRRP Router may backup one or more virtual routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| VRID             | Virtual Router ID — a unique number associated with each virtual router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| VRRP Router      | <p>A router running the Virtual Router Redundancy Protocol. It may participate in one or more virtual routers.</p> <p>A VRRP router may associate a virtual router with its real addresses on an interface, and may also be configured with additional virtual router mappings and priority for virtual routers it is willing to backup.</p>                                                                                                                                                                                                                                                                                                                                                                                                                        |



## Configuring Access Control Lists

This chapter describes how to configure access control lists on the Fixed Switch platforms. ACLs on the A4 are described separately in this chapter since ACL support on the A4 is different from the support on the other Fixed Switch platforms.

| For information about...                                          | Refer to page... |
|-------------------------------------------------------------------|------------------|
| <a href="#">Using Access Control Lists (ACLs) in Your Network</a> | 24-1             |
| <a href="#">Implementing ACLs</a>                                 | 24-1             |
| <a href="#">ACL Configuration Overview</a>                        | 24-2             |
| <a href="#">Configuring ACLs</a>                                  | 24-7             |
| <a href="#">Access Control Lists on the A4</a>                    | 24-11            |

### Using Access Control Lists (ACLs) in Your Network

ACLs allow the configuration of permit and denial of IPv4, IPv6, and MAC packet forwarding based upon IP address, protocol and port matching, and other criteria, depending upon the ACL type. The Fixed Switch firmware supports configuration of both standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs.

- Standard IPv4 ACLs support standard rules based on source IPv4 address and mask. Standard IP ACLs are uniquely identified by number.
- Extended IPv4 ACLs support extended rules based on protocol, IPv4 source and destination addresses, layer 4 port, precedence, TOS or DSCP values. Extended IP ACLs are uniquely identified by number.
- MAC ACLs support rules-based source and destination MAC addresses as well as Ether type, VLAN tag, and priority tag values. MAC ACLs are uniquely identified by name.
- IPv6 ACLs support rules based on protocol, IPv6 source and destination addresses, layer 4 port, DSCP value, and Flow Label value. IPv6 ACLs are uniquely identified by name.

### Implementing ACLs

To implement an ACL on your network:

- Create the ACL
- Enter the rules for this ACL that will determine which packets will be forwarded or not forwarded on the routing interface this ACL will be applied to
- Optionally manage your ACL by:
  - Deleting or replacing an ACL rule entry

- Inserting a new ACL rule entry into an ACL
- Moving an ACL rule to a new location in an ACL
- Apply the ACL to VLAN interfaces, to ports, or to Link Aggregation ports.

## ACL Configuration Overview

This section describes ACL creation, rule entry, and application of the ACL to a port or routing VLAN required to implement an ACL, as well as, the features available for managing ACL rules and displaying ACLs.

### Creating IPv4 ACLs

There are two types of IPv4 ACLs: standard and extended. The type of ACL you need depends exclusively upon the packet field(s) that will generate a hit for the rules specified in the ACL. For a standard ACL, only the source IP address is configurable. For an extended ACL, the protocol, source IP address, destination IP address, IP precedence, TOS or DSCP values, and in the case of the TCP or UDP protocols, matching source and destination ports are configurable.

IPv4 ACLs are identified by number only. Standard IPv4 ACL numbers range from **1** to **99**. Extended IPv4 ACL numbers range from **100** to **199**.

Once you have determined the appropriate ACL type, use the **access-list** command in router global configuration mode to create the list, specifying the number for the access control list, and the rule you want to add to the list.

IPv4 standard and extended access control lists are applied to VLAN interfaces by using the **ip access-group** command and to ports with the **access-list interface** command.

### Creating IPv6 and MAC ACLs

In order to configure IPv6 or MAC ACLs, the switch must be put into access list “**ipv6mode**” with the **access-list ipv6mode** command. By default, this mode is disabled and the rule limits for standard and extended IPv4 ACLs remain unchanged.

When **ipv6mode** is disabled, IPv6 and MAC ACLs cannot be configured, and any existing IPv6 and MAC ACLs are removed from the configuration. The **ipv6mode** cannot be enabled if Policy is configured on the switch, and Policy configurations will not be accepted when the switch is in **ipv6mode**.

When **ipv6mode** is enabled or disabled, a system reset is required to change the mode. The configuration of **ipv6mode** is persistent and is shown in the running configuration.

After **ipv6mode** is enabled, IPv6 ACLs are created and configured in router global configuration mode with the **access-list ipv6** command, specifying the name of the access control list and the rule you want to add to the list. IPv6 rules can be based on protocol, IPv6 source and destination addresses, layer 4 port, DSCP value, and Flow Label value.

IPv6 access control lists are applied to VLAN interfaces by using the **ipv6 access-group** command and to ports with the **access-list interface** command.

MAC ACLs are created and configured in router global configuration mode with the **access-list mac** command, specifying the name of the access control list and the rule you want to add to the list. MAC rules can be based on source and destination MAC addresses as well as Ether type, VLAN tag, and priority tag values.

MAC access control lists are applied to VLAN interfaces by using the **ip access-group** command and to ports with the **access-list interface** command.

## Creating ACL Rules

ACL rules define the basis upon which a hit will take place for the ACL. Rules in an ACL are order-dependent. A packet is either forwarded (a **permit** rule) or not forwarded (a **deny** rule) according to the first rule that is matched. The matching criteria available is determined based upon whether the ACL is a standard or extended IPv4 ACL, an IPv6 ACL, or a MAC ACL. As soon as a rule is matched, processing of the access list stops. There is an implicit “deny all” rule at the end of every ACL. If all rules are missed, the packet is not forwarded.

### IPv4 Rules

For a standard ACL, a source IPv4 address and an optional wildcard are specified for the rule. For an extended ACL a source and destination IP address and wildcard are specified for the rule. In the case of an IPv4 address, source and destination wildcards provide an inverted mask (specifies the don't care bits as 1s). 0.0.0.0 specifies an exact match. An **any** option is available, which is short hand for 0.0.0.0 255.255.255.255.

For an extended IPv4 ACL, the following protocols can be specified in a rule:

- A specific or all IPv4 protocols
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Internet Control Message Protocol (ICMP)

TCP and UDP rules can match specific source and destination ports.

Extended ACLs can optionally be set to match a Diffserv codepoint (DSCP), IP precedence, or IP Type of Service (ToS) value.

IPv4 **permit** rules also allow you to specify the queue to which a packet matching the permit rule will be assigned. Valid values for *queue-id* are from 0 to 5.

### IPv4 Rule Examples

This example shows how to create IPv4 standard access list 1 with three entries that allow access to only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the access list entries will be rejected:

```
C5(su)->router(Config)#access-list 1 permit 192.5.34.0 0.0.0.255
C5(su)->router(Config)#access-list 1 permit 128.88.0.0 0.0.255.255
C5(su)->router(Config)#access-list 1 permit 36.0.0.0 0.255.255.255
```

This example shows how to define IPv4 extended access list 145 to deny ICMP transmissions from any source and for any destination:

```
C5(su)->router(Config)#access-list 145 deny ICMP any any
```

This example appends to access list 145 a permit statement that allows the host with IP address 88.255.255.254 to perform SSH remote logins to any destination on TCP port 22.

```
C5(su)->router(Config)#access-list 145 permit tcp host 88.255.255.254 any eq 22
```

This example appends to access list 145 a permit statement that allows SNMP control traffic (from UDP port 161) to be sent from IP addresses within the range defined by 88.255.128.0 0.0.127.255 to any destination.

```
C5(su)->router(Config)#access-list 145 permit udp 88.255.128.0 0.0.127.255 eq 161
any
```

## IPv6 Rules

For IPv6 rules, IPv6 source and destination addresses and prefix length are specified, or the **any** option can be used.

For an IPv6 ACLs, the following protocols can be specified in a rule:

- Any IPv6 protocol
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- IPv6 Internet Control Message Protocol (ICMPv6)

TCP and UDP rules can match specific source and destination ports.

IPv6 ACLs can optionally be set to match a Diffserv codepoint (DSCP) or flow label value.

IPv6 **permit** rules also allow you to specify the queue to which a packet matching the permit rule will be assigned. Valid values for *queue-id* are from 0 to 5.

### IPv6 Rule Example

This example creates an IPv6 access control list named “ipv6list1” with a rule that denies ICMPv6 transmissions from IPv6 address 2001:db08:10::1/64 to any destination.

```
C5(su)->router(Config)#access-list ipv6 ipv6list1 deny icmpv6 2001:db08:10::1/64 any
```

## MAC Rules

For MAC rules, the source and destination addresses are specified as MAC addresses, or the **any** option can be used. The format of the MAC address can be xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx.

MAC ACL rules can filter on:

- The Ethernet II type of the packet.  
You can specify the type with either a four digit hexadecimal number in the range 0x0600 to 0xFFFF, or one of the following key words: **appletalk**, **arp**, **ibmsna**, **ipv4**, **ipv6**, **ipx**, **mplsmcast**, **mplsucast**, **netbios**, **novell**, **pppoe**, **rarp**.
- VLAN ID.
- 802.1p priority value, which can range from 0 to 7.

MAC **permit** rules also allow you to specify the queue to which a packet matching the permit rule will be assigned. Valid values for *queue-id* are from 0 to 5.

### MAC Rule Example

This example creates a MAC-based access control list named “myaclist” with a rule that permits ARP packets from any source to the destination address 00-E0-ED-1D-90-D5 and assigns the packets to queue 1.

```
B3(su)->router(Config)#access-list mac myaclist permit any 00-E0-ED-1D-90-D5 ethertype arp assign-queue 1
```

## Managing ACLs

### Deleting ACLs and Rules

An access control list, or a single rule or range of rules, can be deleted using the **no** version of the **access-list** commands.

The following example displays IPv4 extended access control list 120, then deletes entries 2 and 3, and redispays the ACL.

```
C5(su)->router(Config)#show access-lists 120

Extended IP access list 120
 1: deny ip 20.0.0.1 0.0.255.255 any
 2: deny ip 30.0.0.1 0.0.255.255 any
 3: deny ip 40.0.0.1 0.0.255.255 any
 4: permit ip any any

C5(su)->router(Config)#no access-list 120 2 3
C5(su)->router(Config)#show access-lists 120

Extended IP access list 120
 1: deny ip 20.0.0.1 0.0.255.255 any
 2: permit ip any any
```

## Moving ACL Rules

An ACL rule or range of rules can be moved to a different location in the ACL using the **move** option.

The following example displays IPv4 extended access control list 121, then moves entries 3 and 4 to before entry 2.

```
C5(su)->router(Config)#show access-lists 121

Extended IP access list 121
 1: deny ip 20.0.0.1 0.0.255.255 any
 2: permit ip any any
 3: deny ip 30.0.0.1 0.0.255.255 any
 4: deny ip 40.0.0.1 0.0.255.255 any

C5(su)->router(Config)#access-list 121 move 2 3 4
C5(su)->router(Config)#show access-lists 121

Extended IP access list 121
 1: deny ip 20.0.0.1 0.0.255.255 any
 2: deny ip 30.0.0.1 0.0.255.255 any
 3: deny ip 40.0.0.1 0.0.255.255 any
 4: permit ip any any
```

## Replacing ACL Rules

An ACL rule can be replaced using the **replace** option.

The following example replaces entry 1 in IPv4 extended ACL 121.

```
C5(su)->router(Config)#show access-lists 121

Extended IP access list 121
 1: deny ip 20.0.0.1 0.0.255.255 any
 2: deny ip 30.0.0.1 0.0.255.255 any
 3: deny ip 40.0.0.1 0.0.255.255 any
 4: permit ip any any

C5(su)->router(Config)#access-list 121 replace 1 deny ip 10.0.0.1 0.0.255.255 any
C5(su)->router(Config)#show access-lists 121

Extended IP access list 121
 1: deny ip 10.0.0.1 0.0.255.255 any
```

```
2: deny ip 30.0.0.1 0.0.255.255 any
3: deny ip 40.0.0.1 0.0.255.255 any
4: permit ip any any
```

## Inserting ACL Rules

When you enter an ACL rule, the new rule is appended to the end of the existing rules by default. You can insert a new rule into a specified entry location using the **insert** option.

The following example inserts a new entry into IPv4 extended ACL 121 before entry 2.

```
C5(su)->router(Config)#show access-lists 121
```

```
Extended IP access list 121
 1: deny ip 10.0.0.1 0.0.255.255 any
 2: deny ip 30.0.0.1 0.0.255.255 any
 3: deny ip 40.0.0.1 0.0.255.255 any
 4: permit ip any any
```

```
C5(su)->router(Config)#access-list 121 insert 2 deny ip 20.0.0.1 0.0.255.255 any
C5(su)->router(Config)#show access-lists 121
```

```
Extended IP access list 121
 1: deny ip 10.0.0.1 0.0.255.255 any
 2: deny ip 20.0.0.1 0.0.255.255 any
 3: deny ip 30.0.0.1 0.0.255.255 any
 4: deny ip 40.0.0.1 0.0.255.255 any
 5: permit ip any any
```

## Applying ACLs

Once you have defined the ACL, it can be applied to both VLAN interfaces and to ports. ACLs are supported on Link Aggregation ports.

- IPv4 standard and extended access control lists are applied to VLAN interfaces by using the **ip access-group** command and to ports with the **access-list interface** command.
- IPv6 access control lists are applied to VLAN interfaces by using the **ipv6 access-group** command and to ports with the **access-list interface** command.
- MAC access control lists are applied to VLAN interfaces by using the **ip access-group** command and to ports with the **access-list interface** command.

When applying an ACL, you can specify the order in which the ACL is applied relative to other ACLs that may already be associated with the interface or port, with the **sequence** option.

The following example applies the IPv4 extended access list 121 in the inbound direction to VLAN 100.

```
C5(su)->router(Config)#interface vlan 100
C5(su)->router(Config-if(Vlan 100))#ip access-group 121 in
C5(su)->router(Config-if(Vlan 100))#exit
C5(su)->router(Config)#show access-lists vlan 100
```

```
Vlan ID Access-list

100 121
```

The following example applies the IPv4 extended ACL 121 to the port ge.1.29.

```
C5(su)->router(Config)#access-list interface 121 ge.1.29
C5(su)->router(Config)#show access-lists interface ge.1.29
```

|             |             |
|-------------|-------------|
| Port-string | Access-list |
| -----       | -----       |
| ge.1.29     | 121         |

## Configuring ACLs

This section provides procedures and examples for configuring IPv4, IPv6, and MAC ACLs. With the exception of A4 ACLs, all ACLs are terminated with an implicit “deny all” rule.

### Configuring IPv4 ACLs

[Procedure 24-1](#) describes how to configure IPv4 standard and extended ACLs.

#### Procedure 24-1 Configuring IPv4 Standard and Extended ACLs

| Step | Task                                                                      | Command(s)                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | In global router configuration mode, create the ACL and define the rules. |                                                                                                                                                                                                                                                      |
| 1a   | Standard ACLs must be numbered from 1 to 99.                              | <code>access-list acl-number {deny   permit} source [source-wildcard] [assign-queue queue-id]</code>                                                                                                                                                 |
| 1b   | Extended ACLs must be numbered from 100 to 199.                           | <code>access-list acl-number {deny   permit} protocol source [source-wildcard] [eq port] destination [destination-wildcard] [eq port][precedence precedence   tos tos tosmask   dscp dscp ] [assign-queue queue-id]</code>                           |
| 2.   | Optionally, insert new or replace existing rules                          |                                                                                                                                                                                                                                                      |
| 2a   | For standard ACLs                                                         | <code>access-list acl-number insert   replace entryno {deny   permit} source [source-wildcard] [assign-queue queue-id]</code>                                                                                                                        |
| 2b   | For extended ACLs                                                         | <code>access-list acl-number insert   replace entryno {deny   permit} protocol source [source-wildcard] [eq port] destination [destination-wildcard] [eq port] [precedence precedence   tos tos tosmask   dscp dscp ] [assign-queue queue-id]</code> |
| 3.   | Optionally, move entries within the ACL.                                  | <code>access-list acl-number move destination source1 [source2]</code>                                                                                                                                                                               |
| 4.   | Display the contents of the ACL.                                          | <code>show access-lists [number]</code>                                                                                                                                                                                                              |
| 5.   | Apply the ACL:                                                            |                                                                                                                                                                                                                                                      |
| 5a   | In router interface configuration mode, apply to a routing VLAN interface | <code>ip access-group acl-number in [sequence sequence]</code>                                                                                                                                                                                       |
| 5b   | In global router configuration mode, apply to an interface                | <code>access-list interface acl-number port-string in [sequence sequence]</code>                                                                                                                                                                     |

**Procedure 24-1 Configuring IPv4 Standard and Extended ACLs (continued)**

| Step | Task                                                                 | Command(s)                                                                                            |
|------|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| 6.   | Optionally, display the ACLs associated with a VLAN or port.         | <b>show access-lists</b> [ <b>interface</b> <i>[port-string]</i> ]   [ <b>vlan</b> <i>[vlan-id]</i> ] |
| 7.   | Optionally, delete an entire ACL or a single rule or range of rules. | <b>no access-list</b> <i>acl-number</i> [ <i>entryno</i> ] [ <i>entryno</i> ]                         |

**Example**

The following example creates an IPv4 extended ACL and associates it with VLAN 100.

```
C5(su)->router
C5(su)->router>enable
C5(su)->router#configure
Enter configuration commands:
C5(su)->router(Config)#access-list 121 deny ip 20.0.0.1 0.0.255.255 any
C5(su)->router(Config)#access-list 121 deny ip 30.0.0.1 0.0.255.255 any
C5(su)->router(Config)#access-list 121 deny ip 40.0.0.1 0.0.255.255 any
C5(su)->router(Config)#access-list 121 permit ip any any

C5(su)->router(Config)#show access-lists 121

Extended IP access list 121
 1: deny ip 20.0.0.1 0.0.255.255 any
 2: deny ip 30.0.0.1 0.0.255.255 any
 3: deny ip 40.0.0.1 0.0.255.255 any
 4: permit ip any any

C5(su)->router(Config)#interface vlan 100
C5(su)->router(Config-if(Vlan 100))#ip access-group 121 in
C5(su)->router(Config-if(Vlan 100))#exit

C5(su)->router(Config)#show access-lists vlan 100

Vlan ID Access-list
----- -
100 121
```

**Configuring IPv6 ACLs**

[Procedure 24-2](#) describes how to configure an IPv6 ACL.

**Procedure 24-2 Configuring IPv6 ACLs**

| Step | Task                                                                                                                                                    | Command(s)                        |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| 1.   | Optionally, display the status of ipv6mode.                                                                                                             | <b>show access-lists ipv6mode</b> |
| 2.   | If necessary, in global router configuration mode, enable ipv6mode, which requires a reset of the switch.<br>Enter y when prompted to reset the switch. | <b>access-list ipv6mode</b>       |



**Procedure 24-2 Configuring IPv6 ACLs (continued)**

| Step | Task                                                                                                      | Command(s)                                                                                                                                                                                                            |
|------|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.   | After the switch resets, return to global router configuration mode, create the ACL and define the rules. | <b>access-list ipv6 name</b> {deny   permit} protocol {srcipv6-addr/prefix-length   any} [eq port] {dstipv6-addr/prefix-length   any} [eq port] [dscp dscp] [flow-label label-value] [assign-queue queue-id]          |
| 4.   | Optionally, insert new or replace existing rules.                                                         | <b>access-list ipv6 name insert   replace entryno</b> {deny   permit} protocol srcipv6-addr/prefix-length [eq port] dstipv6-addr/prefix-length [eq port] [dscp dscp] [flow-label label-value] [assign-queue queue-id] |
| 5.   | Optionally, move entries within the ACL                                                                   | <b>access-list ipv6 name move destination source1</b> [source2]                                                                                                                                                       |
| 6.   | Display the contents of the ACL                                                                           | <b>show access-lists name</b>                                                                                                                                                                                         |
| 7.   | Apply the ACL:                                                                                            |                                                                                                                                                                                                                       |
| 7a   | In router interface configuration mode, apply to a routing VLAN interface                                 | <b>ipv6 access-group acl-name in</b> [sequence sequence]                                                                                                                                                              |
| 7b   | In global router configuration mode, apply to an interface                                                | <b>access-list interface acl-name port-string in</b> [sequence sequence]                                                                                                                                              |
| 8.   | Optionally, display the ACLs associated with a VLAN or port.                                              | <b>show access-lists</b> [interface [port-string]]   [vlan [vlan-id]]                                                                                                                                                 |
| 9.   | Optionally, delete an entire ACL or a single rule or range of rules.                                      | <b>no access-list ipv6 acl-name</b> [entryno [entryno]]                                                                                                                                                               |

**Example**

The following example puts the switch into ipv6mode, creates an IPv6 ACL, and associates it with VLAN 200.

```
C5(su)->router
C5(su)->router>enable
C5(su)->router#show access-lists ipv6mode
ipv6mode disabled
```

```
C5(su)->router#configure
Enter configuration commands:
C5(su)->router(Config)#access-list ipv6mode
Changing ipv6mode will result in a system reset.
Do you wish to proceed? (y/n) y
```

```
C5(su)->router
C5(su)->router>enable
C5(su)->router#configure
Enter configuration commands:
C5(su)->router(Config)#access-list ipv6 ipv6list1 deny icmpv6 2001:db08:10::1/64
any
C5(su)->router(Config)#access-list ipv6 ipv6list1 permit tcp 2001:db08:20::20/64
eq snmp any assign-queue 5
C5(su)->router(Config)#access-list ipv6 ipv6list1 permit ipv6 2001:FFFF:30::30/64
any
```

```

C5(su)->router(Config)#show access-lists ipv6list1
ipv6list1 IPV6 access-list
 1: deny icmpv6 2001:DB08:10::1/64 any
 2: permit tcp 2001:db08:20::20/64 eq snmp any assign-queue 5
 3: permit ipv6 2001:FFFF:30::30/64 any

C5(su)->router(Config)#interface vlan 200
C5(su)->router(Config-if(Vlan 200))#ipv6 access-group ipv6list1 in
C5(su)->router(Config-if(Vlan 200))#exit

```

## Configuring MAC ACLs

Procedure 24-3 describes how to configure a MAC ACL.

### Procedure 24-3 Configuring MAC ACLs

| Step | Task                                                                                                                                                        | Command(s)                                                                                                                                                                      |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Optionally, display the status of ipv6mode.                                                                                                                 | <b>show access-lists ipv6mode</b>                                                                                                                                               |
| 2.   | If necessary, in global router configuration mode, enable ipv6mode, which requires a reset of the switch.<br><br>Enter y when prompted to reset the switch. | <b>access-list ipv6mode</b>                                                                                                                                                     |
| 3.   | After the switch resets, return to global router configuration mode, create the ACL and define the rules.                                                   | <b>access-list mac name {deny   permit} {srcmac   any} {destmac   any} [ethertype ethertype] [vlan vlan-id] [priority pri] [assign-queue queue-id]</b>                          |
| 4.   | Optionally, insert new or replace existing rules.                                                                                                           | <b>access-list mac name insert   replace entryno {deny   permit} {srcmac   any} {destmac   any} [ethertype ethertype] [vlan vlan-id] [priority pri] [assign-queue queue-id]</b> |
| 5.   | Optionally, move entries within the ACL                                                                                                                     | <b>access-list mac name move destination source1 [source2]</b>                                                                                                                  |
| 6.   | Display the contents of the ACL                                                                                                                             | <b>show access-lists name</b>                                                                                                                                                   |
| 7.   | Apply the ACL:                                                                                                                                              |                                                                                                                                                                                 |
| 7a   | In router interface configuration mode, apply to a routing VLAN interface                                                                                   | <b>ip access-group acl-name in [sequence sequence]</b>                                                                                                                          |
| 7b   | In global router configuration mode, apply to an interface                                                                                                  | <b>access-list interface acl-name port-string in [sequence sequence]</b>                                                                                                        |
| 8.   | Optionally, display the ACLs associated with a VLAN or port.                                                                                                | <b>show access-lists [interface [port-string]]   [vlan [vlan-id]]</b>                                                                                                           |
| 9.   | Optionally, delete an entire ACL or a single rule or range of rules.                                                                                        | <b>no access-list mac acl-name [entryno [entryno]]</b>                                                                                                                          |

### Example

The following example puts the switch into ipv6mode, creates a MAC ACL, and associates it with VLAN 300.

```
C5(su)->router
```

```

C5(su)->router>enable
C5(su)->router#show access-lists ipv6mode
ipv6mode disabled

C5(su)->router#configure
Enter configuration commands:
C5(su)->router(Config)#access-list ipv6mode
Changing ipv6mode will result in a system reset.
Do you wish to proceed? (y/n) y

C5(su)->router
C5(su)->router>enable
C5(su)->router#configure
Enter configuration commands:

C5(su)->router(Config)#access-list mac mymaclist1 deny any any ethertype
appletalk
C5(su)->router(Config)#access-list mac mymaclist1 deny any any ethertype ipx
C5(su)->router(Config)#access-list mac mymaclist1 permit 00-E0-ED-1D-90-D5 any
priority 5 assign-queue 5

C5(su)->router(Config)#show access-lists mymaclist1
mymaclist1 MAC access-list
 1: deny any any ethertype appletalk
 2: deny any any ethertype ipx
 3: permit 00-E0-ED-1D-90-D5 any priority 5 assign-queue 5

C5(su)->router(Config)#interface vlan 300
C5(su)->router(Config-if(Vlan 300))#ip access-group mymaclist1 in
C5(su)->router(Config-if(Vlan 300))#exit

```

## Access Control Lists on the A4

Access control list support on the A4 is different from the support on the other Fixed Switch platforms. On the A4, an ACL can be configured as a MAC ACL or as an extended IP ACL, and each type of list can contain only one type of rule:

- MAC ACL rules can contain source and destination MAC addresses. MAC ACLs are uniquely identified by name.
- Extended IP ACL rules can contain source and destination IP addresses. Extended IP ACLs are uniquely identified by number, from 100 to 199.

ACLs can be applied to ports with the **access-list interface** command. ACLs are supported on Link Aggregation ports as well as physical ports. You can apply MAC, IP, or both types of ACLs to a port. Rule precedence is based on the priority levels shown in [Table 24-1](#), where highest priority has precedence.

**Table 24-1 ACL Rule Precedence**

| ACL Type and Rule    | Priority | Example                                    |
|----------------------|----------|--------------------------------------------|
| MAC SA DA exact      | 23       | permit 00-01-01-00-00-01 00-01-02-00-00-23 |
| MAC SA exact DA any  | 22       | deny 00:01:01:00:00:05 any                 |
| MAC SA any DA exact  | 21       | deny any 00:01:01:00:00:01                 |
| IP SIP DIP exact     | 20       | deny 10.0.1.15 10.0.1.5                    |
| IP SIP exact DIP any | 19       | deny 10.0.1.8 any                          |

**Table 24-1 ACL Rule Precedence (continued)**

| ACL Type and Rule    | Priority | Example              |
|----------------------|----------|----------------------|
| IP SIP any DIP exact | 18       | permit any 10.0.1.22 |
| IP SIP any DIP any   | 17       | deny any any         |
| MAC SA any DA any    | 16       | deny any any         |

Rule actions include:

- Deny — drop the packet.
- Permit — allow the frame to be switched.
- Assign to queue — assign the packet to a queue



**Note:** Unlike other Fixed Switch platforms, A4 ACLs are **not** terminated with an implicit “deny all” rule. You must add such a rule manually.

## Configuring A4 ACLs

This section provides procedures for configuring IPv4 extended and MAC ACLs on the A4.

### Extended IPv4 ACL Configuration

[Procedure 24-4](#) describes how to configure an IPv4 extended ACL on the A4.

#### Procedure 24-4 Configuring an IPv4 Extended ACL on the A4

| Step | Task                                                                                                                                   | Command(s)                                                                                                                                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | In global router configuration mode, create the ACL and define the rules.<br>The number of the ACL must be in the range of 100 to 199. | <b>access-list</b> <i>number</i> { <b>deny</b>   <b>permit</b> }<br><b>ip</b> ( <b>any</b>   <b>host</b> <i>src-ipaddr</i> ) { <b>any</b>   <b>host</b> <i>dest-ipaddr</i> } [ <b>assign-queue</b> <i>queue-id</i> ]                                                |
| 2.   | Optionally, insert new or replace existing rules                                                                                       | <b>access-list</b> <i>number</i> { <b>insert</b>   <b>replace</b> } <i>entryno</i> { <b>deny</b>   <b>permit</b> } <b>ip</b> ( <b>any</b>   <b>host</b> <i>src-ipaddr</i> ) { <b>any</b>   <b>host</b> <i>dest-ipaddr</i> } [ <b>assign-queue</b> <i>queue-id</i> ] |
| 3.   | Optionally, move entries within the ACL.                                                                                               | <b>access-list</b> <i>number</i> <b>move</b> <i>destination</i> <i>source1</i> [ <i>source2</i> ]                                                                                                                                                                   |
| 4.   | Display the contents of the ACL.                                                                                                       | <b>show access-lists</b> [ <i>number</i> ]                                                                                                                                                                                                                          |
| 5.   | Apply the ACL to an interface.                                                                                                         | <b>access-list interface</b> <i>number</i> <i>port-string</i> <b>in</b> [ <b>sequence</b> <i>sequence</i> ]                                                                                                                                                         |
| 6.   | Optionally, display the ACLs associated with a port.                                                                                   | <b>show access-lists</b> [ <b>interface</b> [ <i>port-string</i> ]]                                                                                                                                                                                                 |
| 7.   | Optionally, delete an entire ACL or a single rule or range of rules.                                                                   | <b>no access-list</b> <i>number</i> [ <i>entryno</i> [ <i>entryno</i> ]]                                                                                                                                                                                            |

### Example

The following example creates an IPv4 access-list numbered 101 and applies it to the port fwe1.1.

```
A4(su)->router
A4(su)->router>enable
```

```

A4(su)->router#configure
Enter configuration commands:

A4(su)->router(Config)#access-list 101 deny ip host 192.168.10.10 any
A4(su)->router(Config)#access-list 101 deny ip host 164.108.20.20 host
164.20.40.40
A4(su)->router(Config)#access-list 101 ip permit host 148.12.111.1 any assign-
queue 5

A4(su)->router(Config)#show access-lists 101
Extended IP access list 101
 1: deny ip host 192.168.10.10 any
 2: deny ip host 164.108.20.20 host 164.20.40.40
 3: permit ip host 148.12.111.1 any assign-queue 5

A4(su)->router(Config)#access-list interface 101 fe.1.1 in
A4(su)->router(Config)#show access-lists interface fe.1.1
Port-string Access-list

fe.1.1 101

```

## MAC ACL Configuration

[Procedure 24-5](#) describes how to configure an A4 MAC ACL.

### Procedure 24-5 Configuring MAC ACLs

| Step | Task                                                                      | Command(s)                                                                                                                  |
|------|---------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| 1.   | In global router configuration mode, create the ACL and define the rules. | <b>access-list mac name</b> {deny   permit} {srcmac   any} {destmac   any} [assign-queue queue-id]                          |
| 2.   | Optionally, insert new or replace existing rules.                         | <b>access-list mac name insert   replace entryno</b> {deny   permit} {srcmac   any} {destmac   any} [assign-queue queue-id] |
| 3.   | Optionally, move entries within the ACL                                   | <b>access-list mac name move destination source1</b> [source2]                                                              |
| 4.   | Display the contents of the ACL                                           | <b>show access-lists name</b>                                                                                               |
| 5.   | In global router configuration mode, apply the ACL to an interface.       | <b>access-list interface name port-string in</b> [sequence sequence]                                                        |
| 6.   | Optionally, display the ACLs associated with a port.                      | <b>show access-lists</b> [interface [port-string]]                                                                          |
| 7.   | Optionally, delete an entire ACL or a single rule or range of rules.      | <b>no access-list mac name</b> [entryno [entryno]]                                                                          |

### Example

The following example creates an A4 MAC ACL and applies it to port fe.1.2.

```

A4(su)->router
A4(su)->router>enable
A4(su)->router#configure
Enter configuration commands:

A4(su)->router(Config)#access-list mac mymac deny 00-E0-ED-1D-90-D5 any

```

```
A4(su)->router(Config)#access-list mac mymac permit 00:01:00:02:00:01 any assign-queue 2
```

```
A4(su)->router(Config)#show access-lists mymac
```

```
mymac MAC access-list
 1: deny 00-E0-ED-1D-90-D5 any
 2: permit 00:01:00:02:00:01 any assign-queue 2
```

```
A4(su)->router(Config)#access-list interface mymac fe.1.2 in
```

```
A4(su)->router(Config)#show access-lists interface fe.1.2
```

```
Port-string Access-list

fe.1.2 mymac
```

## Configuring and Managing IPv6

This chapter provides information about the following topics:

| For information about...                   | Refer to page... |
|--------------------------------------------|------------------|
| <a href="#">Managing IPv6</a>              | 25-1             |
| <a href="#">IPv6 Routing Configuration</a> | 25-3             |
| <a href="#">IPv6 Neighbor Discovery</a>    | 25-11            |
| <a href="#">DHCPv6 Configuration</a>       | 25-14            |

### Managing IPv6

At the switch command level, you can:

- Enable or disable the IPv6 management function
- Configure the IPv6 host and default gateway addresses
- Monitor network connectivity

By default, IPv6 management is disabled. When you enable IPv6 management on the switch, the system automatically generates a link-local host address for the switch from the host MAC address and a link-local address for the default gateway. You can set a different host IPv6 address with the **set ipv6 address** command and a different gateway address with the **set ipv6 gateway** command.

When you manually configure a global unicast IPv6 address for IPv6 management, you can specify the address completely, or you can use the optional **eui64** parameter to allow the switch to generate the lower order 64 bits of the address. When using the **eui64** parameter, you specify only the network prefix and length.

At the switch level, monitoring network connectivity includes:

- Displaying IPv6 network connection information with the **show ipv6 netstat** command.
- Displaying the system IPv6 Neighbor Discovery cache with the **show ipv6 neighbors** command.
- Testing network connectivity by sending IP ping requests to a specific IPv6 address or to a link local address with the **ping ipv6** command.
- Discovering the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis with the **traceroute ipv6** command.

## Configuring IPv6 Management

[Procedure 25-1](#) describes how to enable IPv6 management and optionally, create a host IPv6 global unicast address and replace the automatically generated default gateway IPv6 address.

Refer to the *CLI Reference* for your platform for more information about the commands listed below.

### Procedure 25-1 Configuring IPv6 Management

| Step | Task                                                                                                                                          | Command(s)                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| 1.   | Display current IPv6 management status.                                                                                                       | <code>show ipv6 status</code>                                                        |
| 2.   | If necessary, enable IPv6 management.<br>Link-local addresses are automatically generated for the host interface and for the default gateway. | <code>set ipv6 enable</code>                                                         |
| 3.   | If desired, configure a global unicast IPv6 address for IPv6 management on the host interface.                                                | <code>set ipv6 address <i>ipv6-addr/prefix-length</i> [<i>eui64</i>]</code>          |
| 4.   | If desired, replace the automatically generated default gateway IPv6 address.                                                                 | <code>set ipv6 gateway <i>ipv6-addr</i></code>                                       |
| 5.   | Optionally, delete one or all manually configured host IPv6 addresses.                                                                        | <code>clear ipv6 [<i>address</i> {<i>all</i> <i>ipv6-addr/prefix-length</i>}]</code> |
| 6.   | Optionally, delete the IPv6 default gateway address.                                                                                          | <code>clear ipv6 gateway</code>                                                      |

### Example

The following example enables IPv6 management, then creates a global unicast IPv6 host address and replaces the automatically generated gateway address.

```
C5(su)->show ipv6 status
IPv6 Administrative Mode: Disabled
C5(su)-> set ipv6 enable

C5(su)->show ipv6 status
IPv6 Administrative Mode: Enabled

C5(su)->show ipv6 address
Name IPv6 Address

host FE80::201:F4FF:FE5C:2880/64
gateway FE80::21F:45FF:FE8C:10D5

C5(su)->set ipv6 address 2001:0db8:1234:5555::/64 eui64

C5(su)->show ipv6 address
Name IPv6 Address

host FE80::201:F4FF:FE5C:2880/64
host 2001:DB8:1234:5555:201:F4FF:FE5C:2880/64
gateway FE80::21F:45FF:FE8C:10D5

C5(su)->set ipv6 gateway fe80::201:f4ff:fe5d:1234
C5(su)->show ipv6 address
Name IPv6 Address
```



```

host FE80::201:F4FF:FE5C:2880/64
host 2001:DB8:1234:5555:201:F4FF:FE5C:2880/64
gateway FE80::201:F4FF:FE5D:1234

```

## Monitoring Network Connections

Table 25-1 describes the tasks and commands used to monitor network connections at the switch level.

Refer to the *CLI Reference* for your platform for more information about the commands listed below.

**Table 25-1 Monitoring Network Connections at the Switch Level**

| Task                                                                                                                         | Command(s)                                                                     |
|------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Display IPv6 network connection information                                                                                  | <code>show ipv6 netstat</code>                                                 |
| Display the system IPv6 Neighbor Discovery cache                                                                             | <code>show ipv6 neighbors</code>                                               |
| Test network connectivity by sending IP ping requests                                                                        | <code>ping ipv6 {ipv6-addr   interface host link-local-addr} [size num]</code> |
| Discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis | <code>traceroute ipv6 ipv6-addr</code>                                         |

## IPv6 Routing Configuration

IPv6 routing must be enabled with a license key. If you have purchased an advanced or IPv6 routing license key, and have enabled routing on the device, you must activate your license as described in the chapter entitled “Activating Licensed Features” in order to enable the IPv6 routing configuration command set. If you wish to purchase an advanced IPv6 routing license, contact Enterasys Networks Sales.

### Overview

IPv6 and IPv4 coexist on the Enterasys Fixed Switch platforms. As with IPv4, IPv6 routing can be enabled on VLAN interfaces. Each Layer 3 routing interface can be used for IPv4, IPv6, or both.

The Enterasys Fixed Switches support all IPv6 address formats, including global unicast addresses, link-local unicast, global multicast, scoped multicast (including local scoped multicast), IPv4 compatible addresses, unspecified addresses, loopback addresses, and anycast addresses.

Refer to the following RFCs for more information about IPv6 address formats:

- RFC 4291, “IP Version 6 Addressing Architecture”
- RFC 3587, “IPv6 Global Unicast Address Format”
- RFC 4007, “IPv6 Scoped Address Architecture”

The basic IPv6 protocol specifies PDU options of two classes, both of which are supported: hop-by-hop options and destination options. While new options can be defined in the future, the following are currently supported: routing (for source routing), fragment, router alert, and pad. Jumbograms are not supported. In IPv6, only source nodes fragment. Path MTU discovery is therefore a requirement. Flow labels are ignored.

Neighbor Discovery is the IPv6 replacement for ARP. The Enterasys Fixed Switches support neighbor advertise and solicit, duplicate address detection, and unreachability detection. Router Advertisement is part of the Neighbor Discovery process and is required for IPv6. Stateless autoconfiguration is part of Router Advertisement and the Enterasys Fixed Switches can support both stateless and stateful autoconfiguration of end nodes. The Enterasys Fixed Switches support both EUI-64 interface identifiers and manually configured interface IDs.

Refer to the following RFCs for more information about Neighbor Discovery and stateless address autoconfiguration:

- RFC 4861, “Neighbor Discovery for IP Version 6”
- RFC 4862, “IPv6 Stateless Address Autoconfiguration”

For ICMPv6, error PDU generation is supported, as are path MTU, echo, and redirect.

Router Advertisement is an integral part of IPv6 and is supported. Numerous options are available including stateless/stateful address configuration, router and address lifetimes, and Neighbor Discovery timer control. Ping and traceroute applications for IPv6 are provided.

## Defaults

[Table 25-2](#) lists the default IPv6 conditions.

**Table 25-2 IPv6 Default Conditions**

| Condition                   | Default Value                                                                                        |
|-----------------------------|------------------------------------------------------------------------------------------------------|
| IPv6 forwarding             | Enabled                                                                                              |
| IPv6 route distance         | 1                                                                                                    |
| IPv6 maximum hop limit      | 64                                                                                                   |
| IPv6 unicast-routing        | Disabled                                                                                             |
| IPv6 enable                 | Disabled                                                                                             |
| IPv6 mtu                    | 1500                                                                                                 |
| IPv6 nd dad attempts        | 1                                                                                                    |
| IPv6 nd managed-config-flag | False                                                                                                |
| IPv6 nd ns-interval         | 0                                                                                                    |
| IPv6 nd other-config-flag   | False                                                                                                |
| IPv6 nd ra-interval         | 600                                                                                                  |
| IPv6 nd ra-lifetime         | 1800                                                                                                 |
| IPv6 nd reachable-time      | 0                                                                                                    |
| IPv6 nd suppress-ra         | Disabled                                                                                             |
| IPv6 nd prefix              | Valid-lifetime — 604800<br>Preferred-lifetime — 2592000<br>Autoconfig — enabled<br>On-link — enabled |

## Setting Routing General Parameters

IPv6 routing parameters are set in router global configuration mode. [Table 25-3](#) lists the tasks and commands. Refer to the *CLI Reference* for your platform for more information about the commands listed below.

**Table 25-3 Setting Routing General Parameters**

| Task                                                                                                                                                                                     | Command(s)                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Enable or disable IPv6 forwarding. Forwarding is enabled by default                                                                                                                      | <code>ipv6 forwarding</code><br><code>no ipv6 forwarding</code>           |
| Set the value of the hop limit field in IPv6 packets originated by this device. This value is also placed in the "Cur Hop Limit" field of router advertisements generated by this router | <code>ipv6 hop-limit hops</code>                                          |
| Enable or disable forwarding of IPv6 unicast datagrams. Disabled by default.                                                                                                             | <code>ipv6 unicast-routing</code><br><code>no ipv6 unicast-routing</code> |
| Display the status of IPv6 forwarding mode and unicast routing mode.                                                                                                                     | <code>show ipv6</code>                                                    |

The following example enables unicast routing mode, to allow the switch to route.

```
C5(su)->router
C5(su)->router>enable
C5su)->router#configure
Enter configuration commands:

C5(su)->router(Config)#ipv6 unicast-routing
```

## Configuring Routing Interfaces

### IPv6 Addressing

One or more global unicast IPv6 addresses and a single link-local address can be configured for an interface using the **ipv6 address** command in router interface configuration mode.

Link-local addresses are network addresses which are intended only for communications within one segment of a local network (a link) or a point-to-point connection. They allow addressing hosts without using a globally-routable address prefix. Routers will not forward packets with link-local addresses. A link local address must begin with **fe80:**.

A single link-local address is supported per interface. A link-local address is automatically generated when IPv6 routing is enabled on an interface.

When you manually configure a global IPv6 unicast address on an interface, you can enter the complete 128-bit address and prefix, or use the **eui64** parameter to configure a global IPv6 address using an EUI-64 identifier in the low order 64 bits of the address. When using the **eui64** parameter, you specify only the network prefix and length, and the Fixed Switch device generates the low order 64 bits.



**Note:** EUI-64 refers to the IEEE's 64-bit Extended Unique Identifier (EUI-64) format, as specified in RFC 2373.

## Enabling an Interface for IPv6 Routing

In addition to enabling an interface for routing, you must enable unicast routing on the switch with the **ipv6 unicast-routing** command in global router configuration mode.

To enable an interface, including VLAN, tunnel, and loopback interfaces, for IPv6 routing, in router interface configuration mode:

- Use the **ipv6 address** command to configure a global IPv6 address on an interface. This command also enables IPv6 processing on the interface and automatically generates a link-local address.
- Use the **ipv6 enable** command to enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address. This command also automatically generates a link-local address for the interface. The interface cannot route until it is assigned a global IPv6 unicast address.

Refer to “[Creating Tunnel Interfaces](#)” on page 25-7 for information about creating tunnel interfaces.

## Configuration Examples

[Procedure 25-2](#) describes the tasks and commands for configuring an IPv6 routing interface. Refer to the *CLI Reference* for your platform for more information about the commands listed below.

### Procedure 25-2 Configuring an IPv6 Routing Interface

| Step | Task                                                                                                                                                                                                                                                                                                         | Command(s)                                                                                             |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| 1.   | Optionally, in router interface configuration mode, enable an interface for IPv6 processing without assigning a global IPv6 address. A link-local IPv6 address is automatically configured on the interface.<br><br>Note that the interface cannot route until it is assigned a global IPv6 unicast address. | <b>ipv6 enable</b>                                                                                     |
| 2.   | Optionally, assign a global IPv6 address to an interface and enable the interface for IPv6 processing. A link-local IPv6 address is automatically configured on the interface.                                                                                                                               | <b>ipv6 address</b> { <i>ipv6-addr/prefix-length</i>   <i>ipv6-prefix/prefix-length eui64</i> }        |
| 3.   | Optionally, configure the maximum transmission unit (MTU) size of IPv6 packets that can be sent on the interface.                                                                                                                                                                                            | <b>ipv6 mtu</b> <i>bytes</i>                                                                           |
| 4.   | In router privileged execution mode, display information about one or all configured IPv6 interfaces.                                                                                                                                                                                                        | <b>show ipv6 interface</b> [ <i>vlan vlan-id</i>   <i>tunnel tunnel-id</i>   <i>loopback loop-id</i> ] |

The following code example assigns a global IPv6 address to VLAN 100, which also generates a link-local address and enables IPv6 processing. The `eui64` option is used to generate the lower 64 bits of the address. The interface’s configuration is then displayed.

```
C5(su)->router
C5(su)->router>enable
C5(su)->router#configure
Enter configuration commands:

C5(su)->router(Config)#ipv6 unicast-routing
C5(su)->router(Config)#interface vlan 100
C5(su)->router(Config-if(Vlan 100))#ipv6 address 3FFE:501:FFFF:101/64 eui64
C5(su)->router(Config-if(Vlan 100))#exit
```

```

C5(su)->router(Config)#show ipv6 interface vlan 100

Vlan 100 Administrative Mode Enabled
Vlan 100 IPv6 Routing Operational Mode Enabled
IPv6 is Enabled
IPv6 Prefix is FE80::211:88FF:FE55:4A7F/128
 3FFE:501:FFFF:101:211:88FF:FE55:4A7F/64

Routing Mode Enabled
Interface Maximum Transmit Unit 1500
Router Duplicate Address Detection Transmits 1
Router Advertisement NS Interval 0
Router Advertisement Lifetime Interval 1800
Router Advertisement Reachable Time 0
Router Advertisement Min Interval 200
Router Advertisement Max Interval 600
Router Advertisement Managed Config Flag Disabled
Router Advertisement Other Config Flag Disabled
Router Advertisement Suppress Flag Disabled

```

## Creating Tunnel Interfaces

IPv6 over IPv4 tunnels allow delivery of IPv6 packets over an IPv4 infrastructure. The IPv6 packets are encapsulated in IPv4 packets at one end of the tunnel and unencapsulated at the other end. Both endpoints of the tunnel must support both IPv4 and IPv6 protocol stacks.

The Enterasys Fixed Switches that support IPv6 allow you to manually configure an IPv6 over IPv4 point-to-point tunnel, specifying both the source and destination endpoints of the tunnel. The interfaces that are used as the endpoints of a tunnel must be configured with both an IPv4 address and an IPv6 address.

Before you create a tunnel interface with the commands shown in [Procedure 25-3](#), make sure that the interface that will be the source of the tunnel has been configured with an IPv4 address.

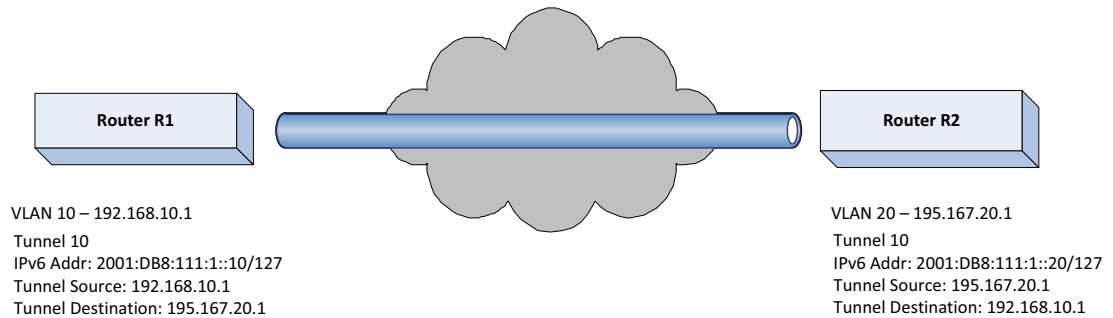
### Procedure 25-3 Creating Tunnel Interfaces

| Step | Task                                                                                                                                                           | Command(s)                                                                                             |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| 1.   | In global configuration mode, create the tunnel interface and enable tunnel interface configuration mode.                                                      | <b>interface tunnel</b> <i>tunnel-id</i>                                                               |
| 2.   | In router tunnel interface configuration mode, specify the IPv4 source transport address of the tunnel.<br><br>If the source is a VLAN, it must already exist. | <b>tunnel source</b> { <i>ipv4-addr</i>   <b>interface</b> <i>vlan vlan-id</i> }                       |
| 3.   | Specify the IPv4 destination transport address of the tunnel.                                                                                                  | <b>tunnel destination</b> <i>ipv4-addr</i>                                                             |
| 4.   | Specify the tunnel mode. Currently, only IPv6-over-IPv4 is supported.                                                                                          | <b>tunnel mode</b> <b>ipv6ip</b>                                                                       |
| 5.   | Configure an IPv6 address on the tunnel interface.                                                                                                             | <b>ipv6 address</b> { <i>ipv6-addr/prefix-length</i>   <i>ipv6-prefix/prefix-length</i> <b>eui64</b> } |
| 6.   | In router global configuration mode or privileged exec mode, display general information.                                                                      | <b>show ipv6 interface tunnel</b> <i>tunnel-id</i>                                                     |

[Figure 25-1](#) on page 25-8 illustrates a point-to-point IPv6 over IPv4 tunnel. The code example following the figure shows the commands used to configure the tunnel on both ends. Note that

the MTU value for the tunnel interfaces was reduced by 20 octets, to allow for the basic IPv4 headers added to IPv6 packets.

**Figure 25-1 Basic IPv6 Over IPv4 Tunnel**



### Router R1

```
R1(su)->router
R1(su)->router>enable
R1(su)->router#configure
Enter configuration commands:

R1(su)->router(Config)#interface vlan 10
R1(su)->router(Config-if(Vlan 10))#ip address 192.168.10.1 255.255.255.0
R1(su)->router(Config-if(Vlan 10))#no shutdown
R1(su)->router(Config-if(Vlan 10))#exit

R1(su)->router(Config)#interface tunnel 10
R1(su)->router(Config-if(Tnnl 101))#ipv6 address 2001:db8:111:1::10/127
R1(su)->router(Config-if(Tnnl 101))#tunnel source 192.168.10.1
R1(su)->router(Config-if(Tnnl 101))#tunnel destination 195.167.20.1
R1(su)->router(Config-if(Tnnl 101))#tunnel mode ipv6ip
R1(su)->router(Config-if(Tnnl 101))#exit

R1(su)->router(Config)#show ipv6 interface tunnel 10

Tunnel 10 Administrative Mode Enabled
Tunnel 10 IPv6 Routing Operational Mode Enabled
Mode for IPv6 Tunnel IPv6OVER4
Source Address for IPv6 Tunnel 192.168.10.1
Destination Address for IPv6 Tunnel 195.167.20.1
IPv6 is Enabled
IPv6 Prefix is FE80::A0C:102/128
 2001:db8:111:1::10/127

Routing Mode Enabled
Interface Maximum Transmit Unit 1480
Router Duplicate Address Detection Transmits 1
Router Advertisement NS Interval 0
Router Advertisement Lifetime 1800
Router Advertisement Reachable Time 0
Router Advertisement Min Interval 200
Router Advertisement Max Interval 600
Router Advertisement Managed Config Flag Disabled
Router Advertisement Other Config Flag Disabled
Router Advertisement Suppress Flag Disabled
```

## Router R2

```

R2(su)->router
R2(su)->router>enable
R2su)->router#configure
Enter configuration commands:

R2(su)->router(Config)#interface vlan 20
R2(su)->router(Config-if(Vlan 20))#ip address 195.167.20.1 255.255.255.0
R2(su)->router(Config-if(Vlan 20))#no shutdown
R2(su)->router(Config-if(Vlan 20))#exit

R2(su)->router(Config)#interface tunnel 10
R2(su)->router(Config-if(Tnnl 101))#ipv6 address 2001:db8:111:1::20/127
R2(su)->router(Config-if(Tnnl 101))#tunnel source 195.167.20.1
R2(su)->router(Config-if(Tnnl 101))#tunnel destination 192.168.10.1
R2(su)->router(Config-if(Tnnl 101))#tunnel mode ipv6ip
R2(su)->router(Config-if(Tnnl 101))#exit

R2(su)->router(Config)#show ipv6 interface tunnel 10

Tunnel 10 Administrative Mode Enabled
Tunnel 10 IPv6 Routing Operational Mode Disabled
Mode for IPv6 Tunnel IPv6OVER4
Source Address for IPv6 Tunnel 195.167.20.1
Destination Address for IPv6 Tunnel 192.168.10.1
IPv6 is Enabled
IPv6 Prefix is FE80::1111:22/128
 2001:db8:111:1::20/127

Routing Mode Enabled
Interface Maximum Transmit Unit 1480
Router Duplicate Address Detection Transmits 1
Router Advertisement NS Interval 0
Router Advertisement Lifetime 1800
Router Advertisement Reachable Time 0
Router Advertisement Min Interval 200
Router Advertisement Max Interval 600
Router Advertisement Managed Config Flag Disabled
Router Advertisement Other Config Flag Disabled
Router Advertisement Suppress Flag Disabled

```

## Configuring Static Routes

Static routes are used to define an explicit path between two network devices. Use the **ipv6 route** command to configure an IPv6 static route in router global configuration mode. You must specify the destination IPv6 prefix and length, and either the global IPv6 address of the next hop or the VLAN or tunnel output interface, and the link-local address of the next hop. Optionally, you can specify a preference value for the route.

[Procedure 25-4](#) on page 25-10 lists the commands used to configure IPv6 static routes. Refer to the *CLI Reference* for your platform for more information about the commands listed below.

**Procedure 25-4 Configuring Static Routers**

| Step | Task                                                                                                                     | Command(s)                                                                                                                                                                                                       |
|------|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | In global configuration mode, configure an IPv6 static route.                                                            | <b>ipv6 route</b> <i>ipv6-prefix/prefix-length</i> { <i>global-next-hop-addr</i>   <b>interface</b> { <b>tunnel</b> <i>tunnel-id</i>   <b>vlan</b> <i>vlan-id</i> } <i>ll-next-hop-addr</i> } [ <i>pref</i> ]    |
| 2.   | Optionally, configure a default distance, or preference, for static IPv6 routes that do not have a preference specified. | <b>ipv6 route distance</b> <i>pref</i>                                                                                                                                                                           |
| 3.   | Display the routing table, including static routes.                                                                      | <b>show ipv6 route</b> [{ <i>ipv6-addr</i> [ <i>route-type</i> ]   {{ <i>ipv6-prefix/prefix-length</i>   <b>interface</b> <i>interface</i> } [ <i>route-type</i> ]   <i>route-type</i>   <b>all</b> }]           |
| 4.   | Optionally, remove a static route.                                                                                       | <b>no ipv6 route</b> <i>ipv6-prefix/prefix-length</i> [ <i>global-next-hop-addr</i>   <b>interface</b> { <b>tunnel</b> <i>tunnel-id</i>   <b>vlan</b> <i>vlan-id</i> } <i>ll-next-hop-addr</i> ] [ <i>pref</i> ] |

This command creates a static IPv6 route to network 2001:0DB8:3333:6677::/64 by way of the next hop with global address 2003::211:88FF:FE56:5BD0.

```
C5(su)->router(Config)# ipv6 route 2001:0DB8:3333:6677::/64
2003::211:88FF:FE56:5BD0
```

The following example creates a static IPv6 route to network 2001:0DB8:2222:4455::/64 by way of VLAN 6, with the next hop link-local address of fe80::1234:5678:2dd:1, and gives the route a preference of 5.

```
C5(su)->router(Config)# ipv6 route 2001:0DB8:2222:4455::/64 interface vlan 6
fe80::1234:5678:2dd:1 5
```

## Viewing Routing Information

Table 25-4 lists the commands you can use to display IPv6 routing information and clear ipv6 statistics. Refer to the *CLI Reference* for your platform for more information about the commands listed below.

**Table 25-4 Displaying Routing Information**

| Task                                                                                                                                                         | Command                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display the IPv6 routing table                                                                                                                               | <b>show ipv6 route</b> [{ <i>ipv6-addr</i> [ <i>route-type</i> ]   {{ <i>ipv6-prefix/prefix-length</i>   <b>interface</b> <i>interface</i> } [ <i>route-type</i> ]   <i>route-type</i>   <b>all</b> }] |
| Display the preference value associated with types of routes                                                                                                 | <b>show ipv6 route preference</b>                                                                                                                                                                      |
| Display the summary of the routing table                                                                                                                     | <b>show ipv6 route summary</b> [ <b>all</b> ]                                                                                                                                                          |
| Show traffic and statistics for IPv6 and ICMPv6. Specify a logical, loopback, or tunnel interface to view information about traffic on a specific interface. | <b>show ipv6 traffic</b> [ <b>vlan</b> <i>vlan-id</i>   <b>tunnel</b> <i>tunnel-id</i>   <b>loopback</b> <i>loop-id</i> ]                                                                              |
| Clear IPv6 statistics for all interfaces or a specific interface                                                                                             | <b>clear ipv6 statistics</b> [ <b>vlan</b> <i>vlan-id</i>   <b>tunnel</b> <i>tunnel-id</i>   <b>loopback</b> <i>loop-id</i> ]                                                                          |



## Testing Network Connectivity

Use the **ping ipv6** command to determine whether another device is on the network. Use the **ping ipv6 interface** command to ping a link-local or global IPv6 address of an interface, specifying a loopback, tunnel, or logical interface as the source.

To use the **ping** commands, configure the switch for network (in-band) connection. Both source and target devices need to support ICMPv6 echo requests and echo responses. Fixed switch devices have ICMPv6 echo requests and echo responses enabled by default. (Note that most IP-capable devices support this feature for basic debugging.)

The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station.

Use the **tracert ipv6** command to trace the hop-by-hop route from the switch to the destination specified.

Refer to the *CLI Reference* for your platform for more information about the commands listed below.

**Table 25-5 Testing Network Connectivity**

| Task                                                                                                                          | Command                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Test routing network connectivity by sending IP ping requests to an IPv6 address.                                             | <b>ping ipv6</b> <i>ipv6-addr</i> [ <b>size</b> <i>num</i> ]                                                                                                                                                               |
| Test routing network connectivity, specifying the interface to be used as the source of the ping.                             | <b>ping ipv6 interface</b> { <b>vlan</b> <i>vlan-id</i>   <b>tunnel</b> <i>tunnel-id</i>   <b>loopback</b> <i>loop-id</i> } { <b>link-local-address</b> <i>ipv6-lladdr</i>   <i>ipv6-addr</i> } [ <b>size</b> <i>num</i> ] |
| Discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. | <b>tracert ipv6</b> <i>ipv6-addr</i>                                                                                                                                                                                       |

## IPv6 Neighbor Discovery

The Neighbor Discovery (ND) protocol for IPv6 is defined in RFC4861. The neighbor discovery protocol uses ICMPv6 messages to determine the link-layer addresses of nodes residing on the same local link, to locate neighboring routers, to learn certain link and address configuration information, and to track the reachability of neighbors.

### Duplicate Address Detection

IPv6 Duplicate Address Detection (DAD) is described in RFC 4862. DAD uses Neighbor Solicitation and Neighbor Advertisement messages to verify the uniqueness of an address. DAD must be performed on unicast addresses prior to assigning them to an interface. An address remains in a tentative state while DAD is being performed. If a tentative address is found to be a duplicate, an error message is returned and the address is not assigned to the interface.

Use the **ipv6 nd dad attempts** command to change the number of Neighbor Solicitation messages that can be sent for Duplicate Address Detection from the default value of 1. The **no** form of the command returns the value to the default of 1. A value of 0 disables Duplicate Address Detection on the interface.

The **show ipv6 interface** command displays the current DAD attempt setting.

## Neighbor Solicitation Messages

Neighbor Solicitation messages are sent on the local link to determine the link-local address of another node on the link, as well as to verify the uniqueness of a unicast address for DAD. Neighbor Solicitation messages are also used to verify the reachability of a neighbor after the link-local address is known.

Use the **ipv6 nd ns-interval** command to configure the interval between Neighbor Solicitation messages sent on an interface.

Use the **ipv6 nd reachable-time** to configure the length of time within which some reachability confirmation must be received from a neighbor for the neighbor to be considered reachable.

## Router Advertisements

Router Advertisement (RA) messages are periodically sent out each IPv6-configured interface on the router. The messages are sent to the all-nodes multicast address. RA messages are also sent in response to router solicitation message from hosts.

RAs typically include the following information:

- The amount of time, in seconds, that this router should be used as a default router.
- A list of prefixes used for on-link determination and/or autonomous address configuration. Flags associated with the prefixes specify the intended uses of a particular prefix. Hosts use the advertised on-link prefixes to build and maintain a list that is used in deciding when a packet's destination is on-link or beyond a router. Hosts can use the advertised autoconfiguration prefixes to perform autonomous (stateless) address configuration, if stateless configuration is allowed.
- The "other stateful configuration" flag. When the flag is true, end nodes should use stateful autoconfiguration (DHCPv6) to obtain additional information (excluding addresses). When the value is false, end nodes do not. Refer to RFC 4862, "IPv6 Stateless Address Autoconfiguration," for more information.
- The length of time within which some reachability confirmation must be received from a neighbor for the neighbor to be considered reachable.

You can configure the following RA parameters:

- Whether router advertisements should be transmitted on the interface.
- The time interval between RA transmissions.
- The router lifetime value, which indicates the length of time the router can be used as a default router. You can also specify that the router should not be used as a default router.
- The value of the "other stateful configuration" flag.
- The list of prefixes for on-link determination and/or autonomous address configuration.
- The amount of time a node considers a neighbor reachable.

## Cache Management

Use the **show ipv6 neighbors** command to display the IPv6 Neighbor Cache.

Use the **clear ipv6 neighbors** command to clear all the dynamically learned entries in the cache, or an entry on a specific interface.

## Neighbor Discovery Configuration

Refer to [Table 25-2](#) on page 25-4 for the default Neighbor Discovery values.

[Procedure 25-5](#) on page 25-13 lists the tasks and commands to configure Neighbor Discovery on routing interfaces. Refer to the *CLI Reference* for your platform for more information about the commands listed below.

### Procedure 25-5 Neighbor Discovery Configuration

| Step | Task                                                                                                                                                                                                                                                            | Command(s)                                                                                                                                       |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | In router interface configuration mode, optionally configure the number of DAD attempts that should be made when configuring IPv6 unicast addresses.<br><br>A value of 0 disables DAD on the interface.                                                         | <code>ipv6 nd dad attempts number</code>                                                                                                         |
| 2.   | Optionally, configure the interval between Neighbor Solicitations sent on the interface.<br><br>A value of 0 means the interval is unspecified.                                                                                                                 | <code>ipv6 nd ns-interval {msec   0}</code>                                                                                                      |
| 3.   | Optionally, configure the amount of time that a remote IPv6 node is considered reachable.<br><br>A value of 0 means that the time is unspecified.                                                                                                               | <code>ipv6 nd reachable-time msec</code>                                                                                                         |
| 4.   | Optionally, set the “other stateful configuration” flag to true, which indicates to end nodes that they should use stateful autoconfiguration (DHCPv6) to obtain additional information.<br><br>Use the <b>no</b> form of the command to set the flag to false. | <code>ipv6 nd other-config-flag</code>                                                                                                           |
| 5.   | Optionally, change the transmission interval between router advertisements.                                                                                                                                                                                     | <code>ipv6 nd ra-interval sec</code>                                                                                                             |
| 6.   | Optionally, change the router lifetime value sent in RAs by this interface.<br><br>A value of 0 indicates that this router should not be used as a default router.                                                                                              | <code>ipv6 nd ra-lifetime sec   0</code>                                                                                                         |
| 7.   | Optionally, suppress the sending of Router Advertisements on this interface. RAs are sent by default.                                                                                                                                                           | <code>ipv6 nd suppress-ra</code>                                                                                                                 |
| 8.   | Optionally, configure the IPv6 prefixes to be included in RAs sent by this interface.                                                                                                                                                                           | <code>ipv6 nd prefix {ipv6-prefix/prefix-length} [{valid-lifetime   infinite} {preferred-lifetime   infinite}] [no-autoconfig] [off-link]</code> |
| 9.   | In router privileged execution or global configuration mode, display the Neighbor Discovery configuration for this interface.                                                                                                                                   | <code>show ipv6 interface [vlan vlan-id   tunnel tunnel-id   loopback loop-id]</code>                                                            |
| 10.  | In router privileged execution mode, display the contents of the Neighbor Cache.                                                                                                                                                                                | <code>show ipv6 neighbors</code>                                                                                                                 |
| 11.  | In router privileged execution mode, clear the contents of the Neighbor Cache.                                                                                                                                                                                  | <code>clear ipv6 neighbors</code>                                                                                                                |

## DHCPv6 Configuration

DHCP is generally used between clients (for example, hosts) and servers (for example, routers) for the purpose of assigning IP addresses, gateways, and other networking definitions such as DNS, NTP, and/or SIP parameters. However, IPv6 natively provides for auto-configuration of IP addresses through the IPv6 Neighbor Discovery Protocol (NDP) and the use of Router Advertisement messages. Thus, the role of DHCPv6 within the network is different from DHCPv4 in that it is less relied upon for IP address assignment.

DHCPv6 server and client interactions are described by RFC 3315. There are many similarities between DHCPv6 and DHCPv4 interactions and options, but the messages and option definitions are sufficiently different. There is no migration or inter-operability from DHCPv4 to DHCPv6.

DHCPv6 incorporates the notion of the stateless server, where DHCPv6 is not used for IP address assignment to a client. Instead, it only provides other networking information such as DNS, NTP, and/or SIP information. The stateless server behavior is described by RFC 3736, which simply contains descriptions of the portions of RFC 3315 that are necessary for stateless server behavior.

In order for a router to drive a DHCPv6 client to utilize stateless DHCPv6, the “other stateful configuration” option must be configured for neighbor discovery on the corresponding IPv6 router interface. This in turn causes DHCPv6 clients to send the DHCPv6 “Information Request” message in response. A DHCPv6 server then responds by providing only networking definitions such as DNS domain name and server definitions, NTP server definitions, and/or SIP definitions.

RFC 3315 also describes DHCPv6 Relay Agent interactions, which are very much like DHCPv4 Relay Agent. RFC 3046 describes the DHCPv6 Relay Agent Information Option, which employs very similar capabilities as those described by DHCPv4 Relay Agent Option in RFC 2132.

With the larger address space inherent to IPv6, addresses within a network can be allocated more effectively in a hierarchical fashion. DHCPv6 introduces the notion of “prefix delegation” as described in RFC 3633 as a way for routers to centralize and delegate IP address assignment.

The Fixed Switches allow you to configure an interface on the switch as either a DHCPv6 server or a DHCPv6 relay agent, but not both.

## DHCPv6 Relay Agent Configuration

The DHCPv6 relay application provides a means for relaying DHCPv6 requests between a subnet to which no DHCP server is connected to other subnets on which servers are attached. The application allows the definition of servers on a per interface basis.

The DHCP Solicit message is a multicast message to the all DHCP server address (ff02::1:2). The all DHCP server address only crosses network segments when explicitly routed. If your network has multiple segments, you must configure a DHCP relay agent on the router interface for each segment, so that all DHCP solicit messages can be forwarded to your DHCP server.

In global router configuration mode, you can configure two options:

- The DHCPv6 Relay Agent Information Option allows for various sub-options to be attached to messages that are being relayed by the local router to a relay server. The relay server may in turn use this information in determining an address to assign to a DHCPv6 client. Refer to RFC 3046 for more information.
- The DHCPv6 Relay Agent Remote-ID sub-option may be added by DHCP relay agents which terminate switched or permanent circuits and have mechanisms to identify the remote host end of the circuit. Refer to RFC 3046 for more information.

Use the **ipv6 dhcp relay** command at router interface configuration mode to configure an interface as a DHCPv6 relay agent. You can specify the IPv6 address of the DHCPv6 server as a global

address, a multicast address, or a link-local address. If the address is a multicast or link-local address, then you must also specify the interface to be used to contact the DHCPv6 server.

Alternatively, you can specify only the interface to be used to contact the DHCPv6 server and the Fixed Switch device will use the DHCPV6-ALL-AGENTS multicast address (FF02::1:2) to relay DHCPv6 messages to the DHCPv6 server.

The **show ipv6 dhcp interface** command, in router privileged execution mode, will display how an interface has been configured.

## DHCPv6 Server Configuration

DHCPv6 server configuration consists of creating pools containing stateless and/or prefix delegation parameters that should be used by the DHCPv6 server, then configuring an interface as a DHCPv6 server and assigning the pools to be used.

### Pool Configuration

DHCPv6 pools are used to specify information for the DHCPv6 server to distribute to DHCPv6 clients. These pools are shared between multiple interfaces over which DHCPv6 server capabilities are configured.

After executing the **ipv6 dhcp pool** command in global router configuration mode, and entering pool configuration mode, you can configure the following pool parameters:

- The DNS domain name for the pool which is provided to DHCPv6 clients by the DHCPv6 server. A DNS domain name is configured for stateless server support. A DHCPv6 pool can have up to 8 domain names configured for it.
- The IPv6 DNS server address which is provided to DHCPv6 clients by the DHCPv6 server. A DNS server address is configured for stateless server support. A DHCPv6 pool can have up to 8 DNS server addresses configured for it.
- An IPv6 address prefix to be delegated to a specific prefix delegation client, identified by their DHCP unique identifier. Refer to RFC 3633, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6," for more information about prefix delegation. Refer to RFC 3315 for information about the DHCP Unique Identifier (DUID) of the prefix delegation client.

### Server Configuration

After configuring the pools, you can configure DHCPv6 server functionality on an interface with the **ipv6 dhcp server** command in interface configuration mode. You can specify:

- The pool to be used, by name.
- Whether the server should use the Rapid Commit option that allows for an abbreviated exchange between DHCPv6 client and server. Refer to RFC 3315 for more information.
- The server's preference value, which is used by clients to determine preference among multiple servers.

## Default Conditions

The following table lists the default DHCPv6 conditions.

| Condition                                              | Default Value   |
|--------------------------------------------------------|-----------------|
| IPv6 DHCP                                              | Disabled        |
| IPv6 DHCP Relay Agent Information Option               | 32              |
| IPv6 DHCP Relay Agent Information Remote ID Sub-option | 1               |
| IPv6 DHCP Preferred Lifetime                           | 2592000 seconds |
| IPv6 DHCP Valid Lifetime                               | 604800 seconds  |

## Configuration Examples

[Procedure 25-6](#) describes the tasks to configure a Fixed Switch interface as a DHCPv6 relay agent. A code example follows the procedure. Refer to the *CLI Reference* for your platform for more information about these commands.

### Procedure 25-6 DHCPv6 Relay Agent Configuration

| Step | Task                                                                                                                                                                                                                                                    | Command(s)                                                                                                                                   |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | In router global configuration mode, enable DHCPv6.                                                                                                                                                                                                     | <code>ipv6 dhcp enable</code>                                                                                                                |
| 2.   | Optionally, configure Relay Agent Information Option parameters/                                                                                                                                                                                        | <code>ipv6 dhcp relay-agent-info-opt option</code><br><code>ipv6 dhcp relay-agent-info-remote-id-subopt option</code>                        |
| 3.   | In interface configuration mode, configure an interface for DHCPv6 relay agent functionality. You can specify the DHCPv6 server destination address or the interface on which to send the relay messages using the DHCPV6-ALL-AGENTS multicast address. | <code>ipv6 dhcp relay {destination dest-addr [interface intf]   interface vlan vlan-id} [remote-id {duid-uuid   user-defined-string}]</code> |
| 4.   | In router global configuration mode, display an interface's DHCP configuration.                                                                                                                                                                         | <code>show ipv6 dhcp interface vlan vlan-id</code>                                                                                           |

```
C5(su)->router
C5(su)->router>enable
C5(su)->router#configure
Enter configuration commands:

C5(su)->router(Config)#ipv6 dhcp enable
C5(su)->router(Config)#interface vlan 200
C5(su)->router(Config-if(Vlan 200))#ipv6 dhcp relay destination
2001:db8:1111:2222::10
C5(su)->router(Config-if(Vlan 200))#exit

C5(su)->router(Config)#show ipv6 dhcp interface vlan 200
IPv6 Interface Vlan 200
Mode Relay
Relay Address 2001:DB8:1111:2222::10
Relay Interface Number
```

Relay Remote ID  
Option Flags

[Procedure 25-7](#) on page 25-17 describes the tasks to configure a Fixed Switch interface as a DHCPv6 server. A code example follows the procedure. Refer to the *CLI Reference* for your platform for more information about these commands.

### Procedure 25-7 DHCPv6 Server Configuration

| Step | Task                                                                                                                                                                                                   | Command(s)                                                                                                                                         |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | In router global configuration mode, enable DHCPv6.                                                                                                                                                    | <code>ipv6 dhcp enable</code>                                                                                                                      |
| 2.   | Create a DHCPv6 pool and enter pool configuration mode for that pool.                                                                                                                                  | <code>ipv6 dhcp pool pool-name</code>                                                                                                              |
| 3.   | Optionally, configure the domain name for the DHCPv6 client.                                                                                                                                           | <code>domain-name name</code>                                                                                                                      |
| 4.   | Optionally, configure the DNS servers for the DHCPv6 client. A pool can have up to 8 DNS servers configured for it.                                                                                    | <code>dns-server server-address</code>                                                                                                             |
| 5.   | Optionally, configure a numeric prefix to be delegated to a specified prefix delegation client.<br><b>Note:</b> To see the DUID of a Fixed Switch device, use the <code>show ipv6 dhcp</code> command. | <code>prefix-delegation prefix/prefix-length DUID [name hostname] [valid-lifetime {secs   infinite}] [preferred-lifetime {secs   infinite}]</code> |
| 6.   | Exit pool configuration mode.                                                                                                                                                                          | <code>exit</code>                                                                                                                                  |
| 7.   | In router global configuration mode, display the pool.                                                                                                                                                 | <code>show ipv6 dhcp pool pool-name</code>                                                                                                         |
| 8.   | In interface configuration mode, configure an interface for DHCPv6 server functionality.                                                                                                               | <code>ipv6 dhcp server pool-name [rapid-commit] [preference pref]</code>                                                                           |
| 9.   | In router global configuration mode, display the interface configuration.                                                                                                                              | <code>show ipv6 dhcp interface vlan vlan-id [statistics]</code>                                                                                    |

The following code example creates a DHCPv6 pool named “pool22” and configures the pool with a DNS server address, a domain name, and two prefixes that can be delegated to the DHCPv6 client identified by the DUID 00:01:00:06:99:a3:ff:11:22:33:44:55:66:77. The example then displays the pool. Interface VLAN 200 is then configured as a DHCPv6 server with pool22 assigned to it, and the interface is displayed.

```
C5(su)->router
C5(su)->router>enable
C5(su)->router#configure
Enter configuration commands:

C5(su)->router(Config)#ipv6 dhcp enable
C5(su)->router(Config)#ipv6 dhcp pool pool22

C5(su)->router(Config-dhcp6s-pool)#dns-server 2001:db8:222:111::10
C5(su)->router(Config-dhcp6s-pool)#domain-name enterasys.com
C5(su)->router(Config-dhcp6s-pool)#prefix-delegation 3001:2222::/48
00:01:00:06:99:a3:ff:11:22:33:44:55:66:77
C5(su)->router(Config-dhcp6s-pool)#prefix-delegation 3001:3333::/48
00:01:00:06:99:a3:ff:11:22:33:44:55:66:77
C5(su)->router(Config-dhcp6s-pool)#exit

C5(rsu)->router(Config)#show ipv6 dhcp pool pool22
```



```
DHCPv6 Pool: pool22
```

```
Static Bindings:
```

```
Binding for Client 00:01:00:06:99:a3:ff:11:22:33:44:55:66:77
IA PD: IA ID not specified,
Prefix: 3001:2222::/48
Preferred Lifetime infinite, Valid Lifetime infinite
```

```
Static Bindings:
```

```
Binding for Client 00:01:00:06:99:a3:ff:11:22:33:44:55:66:77
IA PD: IA ID not specified,
Prefix: 3001:3333::/48
Preferred Lifetime infinite, Valid Lifetime infinite
```

```
DNS Server: 2001:DB8:222:111::10
DNS Server: 2001:DB8:4444:5555::20
Domain Name: enterasys.com
```

```
C5(su)->router(Config)#interface vlan 200
C5(su)->router(Config-if(Vlan 200))#ipv6 dhcp server pool22
C5(su)->router(Config-if(Vlan 200))#exit
```

```
C5(su)->router(Config)#show ipv6 dhcp interface vlan 200
IPv6 Interface Vlan 200
Mode Server
Pool Name pool22
Server Preference 20
Option Flags
```

## Viewing DHCPv6 Statistics

[Table 25-6](#) lists the commands you can use to display DHCPv6 statistics and status. Refer to the *CLI Reference* for your platform for more information about the output of these commands.

**Table 25-6 Displaying DHCPv6 Statistics**

| Task                                                                                      | Command                                                                                                            |
|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Display statistics for one interface or for all interfaces.                               | <code>show ipv6 dhcp interface vlan <i>vlan-id</i> statistics</code><br><br><code>show ipv6 dhcp statistics</code> |
| Clear statistics for one interface or all interfaces.                                     | <code>clear ipv6 dhcp statistics [<i>vlan</i> <i>vlan-id</i>]</code>                                               |
| Display binding information about one or all DHCP prefix delegation clients.              | <code>show ipv6 dhcp binding [<i>ipv6-addr</i>]</code>                                                             |
| Display the state of DHCPv6 on the switch and the switch's DHCP unique identifier (DUID). | <code>show ipv6 dhcp</code>                                                                                        |



## Configuring Security Features

This chapter describes the following security features and how to configure them on the Fixed Switch platforms.

| For information about...                         | Refer to page... |
|--------------------------------------------------|------------------|
| <a href="#">Security Mode Configuration</a>      | 26-1             |
| <a href="#">IPsec Configuration</a>              | 26-4             |
| <a href="#">RADIUS Management Authentication</a> | 26-6             |
| <a href="#">MAC Locking</a>                      | 26-7             |
| <a href="#">TACACS+</a>                          | 26-11            |
| <a href="#">Service ACLs</a>                     | 26-16            |
| <a href="#">DHCP Snooping</a>                    | 26-18            |
| <a href="#">Dynamic ARP Inspection</a>           | 26-22            |

### Security Mode Configuration

| For information about...                                            | Refer to page... |
|---------------------------------------------------------------------|------------------|
| <a href="#">About the Security Mode</a>                             | 26-1             |
| <a href="#">Security Mode and SNMP</a>                              | 26-2             |
| <a href="#">Security Mode and User Authentication and Passwords</a> | 26-3             |
| <a href="#">Security Mode and System Logging</a>                    | 26-3             |
| <a href="#">Security Mode and File Management</a>                   | 26-4             |

### About the Security Mode

The security mode of a Fixed Switch determines how the switch performs all cryptographic functions. The security mode is set with the **set security profile** command. Currently, the modes supported are:

- Normal, when all supported cryptographic algorithms are available to be selected and used.
- Federal Information Processing Standard (FIPS) 140-2 mode, when the switch adheres to the FIPS 140-2 Security Requirements for Cryptographic Modules. In this mode, all cryptographic functions are performed by the FIPs Cryptographic Module, including SSH, SSL, SNMPv3, and password encryption. Optional selection of non-FIPS approved algorithms will fail.

FIPS mode is disabled by default. It can be enabled using the **set security profile c2** command. FIPS mode is persistent and shown in the running configuration. When changing between Normal and FIPS mode, a system reboot is required, indicated by a warning message:

```
Warning: Changing the security profile requires system reset.
Do you want to continue (y/n) [n]?
```

FIPS mode can be cleared using the **clear security profile** command.

When FIPS mode (security profile = c2) is enabled, FIPS cryptographic module initialization is invoked as per Section 2.3 of the OpenSSL FIPS 140-2 Security Policy.

## Configuring the Security Mode

[Procedure 26-1](#) on page 26-2 lists the commands to configure the security mode of the switch. Refer to the *CLI Reference* for your platform for details of the commands listed.

### Procedure 26-1 Configuring the Security Mode

| Step | Task                                                                                                                              | Command(s)                                |
|------|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| 1.   | Display the current security mode setting.                                                                                        | <b>show security profile</b>              |
| 2.   | If necessary, change the security mode.<br>When prompted for a system reboot, enter y.                                            | <b>set security profile {c2   normal}</b> |
| 3.   | If desired, return the switch to the default state of FIPS mode disabled (normal).<br>When prompted for a system reboot, enter y. | <b>clear security profile</b>             |

## Security Mode and SNMP

When FIPS mode (security profile = c2) is enabled, the default authentication mechanism for SNMPv3 is HMAC-SHA-1. The entire SNMPv3 message will be checked for integrity using HMAC-SHA-1. The authentication option of the **set snmp user** command will not accept MD5 as an option. Only the FIPS cryptographic module will be used for HMAC-SHA-1 even if this same algorithm is provided by other functions.

When FIPS mode (security profile = c2) is enabled, the encryption mechanism for SNMPv3 will be AES-128. The encryption option of the **set snmp user** command will not accept DES as an option while in FIPS mode. Only the FIPS cryptographic module will be used for AES-128 even if this same algorithm is provided by other functions.

[Table 26-1](#) lists the SNMP commands that require different user access permissions when the security mode is set to C2.

**Table 26-1 SNMP Commands Affected by Security Mode Settings**

| Commands                                 | Access When Security Mode Setting Is: |            |
|------------------------------------------|---------------------------------------|------------|
|                                          | Normal                                | C2         |
| <code>set/clear snmp user</code>         | Read-Write                            | Super User |
| <code>set/clear snmp group</code>        | Read-Write                            | Super User |
| <code>set/clear snmp community</code>    | Read-Write                            | Super User |
| <code>set/clear snmp access</code>       | Read-Write                            | Super User |
| <code>set/clear snmp view</code>         | Read-Write                            | Super User |
| <code>set/clear snmp targetparams</code> | Read-Write                            | Super User |

**Table 26-1 SNMP Commands Affected by Security Mode Settings (continued)**

| Commands                     | Access When Security Mode Setting Is: |            |
|------------------------------|---------------------------------------|------------|
|                              | Normal                                | C2         |
| set/clear snmp targetaddr    | Read-Write                            | Super User |
| set/clear snmp notify        | Read-Write                            | Super User |
| set/clear snmp notifyfilter  | Read-Write                            | Super User |
| set/clear snmp notifyprofile | Read-Write                            | Super User |

## Security Mode and User Authentication and Passwords

The switch ensures that passwords are safeguarded during transit and while in storage using FIPS 140-2 commercial encryption provided by the FIPS module.

Password feature behavior and defaults differ depending on the security mode of the switch. The default values for user account and password parameters are listed in the following table by the security mode of the switch.

**Table 26-2 User Account and Password Parameter Defaults by Security Mode**

| Parameter                                              | Normal Mode Default      | C2 Mode Default         |
|--------------------------------------------------------|--------------------------|-------------------------|
| Password history                                       | 0 (no history)           | 8 previous passwords    |
| Password change frequency                              | 0 (no waiting)           | 1440 minutes (24 hours) |
| Minimum number of characters in password               | 8                        | 9                       |
| Allow consecutively repeating characters in password   | yes                      | 2 characters            |
| Aging of system passwords                              | disabled                 | 90 days                 |
| Password required at time of new user account creation | no                       | yes                     |
| Substring matching at password validation              | 0 (no checking)          | 0 (no checking)         |
| New users required to change password at first log in  | no                       | yes                     |
| Lockout based on inactivity                            | 0 (no activity checking) | 90 days of inactivity   |
| Lockout based on failed login attempts                 | 3 failed attempts        | 3 failed attempts       |
| Lockout period duration after unsuccessful log ins     | 15 minutes               | 1 minute                |
| Grace period after password expiration                 | 0                        | 30 days                 |
| Grace login limit                                      | 0                        | 3                       |
| Warning period                                         | 20 days                  | 20 days                 |

Refer to [Chapter 5, User Account and Password Management](#) for more information about creating and managing user accounts and passwords.

## Security Mode and System Logging

Security audit logging provides a mechanism to generate a separate and secure log file, in addition to the previously existing unsecured log file ("current.log"). Refer to "[About Security Audit Logging](#)" on page 14-6 for information about the secure permanent log file (secure.log) and

how to enable security audit logging. Refer to [Chapter 14, Configuring Syslog](#) for more information about system logging in general.

[Table 26-3](#) lists the logging commands that require different user access permissions when the security mode is set to C2.

**Table 26-3 Logging Commands Affected by Security Mode Settings**

| Commands                      | Access When Security Mode Setting Is: |            |
|-------------------------------|---------------------------------------|------------|
|                               | Normal                                | C2         |
| set/clear logging server      | Read-Write                            | Super User |
| set/clear logging default     | Read-Write                            | Super User |
| set/clear logging application | Read-Write                            | Super User |
| set/clear logging local       | Read-Write                            | Super User |
| show logging buffer           | Read-Only                             | Super User |

## Security Mode and File Management

The “secure.log” file is stored in the **secure/logs** directory. This directory is only visible to and accessible by super user accounts. Super-users can create, edit, and delete files in the secure directory, and can copy files to and from the secure directory.

The secure.log file stored in the **secure/logs** directory cannot be deleted, edited, or renamed. Super-users can copy the secure.log file using SCP, SFTP, or TFTP.

[Table 26-4](#) on page 26-4 describes the security mode implications for the **show config**, and **configure** commands.

**Table 26-4 File Management Commands Affected by Security Mode Settings**

| Commands    | Command Behavior When Security Mode Setting Is:                   |                                                                                                                                                                                                        |
|-------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | Normal                                                            | C2                                                                                                                                                                                                     |
| show config | Output of command obfuscates user passwords for all access modes. | For Read-Only and Read-Write users, user passwords are redacted entirely. The line containing the password is also commented out in the output.<br><br>For Super Users, user passwords are obfuscated. |
| configure   | Command is available for Read-Write user access.                  | Command is available only for Super User access                                                                                                                                                        |

## IPsec Configuration

### About IPsec

The Security Architecture for IP (IPsec), defined in RFC 4301, describes how to provide a set of security services for traffic at the IP layer in both IPv4 and IPv6 environments. As described in the RFC, most of the security services are provided through use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols.

The current IPsec implementation on the Fixed Switches provides the following functionality:

- IPsec and IKE (Internet Key Exchange protocol) are defined for the RADIUS host application only. This implementation supports the creation of Security Associations (SAs) with servers configured for RADIUS, and the RADIUS application helps define the IPsec flow.
- Only the Encapsulating Security Payload (ESP) mode of operation is supported. Authentication Header (AH) mode is not supported.
- Currently, IKEv1 is supported, and the RADIUS shared secret is used as the IKE pre-shared key.



**Note:** Although the use of certificates will be supported for IPsec in future releases, in the current release only use of a shared secret is supported.

- HMAC-SHA1 is the default IKE integrity mechanism.
- 3DES and the Advanced Encryption Standard (AES) encryption algorithms are supported. AES supports key lengths of 128, 192, and 256 bits. The default IPsec encryption algorithm is AES-128.
- IPsec does not prevent the independent simultaneous use of MSCHAP-V2 style encryption of user passwords between the switch and the RADIUS server.

## IPsec Defaults

**Table 26-5 IPsec Defaults**

| Parameter                             | Default            |
|---------------------------------------|--------------------|
| IPsec status for RADIUS transactions  | Disabled           |
| Authentication protocol               | HMAC-SHA1          |
| Encryption method                     | AES128             |
| IKE Diffie-Hellman key exchange group | Group-1 (768 bits) |
| IKE lifetime main mode interval       | 60 minutes         |
| IKE lifetime quick mode interval      | 5 minutes          |
| IKE lifetime bandwidth                | 100000 bytes       |
| IKE protocol                          | Main               |
| Authentication method                 | Secret             |

## IPsec Configuration

[Procedure 26-2](#) lists the commands to configure IPsec parameters and enable or disable IPsec on one or all RADIUS servers. The **set** and **clear** commands listed below require super user access rights if the security mode setting is C2. Refer to the *CLI Reference* for your platform for details about using the commands listed.

**Procedure 26-2 Configuring IPsec**

| Step | Task                                                                                                                              | Command(s)                                                                                 |
|------|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 1.   | Display the current IPsec settings.                                                                                               | <code>show ipsec</code>                                                                    |
| 2.   | Optionally, change the authentication protocol.<br><b>Note:</b> This command is not available if the security mode setting is C2. | <code>set ipsec authentication {md5   sha1}</code>                                         |
| 3.   | Optionally, change the encryption type.                                                                                           | <code>set ipsec encryption {3des   aes128   aes192   aes256}</code>                        |
| 4.   | Optionally, change the IKE Diffie-Hellman key exchange group                                                                      | <code>set ipsec ike dh-group {group-1   group-2   group-5   group-14}</code>               |
| 5.   | Optionally, change the IKE timeout intervals.                                                                                     | <code>set ipsec ike lifetime {[bandwidth bytes]   [main minutes]   [quick minutes]}</code> |
| 6.   | Enable IPsec on one or all RADIUS servers.                                                                                        | <code>set radius ipsec enable [index]</code>                                               |
| 7.   | Optionally, use one of these commands to disable IPsec on one or all RADIUS servers.                                              | <code>set radius ipsec disable [index]</code><br><code>clear radius ipsec [index]</code>   |

## RADIUS Management Authentication

MS-CHAP is the Microsoft version of the Challenge-Handshake Authentication Protocol (CHAP). MS-CHAPv2 is defined in RFC 2759.

When you enable MS-CHAPv2 management authentication with the `set radius attribute mgmt password mschapv2` command, the following features are supported:

- MS-CHAPv2 style encryption of user passwords between the switch and RADIUS server.
- Support for the following MS-CHAPv2 RADIUS attributes:
  - MS-CHAP2-Response
  - MS-CHAP2-Success
- Support for MS-CHAPv2 password changing, which requires support of these attributes:
  - MS-CHAP2-CPW
  - MS-CHAP-Error
  - MS-CHAP-NT-Enc-PW

### Request Transmission

If the `mschapv2` option has been configured, the RADIUS client software will take the clear text user password indicated by the management session and use it to properly fill the MS-CHAP2-Response RADIUS attribute, following the guidelines set forth in both RFC2548 and RFC2759.

In short, the attribute is filled with both a randomly generated challenge as well as the appropriate MS-CHAPv2 response calculated using the challenge and the passed clear text password. No User-Password RADIUS attribute will be passed in this case.

## Response Validation

When the MS-CHAP2-Success attribute is received in an access accept RADIUS response frame, it will be validated according to RFC2548 and RFC2759. This attribute contains the 42 byte authenticator response. Upon receipt, the RADIUS client software will calculate its own authenticator response using the information that was passed in the MS-CHAP2-Response attribute and the user's passed clear text password.

If the value calculated does not match the value in the attribute, it will be assumed that the message is not from the RADIUS server and the response message will be dropped. A log message will be output that indicates this condition has occurred.

## Password Changing

If an Access Reject packet is received from the RADIUS server and it includes an MS-CHAP-Error attribute that indicates that the user's password has expired, the switch will prompt the user for a new password. If the user appropriately enters a new password, then that password will be sent to the RADIUS server via the MS-CHAPv2 password change RADIUS attributes.

If the server responds with an Access Accept, then the user will be allowed access and the password has been successfully changed. If an Access Reject is sent from the server, then the password has not been changed and the user will be denied access.

## Example

This example changes the RADIUS management authentication mode to MS-CHAPv2, then displays the RADIUS configuration.

```
A4(su)->set radius attribute mgmt password mschapv2
A4(su)->show radius
RADIUS status: Disabled
RADIUS retries: 2
RADIUS timeout: 5 seconds
RADIUS attribute mgmt password: mschapv2
RADIUS Server IP Address Auth-Port Realm-Type IPsec

1 10.1.0.27 1812 any disabled
2 192.168.10.10 1812 any enabled
```

Note that although **standard** is the factory default mode, once you change the mode to MS-CHAPv2, you must execute the **set radius attribute mgmt password standard** command to change the mode back to standard RADIUS management authentication.

## MAC Locking

This feature locks a MAC address to one or more ports, preventing connection of unauthorized devices through the port(s). When source MAC addresses are received on specified ports, the switch discards all subsequent frames not containing the configured source addresses. The only frames forwarded on a "locked" port are those with the "locked" MAC address(es) for that port.

There are two methods of locking a MAC to a port: first arrival and static. The first arrival method is defined to be locking the first *n* number of MACs which arrive on a port configured with MAC locking enabled. The value *n* is configured with the **set maclock firstarrival** command.

The static method is defined to be statically provisioning a MAC-port lock using the **set maclock static** command. The maximum number of static MAC addresses allowed for MAC locking on a port is 20 MAC addresses.

You can configure the switch to issue a violation trap if a packet arrives with a source MAC address different from any of the currently locked MAC addresses for that port.

MACs are unlocked as a result of:

- A link down event
- When MAC locking is disabled on a port
- When a MAC is aged out of the forwarding database when FirstArrival aging is enabled

When properly configured, MAC locking is an excellent security tool as it prevents MAC spoofing on configured ports. Also if a MAC were to be secured by something like Dragon Dynamic Intrusion Detection, MAC locking would make it more difficult for a hacker to send packets into the network because the hacker would have to change their MAC address and move to another port. In the meantime the system administrator would be receiving a maclock trap notification.

MAC locking is disabled by default at device startup. Configuring one or more ports for MAC locking requires globally enabling it on the device and then enabling it on the desired ports.

## First Arrival Configuration

Use the **set maclock firstarrival** command to restrict MAC locking on a port to a maximum number of end station addresses first connected to that port (dynamic MAC locking).

By default, the maclock first arrival count resets when the link goes down and dynamic MAC locking addresses are dropped on loss of link. This feature is beneficial if you have roaming users—the first arrival count will be reset every time a user moves to another port, but will still protect against connecting multiple devices on a single port and will protect against MAC address spoofing.



**Note:** Setting a port's first arrival limit to 0 does not deny the first MAC address learned on the port from passing traffic.

Use the **set maclock agefirstarrival** command to enable or disable the aging of first arrival MAC addresses. When enabled, first arrival MAC addresses that are aged out of the forwarding database will be removed from the associated port MAC lock.

Use the **set maclock clearonlinkchange** command to manage the behavior of First Arrival MAC locking with link state change. By default, dynamic MAC locking addresses are dropped on loss of link. If you disable clearing of First Arrival MAC locking, First Arrival MAC addresses will be maintained on a loss of link.

Use the **set maclock move** command to move all current first arrival MACs to static entries. If there are more first arrival MACs than the allowed maximum static MACs, then only the latest first arrival MACs will be moved to static entries. For example, if you set the maximum number of static MACs to 2 with the **set maclock static** command, and then executed the **set maclock move** command, even though there were five MACs in the first arrival table, only the two most recent MAC entries would be moved to static entries.

## MAC Locking Notifications

You can configure MAC locking notifications as SNMP traps and/or Syslog messages.

Use the **set maclock trap** command to enable or disable MAC locking SNMP trap messaging, and to specify when a trap should be sent. You can specify that a trap should be sent:

- If the MAC address table threshold is reached, or



- If a connected end station exceeds the maximum values configured with the **set maclock firstarrival** and **set maclock static** commands (a violation).

When “send-on-violation” is enabled, this feature authorizes the switch to send an SNMP trap message if an end station is connected that exceeds the maximum values configured using the **set maclock firstarrival** and **set maclock static** commands. Violating MAC addresses are dropped from the device’s (or stack’s) filtering database.

When “send-on-threshold” is enabled, the agent issues a trap when the MAC address table threshold, as defined in the etsysMACLockingFirstArrivalStationsAllocated object, is reached.

Use the **set maclock syslog** command to set the status of MAC locking syslog messages. Syslog messages are disabled by default. You can specify that a syslog message should be set:

- When the MAC address table threshold is reached, or
- If a connected end station exceeds the maximum values configured with the **set maclock firstarrival** and **set maclock static** commands (a violation).

When “send-on-violation” is enabled, this feature authorizes the switch to send a syslog message if an end station is connected that exceeds the maximum values configured using the **set maclock firstarrival** and **set maclock static** commands. Violating MAC addresses are dropped from the device’s (or stack’s) filtering database.

When “send-on-threshold” is enabled, the agent issues a syslog message when the MAC address table threshold, as defined in the etsysMACLockingFirstArrivalStationsAllocated object, is reached.

## Disabling and Enabling Ports

Use the **set maclock disable-port** command to enable MAC locking threshold shutdown (corresponds to etsMACLockingThresholdShutdown) on one or more ports. By default, this threshold shutdown is disabled on all ports. When threshold shutdown is enabled, the agent attempts to disable a port (operstatus down) when the MAC address table threshold, as defined in etsysMACLockingFirstArrival Stations-Allocated object, is exceeded.

Use the **clear maclock disable-port** command to clear MAC locking threshold shutdown to the default condition of disabled.

Use the **clear maclock violation disabled-port** command to clear ports disabled due to a MAC lock violation (corresponds to etsMACLockingShutdownState). This command will clear the operstatus down caused by a MAC lock disable-port threshold and clear the port’s etsMacLockingShutdownState.

## MAC Locking Defaults

**Table 26-6 MAC Locking Defaults**

| Parameter                               | Description                                                                                                     | Default Value                  |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------|--------------------------------|
| MAC locking state                       | Specifies whether MAC locking is enabled or disabled, both globally and on specific ports.                      | Disabled globally and on ports |
| Maximum number of dynamic MAC addresses | Specifies the maximum number of MAC addresses that will be locked on a port configured for dynamic MAC locking. | 600                            |
| Maximum number of static MAC addresses  | Specifies the maximum number of static MAC addresses allowed on a port.                                         | 20                             |

**Table 26-6 MAC Locking Defaults (continued)**

| Parameter                       | Description                                                                                                                                                                                 | Default Value                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| First arrival MAC address aging | Specifies that dynamic MAC locked addresses will be aged out of the database.                                                                                                               | Disabled                                                    |
| MAC lock traps                  | Specifies whether SNMP traps associated with MAC locking will be sent.                                                                                                                      | Disabled                                                    |
| MAC lock Syslog messages        | Specifies whether Syslog messages associated with MAC locking will be sent.                                                                                                                 | Disabled                                                    |
| Clear on link change            | Specifies whether First Arrival MAC addresses will be dropped or maintained on a loss of link.                                                                                              | Enabled (dynamic MAC addresses are dropped on loss of link) |
| MAC lock threshold shutdown     | Specifies whether a port is disabled (operstatus down) when the MAC address table threshold, as defined in <code>etsysMACLockingFirstArrival Stations-Allocated</code> object, is exceeded. | Disabled                                                    |

## MAC Locking Configuration

[Procedure 26-3](#) lists the commands used to configure MAC locking on the Fixed Switch platforms. Refer to the *CLI Reference* for your platform for details about using the commands listed.

### Procedure 26-3 MAC Locking Configuration

| Step | Task                                                                                                                                                                                                                                                                        | Command(s)                                                                                                         |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| 1.   | Globally enable MAC locking.                                                                                                                                                                                                                                                | <code>set maclock enable</code>                                                                                    |
| 2.   | Enable MAC locking on ports.                                                                                                                                                                                                                                                | <code>set maclock enable port-string</code>                                                                        |
| 3.   | Optionally, create static MAC address-to-port locking entries. The MAC locking entry is automatically enabled when you create the entry.<br>Use the <b>clear maclock</b> command to remove a static locking entry.                                                          | <code>set maclock mac-address port-string create</code><br><br><code>clear maclock mac-address port-string</code>  |
| 4.   | Optionally, disable or enable a static locking entry.                                                                                                                                                                                                                       | <code>set maclock mac-address port-string enable   disable</code>                                                  |
| 5.   | Optionally, set the maximum number of static MAC addresses allowed per port.<br>Use the <b>clear maclock static</b> command to return to the default of 20.                                                                                                                 | <code>set maclock static port-string value</code><br><br><code>clear maclock static port-string</code>             |
| 6.   | Optionally, restrict MAC locking on a port to a maximum number of end station addresses first connected to that port.<br>Use the <b>clear maclock firstarrival</b> command to reset the number of first arrival MAC addresses allowed per port to the default value of 600. | <code>set maclock firstarrival port-string value</code><br><br><code>clear maclock firstarrival port-string</code> |

**Procedure 26-3 MAC Locking Configuration (continued)**

| Step | Task                                                                                                                                                                                                                        | Command(s)                                                                                                                                                                                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.   | Optionally, enable the aging of first arrival MAC addresses on a port or ports.<br><br>Use either the <b>set maclock agefirstarrival disable</b> or <b>clear maclock firstarrival</b> commands to disable aging.            | <b>set maclock agefirstarrival</b><br><i>port-string</i> <b>enable</b>                                                                                                                                                                               |
| 8.   | Optionally, disable clearing of dynamic MAC addresses on link change.<br><br>Use either the <b>set maclock clearonlinkchange enable</b> or <b>clear maclock clearonlinkchange</b> commands to enable clearing on link loss. | <b>set maclock clearonlinkchange</b><br><i>port-string</i> <b>disable</b>                                                                                                                                                                            |
| 9.   | Optionally, move all current first arrival MACs to static entries.                                                                                                                                                          | <b>set maclock move</b> <i>port-string</i>                                                                                                                                                                                                           |
| 10.  | Optionally, configure MAC locking notifications.                                                                                                                                                                            | <b>set maclock trap</b> <i>port-string</i> { <b>enable</b>   <b>disable</b> } [ <b>threshold</b>   <b>violation</b> ]<br><br><b>set maclock syslog</b> <i>port-string</i> { <b>disable</b>   <b>enable</b> } [ <b>threshold</b>   <b>violation</b> ] |
| 11.  | Optionally, enable port shutdown when the first arrival threshold has been exceeded.<br><br>Use the <b>clear maclock disable-port</b> command to disable port shutdown.                                                     | <b>set maclock disable-port</b> <i>port-string</i><br><br><b>clear maclock disable-port</b><br><i>port-string</i>                                                                                                                                    |
| 12.  | Clear ports disabled due to a MAC lock violation.                                                                                                                                                                           | <b>clear maclock violation</b><br><b>disabled-port</b> <i>port-string</i>                                                                                                                                                                            |
| 13.  | Display MAC locking information.                                                                                                                                                                                            | <b>show maclock</b> [ <i>port-string</i> ]<br><br><b>show maclock stations</b> [ <b>firstarrival</b>   <b>static</b> ] [ <i>port-string</i> ]                                                                                                        |

## TACACS+

TACACS+ (Terminal Access Controller Access-Control System Plus), is a security protocol developed by Cisco Systems which can be used as an alternative to the standard RADIUS security protocol (RFC 2865). TACACS+ runs over TCP and encrypts the body of each packet.

Based on the now obsolete TACACS protocol (defined in RFC 1492), TACACS+ is defined in an unpublished and expired Internet Draft draft-grant-tacacs-02.txt, "The TACACS+ Protocol Version 1.78," January, 1997.

TACACS+ provides the following services:

- User authentication
- User authorization
- Accounting (user activity)

You can configure the TACACS+ client on your Enterasys device in conjunction with one or more TACACS+ access servers to provide authentication, authorization, or accounting services on your network. Each of the TACACS+ services can be implemented on separate servers.

You can also configure TACACS+ to use a single TCP connection for all TACACS+ client requests to a given TACACS+ server.

Up to 5 TACACS+ servers can be configured, with the index value of 1 having the highest priority. If you want to change the default timeout value for a specific server or all servers, you must enter the **set tacacs server** command using the **timeout** parameter.

When at least one backup server has been configured and the switch loses contact with the primary server, the switch will contact the next server in priority. If the switch was trying to authenticate a user when the connection was lost, or if the default login access (read-only permissions) had been received, the switch will try to authenticate again.

If a user had already been authenticated and authorized, then the backup server is contacted without requiring any authentication. The backup server will just authorize or account for the packets coming in for that user. Since a task ID is associated with each accounting session, if there is a failover to a backup server, the accounting information will still be associated with the correct session using the task ID.

When a failover to a backup server occurs, syslog messages are generated containing the reason for the failure.

## TACACS+ Client Functionality

TACACS+ client functionality falls into four basic capabilities:

- Authentication and session authorization
- Command authorization
- Session accounting
- Command accounting

### Session Authorization and Accounting

The TACACS+ client is disabled by default. When the TACACS+ client is enabled on an Enterasys device and a session is initiated, the configured session authorization parameters are sent by the client to the TACACS+ server. The parameter values must match a service and access level attribute-value pair configured on the server for the session to be authorized. If the parameter values do not match, the session is not allowed.

The service name and attribute-value pairs can be any character string, and are determined by your TACACS+ server configuration.

When session accounting is enabled, the TACACS+ server logs accounting information, such as start and stop times, IP address of the remote user, and so forth, for each authorized client session.

### Command Authorization and Accounting

TACACS+ command authorization and accounting can occur only during a TACACS+ authorized session.

When command authorization is enabled, the TACACS+ server checks whether each command is permitted for that authorized session and returns a success or failure for each one. If the authorization fails, the command is not executed.

When command accounting is enabled, the TACACS+ server logs accounting information, such as the command string and IP address of the remote user for each command executed during the session.

## Configuring the Source Address

You can configure the source IP address used by the TACACS+ application on the switch when generating packets for management purposes. Any of the management interfaces, including VLAN routing interfaces, can be configured as the source IP address used in packets generated by the TACACS+ client.

An interface must have an IP address assigned to it before it can be set as the TACACS+ source.

If no interface is specified, then the IP address of the Host interface will be used.

If a non-loopback interface is configured as the source, application packet egress is restricted to that interface if the server can be reached from that interface. Otherwise, the packets are transmitted over the first available route. Packets from the application server are received on the configured interface.

If a loopback interface is configured, and there are multiple paths to the application server, the outgoing interface (gateway) is determined based on the best route lookup. Packets from the application server are then received on the sending interface. If route redundancy is required, therefore, a loopback interface should be configured.

## Default Settings

Table 26-7 lists the TACACS+ parameters (as displayed through the **show tacacs** command) and their default values.

**Table 26-7 TACACS+ Parameters**

| Parameter                               | Description                                                                                                                                                           | Default Value                                                                       |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| TACACS+ state                           | Whether the TACACS+ client is enabled or disabled.                                                                                                                    | Disabled                                                                            |
| TACACS+ service                         | The name of the service that is requested by the TACACS+ client for session authorization.                                                                            | exec                                                                                |
| TACACS+ session authorization A-V pairs | The attribute-value pairs that are mapped to the A4read-only, read-write, and super-user access privilege levels for the service requested for session authorization. | read-only: "priv-lvl", 0<br>read-write: "priv-lvl", 1<br>super-user: "priv-lvl", 15 |
| TACACS+ session accounting state        | The TACACS+ client sends session accounting information, such as start and stop times, to a TACACS+ server for logging.                                               | Disabled                                                                            |
| TACACS+ command authorization state     | The TACACS+ client checks with a TACACS+ server whether each command is permitted for that authorized session.                                                        | Disabled                                                                            |
| TACACS+ command accounting state        | The TACACS+ client sends command accounting information, such as the command string and IP address of the remote user, to a TACACS+ server for logging.               | Disabled                                                                            |
| TACACS+ singleconnect state             | The TACACS+ client sends multiple requests to a TACACS+ server over a single TCP connection.                                                                          | Disabled                                                                            |
| TACACS+ Server Timeout                  | The period of time (in seconds) the device A4waits for a response from the TACACS+ server before it times out and declares an error.                                  | 10 seconds                                                                          |

## Basic TACACS+ Configuration

[Procedure 26-4](#) describes the basic steps to configure TACACS+ on Enterasys devices. It assumes that you have gathered the necessary TACACS+ server information, such as the server's IP address, the TCP port to use, shared secret, the authorization service name, and access level attribute-value pairs.



**Note:** You must be logged in to the Enterasys device with read-write access rights to use the commands shown in this procedure.

### Procedure 26-4 TACACS+ Configuration

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                     | Command(s)                                                                                                                                               |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Enable the TACACS+ client.<br>To disable the TACACS+ client, use the <b>set tacacs disable</b> command.                                                                                                                                                                                                                                                                                                                                  | <b>set tacacs enable</b>                                                                                                                                 |
| 2.   | Configure the TACACS+ servers, up to a maximum of five, to be used by the TACACS+ client. Define the IP address, TCP port, and secret for each server.<br>To remove one or all configured TACACS+ servers, use the <b>clear tacacs server {all   index}</b> command.                                                                                                                                                                     | <b>set tacacs server</b> <i>index address port secret</i>                                                                                                |
| 3.   | Optionally, change the timeout for each server from the default, 10 seconds. Possible timeout values are 1–30 seconds.<br>To return the timeout value to its default value for one or all configured TACACS+ servers, use the <b>clear tacacs server {all   index} timeout</b> command.                                                                                                                                                  | <b>set tacacs server</b> { <i>all   index</i> } <b>timeout</b> <i>seconds</i>                                                                            |
| 4.   | Optionally, enable session accounting.<br>To disable TACACS+ session accounting, use the <b>set tacacs session accounting disable</b> command.                                                                                                                                                                                                                                                                                           | <b>set tacacs session accounting enable</b>                                                                                                              |
| 5.   | Optionally, configure the TACACS+ session authorization service or access level. The default service name is "exec."<br>Refer to <a href="#">Table 26-7</a> on page 26-13 for the default values of the access level attribute-value pairs.<br>To return the TACACS+ session authorization settings to their default values, use the <b>clear tacacs session authorization {[service] [read-only] [read-write] [superuser]}</b> command. | <b>set tacacs session</b><br>{ <i>authorization service name   read-only attribute value   read-write attribute value   super-user attribute value</i> } |
| 6.   | Optionally, enable per-command accounting.<br>To disable TACACS+ accounting on a per-command basis, use the <b>set tacacs command accounting disable</b> command.                                                                                                                                                                                                                                                                        | <b>set tacacs command accounting enable</b>                                                                                                              |
| 7.   | Optionally, enable per-command authorization.<br>To disable TACACS+ authorization on a per-command basis, use the <b>set tacacs command authorization disable</b> command.                                                                                                                                                                                                                                                               | <b>set tacacs command authorization enable</b>                                                                                                           |

**Procedure 26-4 TACACS+ Configuration (continued)**

| Step | Task                                                                                                                                                                                                                                                                                                              | Command(s)                                                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| 8.   | Optionally, enable the TACACS+ client to send multiple requests to the server over a single TCP connection.<br><br>To disable the use of a single TCP connection, use the <b>set tacacs singleconnect disable</b> command.                                                                                        | <b>set tacacs singleconnect enable</b>                           |
| 9.   | Optionally, set the interface used for the source IP address of the TACACS+ packets generated by the switch.<br><br>Use the clear tacacs interface command to reset the source IP address to the host IP address of the switch.<br><br><b>Note:</b> This functionality is not supported on the I-Series platform. | <b>set tacacs interface</b> {loopback<br>loop-ID   vlan vlan-ID} |
| 10.  | If not already configured, set the primary login authentication method to TACACS+.                                                                                                                                                                                                                                | <b>set authentication login tacacs</b>                           |

## Example TACACS+ Configuration

In the following configuration example, the TACACS+ server is defined as having the IP address 192.168.10.10. The TCP port is set to 49, which is the standard TACACS+ TCP port. The authorization service is set to “basic” and the read-write access privilege is set to 5. Session and command accounting are enabled, as is command authorization. A single TCP connection will be used for all TACACS+ communication with 192.168.10.10. Finally, the primary login authentication method is set to TACACS+.

```
C5(rw)->set tacacs enable
C5(rw)->set tacacs server 1 192.168.10.10 49 mysecret
C5(rw)->set tacacs session accounting enable
C5(rw)->set tacacs session authorization service basic
C5(rw)->set tacacs session authorization read-write priv-lvl 5
C5(rw)->set tacacs command accounting enable
C5(rw)->set tacacs command authorization enable
C5(rw)->set tacacs singleconnect enable
C5(rw)->set authentication login tacacs
```

## TACACS+ Display Commands

[Table 26-8](#) lists TACACS+ show commands.

**Table 26-8 TACACS+ Show Commands**

| Task                                                                    | Command                                 |
|-------------------------------------------------------------------------|-----------------------------------------|
| Displays all current TACACS+ configuration information and status.      | <b>show tacacs [state]</b>              |
| Displays only the current configuration for one or all TACACS+ servers. | <b>show tacacs server</b> {index   all} |

**Table 26-8 TACACS+ Show Commands (continued)**

| Task                                                                                                                                                                     | Command                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| Displays only the current TACACS+ session settings. The <b>[state]</b> option is valid only for S-Series and Matrix N-Series devices.                                    | <code>show tacacs session {authorization   accounting} [state]</code> |
| Displays only the current status for TACACS+ per-command authorization and accounting. The <b>[state]</b> option is valid only for S-Series and Matrix N-Series devices. | <code>show tacacs command {accounting   authorization} [state]</code> |
| Displays only the current singleconnect status. The <b>[state]</b> option is valid only for S-Series and Matrix N-Series devices.                                        | <code>show tacacs singleconnect [state]</code>                        |
| Displays the currently configured interface to use as the source interface for TACACS+ packets, if one is configured.                                                    | <code>show tacacs interface</code>                                    |

Refer to your platform's *CLI Reference* for more information about each command.

## Service ACLs

A Service Access Control List (SACL) can provide security for switch management features, by ensuring that only known and trusted devices are allowed to remotely manage the switch via TCP/IP.

A Service ACL can be applied to a specific host service, or to all supported host services. The following host services are currently supported:

- HTTP
- HTTPS
- SNMP
- SSH
- Telnet
- TFTP

Service ACLs are applied to inbound traffic only. When a Service ACL is enabled, incoming TCP packets initiating a connection (TCP SYN) and all UDP packets will be filtered based on their source IP address and destination port. Additionally, other attributes such as incoming port and VLAN ID can be used to determine if the traffic should be allowed to the management interface. When the component is disabled, incoming TCP/UDP packets are not filtered and are processed normally.

Only one Service ACL can be configured on the switch, with a maximum of 64 rules. The Service ACL will not be actively used on the switch until it is activated with the `set system service-class` command. Both IPv4 and IPv6 address rules are supported.

A trap is sent if a packet is dropped due to a service ACL rule hit. A trap will not be generated if traffic is dropped due to the "console-only" option (see [Restricting Management Access to the Console Port](#) below). The Enterasys Threat Notification MIB is used for trap generation.



## Restricting Management Access to the Console Port

You can restrict access to system management to the switch's serial port only. This is done using the **set system service-class console-only** command. When console-only access is configured, all TCP SYN packets and UDP packets are dropped, with the exception of UDP packets sent to the DHCP Server or DHCP Client ports. Attempting to map a router ACL to a host service will fail.

## Configuring a Service Access Control List

Use the **set system service-acl** command to configure a service access control list. Each rule should have a unique priority. New rules without a priority will be entered at the end of the service ACL. Use the **set system access-class** command to choose the active service-acl. The active management list can't be updated or removed.

A service ACL has an implicit deny all rule at the end. If you want to allow access by a network server that is not covered by the specific *services* listed with the **service** parameter, such as a network NTP/SNTP server, you can add a permit rule for the IP address of that server.

[Procedure 26-5](#) lists the commands used to create a service ACL and apply it to the switch. Refer to the CLI Reference for your platform for more information about these commands.

### Procedure 26-5 Configuring a Service ACL

| Step | Task                                                                                                                                                                                                           | Command(s)                                                                                                                                                                                                                                                                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Create and add rules to a service access control list. Only a single list is allowed in the system with a maximum of 64 rules.<br><br>Use the <b>clear system service-acl</b> command to remove a service ACL. | <b>set system service-acl</b> <i>name</i><br>{ <b>permit</b>   <b>deny</b> }<br>[ <b>ip-source</b> <i>ip-addr</i> [ <b>wildcard</b> <i>bits</i> ]<br>  <b>ipv6-source</b> <i>ipv6-addr</i> [ <b>wildcard</b> / <i>prefix-length</i> ]]<br>[ <b>port</b> <i>port-string</i>   <b>vlan</b> <i>vlan-id</i> ]<br>[ <b>service</b> <i>service</i> ]<br>[ <b>priority</b> <i>priority-value</i> ] |
| 2.   | Activate a service ACL on the switch, or restrict management access to the console port.                                                                                                                       | <b>set system service-class</b> { <i>name</i>   <b>console-only</b> }                                                                                                                                                                                                                                                                                                                       |
| 3.   | De-activate a service ACL or remove the restriction of management to the console port.                                                                                                                         | <b>clear system service-class</b>                                                                                                                                                                                                                                                                                                                                                           |
| 4.   | Display the contents of the service ACL configured on the switch.                                                                                                                                              | <b>show system service-acl</b> [ <i>name</i> ]                                                                                                                                                                                                                                                                                                                                              |
| 5.   | Display the current system service ACL status.                                                                                                                                                                 | <b>show system service-class</b>                                                                                                                                                                                                                                                                                                                                                            |

The following example adds two rules to allow remote management for all host services through ports ge.1.1 and ge.1.2. A third rule permits traffic from the SNTP network server with IP address 10.10.22.2.

Since no priority is specified, the rules will be added in the order in which they entered. Then a rule is added that denies SSH access from source IPv4 address 192.168.10.10 and sets the priority of the rule to 1. The contents of the service ACL is then displayed, and it is activated on the switch.

```
C5(su)->set system service-acl my-sacl permit port ge.1.1
C5(su)->set system service-acl my-sacl permit port ge.1.2
C5(su)->set system service-acl my-sacl permit ip-source 10.10.22.2 port 123
C5(su)->set system service-acl my-sacl deny service ssh ip-source 192.168.10.10
priority 1
C5(su)->show system service-acl
my-sacl
```

```

set system service-acl my-sacl deny ip-source 192.168.10.10 mask 255.255.255.255
service ssh priority 1
set system service-acl my-sacl permit port ge.1.1 priority 2
set system service-acl my-sacl permit port ge.1.2 priority 3
set system service-acl my-sacl permit ip-source 10.10.22.2 port 123
! (Note: all other access implicitly denied)
C5(su)->set system service-class my-sacl
```

## DHCP Snooping

DHCP snooping monitors DHCP messages between DHCP clients and DHCP servers to filter harmful DHCP messages and to build a bindings database of {MAC address, IP address, VLAN ID, port} tuples that are considered authorized.

DHCP snooping is disabled globally and on all VLANs by default. Ports are untrusted by default. DHCP snooping must be enabled globally and on specific VLANs. Ports within the VLANs must be configured as trusted or untrusted. On trusted ports, DHCP client messages are forwarded directly by the hardware. On untrusted ports, client messages are given to the DHCP snooping application. DHCP servers must be reached through trusted ports.

DHCP snooping enforces the following security rules:

- DHCP packets from a DHCP server (DHCP OFFER, DHCP ACK, DHCP NAK) are dropped if received on an untrusted port.
- DHCP RELEASE and DHCP DECLINE messages are dropped if they are for a MAC address in the snooping database but the binding's interface in the database is different from the interface where the message was received.
- On untrusted interfaces, the switch drops DHCP packets whose source MAC address does not match the client hardware address. This feature is a configurable option.

## DHCP Message Processing

The hardware identifies all incoming DHCP packets on ports where DHCP snooping is enabled. On untrusted ports, the hardware traps all incoming DHCP packets to the CPU. On trusted ports, the hardware forwards client messages and copies server messages to the CPU so DHCP snooping can learn the binding.

The DHCP snooping application processes incoming DHCP messages. For DHCP RELEASE and DHCP DECLINE messages, the application compares the receive interface and VLAN with the client's interface and VLAN in the bindings database. If the interfaces do not match, the application logs the event and drops the message. For valid client messages, DHCP snooping compares the source MAC address to the DHCP client hardware address. Where there is a mismatch, DHCP snooping logs and drops the packet. You can disable this feature using the **set dhcpsnooping verify mac-address disable** command.



**Note:** If the switch has been configured as a DHCP relay agent, to forward client requests to a DHCP server that does not reside on the same broadcast domain as the client, MAC address verification should be disabled in order to allow DHCP RELEASE packets to be processed by the DHCP snooping functionality and client bindings removed from the bindings database.

DHCP snooping can be configured on switching VLANs and routing VLANs. When a DHCP packet is received on a routing VLAN, the DHCP snooping application applies its filtering rules and updates the bindings database. If a client message passes filtering rules, the message is placed

into the software forwarding path, where it may be processed by the DHCP relay agent, the local DHCP server, or forwarded as an IP packet.

DHCP snooping forwards valid DHCP client messages received on non-routing VLANs. The message is forwarded on all trusted interfaces in the VLAN. If a DHCP relay agent or local DHCP server co-exist with the DHCP snooping feature, DHCP client messages will be sent to the DHCP relay agent or local DHCP server to process further.

The ports on the switch through which DHCP servers are reached must be configured as trusted ports so that packets received from those ports will be forwarded to clients in hardware. DHCP packets from a DHCP server (DHCP OFFER, DHCP ACK, DHCP NAK) are dropped if received on an untrusted port.

## Building and Maintaining the Database

The DHCP snooping application uses DHCP messages to build and maintain the bindings database. The bindings database includes only data for clients on untrusted ports. The bindings database includes the following information for each entry:

- Client MAC address
- Client IP address
- Time when client's lease expires
- Client VLAN ID
- Client port

DHCP snooping creates a tentative binding from DHCP DISCOVER and REQUEST messages. Tentative bindings tie a client to a port (the port where the DHCP client message was received). Tentative bindings are completed when DHCP snooping learns the client's IP address from a DHCP ACK message on a trusted port. DHCP snooping removes bindings in response to DECLINE, RELEASE, and NACK messages. The DHCP snooping application ignores the ACK messages sent in reply to the DHCP Inform messages received on trusted ports. You can also enter static bindings into the bindings database with the **set dhcpsnooping binding** command.

When a switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database.

If the absolute lease time of a snooping database entry expires, then that entry will be removed. Care should be taken to ensure that system time is consistent across the reboots. Otherwise, snooping entries will not expire properly. If a host sends a DHCP RELEASE message while the switch is rebooting, when the switch receives a DHCP DISCOVERY or REQUEST message, the client's binding will go to a tentative binding state.

## Rate Limiting

To protect the switch against DHCP attacks when DHCP snooping is enabled, the snooping application enforces a rate limit for DHCP packets received on untrusted interfaces. DHCP snooping monitors the receive rate on each interface separately. If the receive rate exceeds a configurable limit, DHCP snooping brings down the interface. Use the **set port enable** command to re-enable the interface. Both the rate and the burst interval can be configured.

## Basic Configuration

[Procedure 26-6](#) on page 26-20 describes the commands used to configure DHCP Snooping. Refer to the *CLI Reference* for your platform for command details.

**Procedure 26-6 Basic Configuration for DHCP Snooping**

| Step | Task                                                                                            | Command(s)                                                                                                          |
|------|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| 1.   | Enable DHCP snooping globally on the switch.                                                    | <code>set dhcpsnooping enable</code>                                                                                |
| 2.   | Determine where DHCP clients will be connected and enable DHCP snooping on their VLANs.         | <code>set dhcpsnooping vlan <i>vlan-list</i> enable</code>                                                          |
| 3.   | Determine which ports will be connected to the DHCP server and configure them as trusted ports. | <code>set dhcpsnooping trust port <i>port-string</i> enable</code>                                                  |
| 4.   | If desired, enable logging of invalid DHCP messages on specific ports.                          | <code>set dhcpsnooping log-invalid port <i>port-string</i> enable</code>                                            |
| 5.   | If desired, add static bindings to the database.                                                | <code>set dhcpsnooping binding <i>mac-address</i> vlan <i>vlan-id</i> ipaddr <i>port</i> <i>port-string</i></code>  |
| 6.   | If the switch has been configured as a DHCP relay agent, disable MAC address verification.      | <code>set dhcpsnooping verify mac-address disable</code>                                                            |
| 7.   | If desired, change the rate limiting values.                                                    | <code>set dhcpsnooping limit <i>port-string</i> {none   rate <i>pps</i> {burst <i>interval</i> <i>secs</i>}}</code> |

**Configuration Notes****DHCP Server**

- When the switch is operating in switch mode, then the DHCP server and DHCP clients must be in the same VLAN.
- If the switch is in routing mode (on those platforms that support routing), then the DHCP server can be remotely connected to a routing interface, or running locally.
- If the DHCP server is remotely connected, then the use of an IP helper address is required and MAC address verification should be disabled (`set dhcpsnooping verify mac-address disable`).
- The DHCP server must use Scopes in order to provide the IP addresses per VLAN.
- DHCP snooping must be enabled on the interfaces where the DHCP clients are connected, and the interfaces must be untrusted DHCP snooping ports.
- The routing interface that is connected to the DHCP server must be enabled for DHCP snooping and must be a trusted DHCP snooping port.

**Default Parameter Values****Table 26-9 DHCP Snooping Default Parameters**

| Parameter                                 | Default Setting                    |
|-------------------------------------------|------------------------------------|
| DHCP snooping                             | Disabled globally and on all VLANs |
| Trusted ports                             | All ports are untrusted            |
| Source MAC address verification           | Enabled                            |
| Logging of invalid DHCP messages on ports | Disabled                           |
| Rate limit for DHCP packets               | 15 packets per second              |

**Table 26-9 DHCP Snooping Default Parameters (continued)**

| Parameter      | Default Setting |
|----------------|-----------------|
| Burst interval | 1 second        |

## Managing DHCP Snooping

Table 26-10 on page 21 lists the commands to display DHCP snooping information. Table 26-11 on page 21 lists the commands to manage DHCP snooping. Refer to the *CLI Reference* for your platform for command details.

**Table 26-10 Displaying DHCP Snooping Information**

| Task                                                                                                                                                                                                                                                                                                                                                                                                           | Command                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| To display <ul style="list-style-type: none"> <li>The status (enabled or disabled) of DHCP snooping globally</li> <li>A list of the VLANs on which DHCP snooping is enabled</li> <li>Whether source MAC address verification is enabled or disabled</li> <li>For ports that are enabled for snooping, whether they are trusted or untrusted and whether logging of invalid packets has been enabled</li> </ul> | <code>show dhcpsnooping</code>                                                                            |
| To display the trust state and rate limiting parameters configured on specified ports                                                                                                                                                                                                                                                                                                                          | <code>show dhcpsnooping port <i>port-string</i></code>                                                    |
| To display the contents of the DHCP snooping bindings database                                                                                                                                                                                                                                                                                                                                                 | <code>show dhcpsnooping binding [dynamic   static] [port <i>port-string</i>] [vlan <i>vlan-id</i>]</code> |
| To display DHCP snooping statistics for untrusted ports                                                                                                                                                                                                                                                                                                                                                        | <code>show dhcpsnooping statistics</code>                                                                 |

**Table 26-11 Managing DHCP Snooping**

| Task                                                                                                      | Command                                                                                 |
|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| To remove bindings from the DHCP snooping bindings database                                               | <code>clear dhcpsnooping binding [port <i>port-string</i>   mac <i>mac-addr</i>]</code> |
| To clear the DHCP snooping statistics counters                                                            | <code>clear dhcpsnooping statistics</code>                                              |
| To reset the rate limit values to the defaults of 15 packets per second with a burst interval of 1 second | <code>clear dhcpsnooping limit <i>port-string</i></code>                                |

## Dynamic ARP Inspection

Dynamic ARP inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. The feature prevents a class of man-in-the-middle attacks where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. ARP poisoning is a tactic where an attacker injects false ARP packets into the subnet, normally by broadcasting ARP responses in which the attacker claims to be someone else. By poisoning the ARP cache, a malicious user can intercept the traffic intended for other hosts on the network.

The Dynamic ARP Inspection application performs ARP packet validation. When DAI is enabled, it verifies that the sender MAC address and the source IP address are a valid pair in the DHCP snooping binding database and drops ARP packets whose sender MAC address and sender IP address do not match an entry in the database. Additional ARP packet validation can be configured.

If DHCP snooping is disabled on the ingress VLAN or the receive interface is trusted for DHCP snooping, ARP packets are dropped.

### Functional Description

DAI is enabled on VLANs, effectively enabling DAI on the interfaces (physical ports or LAGs) that are members of that VLAN. Individual interfaces are configured as trusted or untrusted. The trust configuration for DAI is independent of the trust configuration for DHCP snooping. A trusted port is a port the network administrator does not consider to be a security threat. An untrusted port is one which could potentially be used to launch a network attack.

DAI considers all physical ports and LAGs untrusted by default.

### Static Mappings

Static mappings are useful when hosts configure static IP addresses, DHCP snooping cannot be run, or other switches in the network do not run dynamic ARP inspection. A static mapping associates an IP address to a MAC address on a VLAN. DAI consults its static mappings before it consults DHCP snooping — thus, static mappings have precedence over DHCP snooping bindings.

ARP ACLs are used to define static mappings for DAI. In this implementation, only the subset of ARP ACL syntax required for DAI is supported. ARP ACLs are completely independent of ACLs used for QoS. A maximum of 100 ARP ACLs can be configured. Within an ACL, a maximum of 20 rules can be configured.

### Optional ARP Packet Validation

If optional ARP packet validation has been configured, DAI verifies that the sender MAC address equals the source MAC address in the Ethernet header. Additionally, the option to verify that the target MAC address equals the destination MAC address in the Ethernet header can be configured. This check only applies to ARP responses, since the target MAC address is unspecified in ARP requests.

You can also enable IP address checking. When this option is enabled, DAI drops ARP packets with an invalid IP address. The following IP addresses are considered invalid:

- 0.0.0.0
- 255.255.255.255
- All IP multicast addresses
- All class E addresses (240.0.0.0/4)

- Loopback addresses (in the range 127.0.0.0/8)

## Logging Invalid Packets

By default, DAI writes a log message to the normal buffered log for each invalid ARP packet it drops. You can configure DAI to not log invalid packets for specific VLANs.

## Packet Forwarding

DAI forwards valid ARP packets whose destination MAC address is not local. The ingress VLAN could be a switching or routing VLAN. ARP requests are flooded in the VLAN. ARP responses are unicast toward their destination. DAI queries the MAC address table to determine the outgoing port. If the destination MAC address is local, DAI gives valid ARP packets to the ARP application.

## Rate Limiting

To protect the switch from DHCP attacks when DAI is enabled, the DAI application enforces a rate limit for ARP packets received on untrusted interfaces. DAI monitors the receive rate on each interface separately. If the receive rate exceeds a configurable limit, DAI error disables the interface, which effectively brings down the interface. You can use the **set port enable** command to re-enable the port.

You can configure both the rate and the burst interval. The default rate is 15 packets per second (pps) on each untrusted interface with a range of 0 to 50 pps. The default burst interval is 1 second with a range to 1 to 15 seconds. The rate limit cannot be set on trusted interfaces since ARP packets received on trusted interfaces do not come to the CPU.

## Eligible Interfaces

Dynamic ARP inspection is enabled per VLAN, effectively enabling DAI on the members of the VLAN, either physical ports or LAGs. Trust is specified on the VLAN members.

DAI may be connected to:

- A single host through a trusted link (for example, a server)
- If multiple hosts need to be connected, there must be a switch between the router and the hosts, with DAI enabled on that switch

## Interaction with Other Functions

- DAI relies on the DHCP snooping application to verify that a {IP address, MAC address, VLAN, interface} tuple is valid.
- DAI registers with dot1q to receive notification of VLAN membership changes for the VLANs where DAI is enabled.
- DAI tells the driver about each untrusted interface (physical port or LAG) where DAI is enabled so that the hardware will intercept ARP packets and send them to the CPU.



## Basic Configuration

[Procedure 26-7](#) below lists the commands used to configure DAI. Refer to the *CLI Reference* for your platform for command details.

### Procedure 26-7 Basic Dynamic ARP Inspection Configuration

| Step | Task                                                                                                                                                                          | Command(s)                                                                                                                                                                                                |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Configure DHCP snooping.                                                                                                                                                      | Refer to <a href="#">Procedure 26-6</a> on page 26-20.                                                                                                                                                    |
| 2.   | Enable ARP inspection on the VLANs where clients are connected, and optionally, enable logging of invalid ARP packets.                                                        | <code>set arpinspection vlan <i>vlan-range</i> [logging]</code>                                                                                                                                           |
| 3.   | Determine which ports are not security threats and configure them as DAI trusted ports.                                                                                       | <code>set arpinspection trust port <i>port-string</i> enable</code>                                                                                                                                       |
| 4.   | If desired, configure optional validation parameters.                                                                                                                         | <code>set arpinspection validate {[src-mac] [dst-mac] [ip]}</code>                                                                                                                                        |
| 5.   | If desired, change the default rate limiting parameters for incoming ARP packets on a port or ports.                                                                          | <code>set arpinspection limit port <i>port-string</i> {none   rate <i>pps</i> {burst interval <i>secs</i>}}</code>                                                                                        |
| 6.   | If desired, configure static mappings for DAI by creating ARP ACLs: <ul style="list-style-type: none"> <li>• Create the ARP ACL</li> <li>• Apply the ACL to a VLAN</li> </ul> | <code>set arpinspection filter <i>name</i> permit ip host <i>sender-ipaddr</i> mac host <i>sender-macaddr</i></code><br><code>set arpinspection filter <i>name</i> vlan <i>vlan-range</i> [static]</code> |

## Default Parameter Values

**Table 26-12 Dynamic ARP Inspection Default Parameters**

| Parameter                                  | Default Setting       |
|--------------------------------------------|-----------------------|
| Dynamic ARP inspection                     | Disabled on all VLANs |
| Logging of invalid ARP packets             | Disabled              |
| Trust state of all physical ports and LAGs | Untrusted             |
| Rate limit for incoming ARP packets        | 15 packets per second |
| Burst interval                             | 1 second              |

## Managing Dynamic ARP Inspection

[Table 26-13](#) on page 24 lists the commands to display dynamic ARP inspection information. [Table 26-14](#) on page 25 lists the commands to manage dynamic ARP inspection. Refer to the *CLI Reference* for your platform for command details.

**Table 26-13 Displaying Dynamic ARP Inspection Information**

| Task                                                  | Command                                                       |
|-------------------------------------------------------|---------------------------------------------------------------|
| To display ARP access list configuration information  | <code>show arpinspection access-list [<i>acl-name</i>]</code> |
| To display the ARP configuration of one or more ports | <code>show arpinspection ports [<i>port-string</i>]</code>    |



**Table 26-13 Displaying Dynamic ARP Inspection Information (continued)**

| Task                                                                      | Command                                                          |
|---------------------------------------------------------------------------|------------------------------------------------------------------|
| To display the ARP configuration of one or more VLANs                     | <code>show arpinspection vlan<br/>vlan-range</code>              |
| To display ARP statistics for all DAI-enabled VLANs or for specific VLANs | <code>show arpinspection statistics<br/>[vlan vlan-range]</code> |

**Table 26-14 Managing Dynamic ARP Inspection**

| Task                                                                                                                                                                                                                                                                                                                    | Command                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| To remove additional optional ARP validation parameters that were previously configured.                                                                                                                                                                                                                                | <code>clear arpinspection validate<br/>{[src-mac] [dst-mac] [ip]}</code>                                                                    |
| To disable dynamic ARP inspection on one or more VLANs or to disable logging of invalid ARP packets on one or more VLANs. To disable both logging and DAI, you must enter this command twice.                                                                                                                           | <code>clear arpinspection vlan<br/>vlan-range [logging]</code>                                                                              |
| To: <ul style="list-style-type: none"> <li>Remove a configured ARP ACL from the switch, or</li> <li>Remove a permit rule from a configured ARP ACL, or</li> <li>Remove the association of an ARP ACL with a VLAN or VLANs, or</li> <li>Disable static mapping of an ARP ACL associated with a VLAN or VLANs.</li> </ul> | <code>clear arpinspection filter name<br/>[permit ip host sender-ipaddr<br/>mac host sender-macaddr]   [vlan<br/>vlan-range [static]</code> |
| To return the DAI rate limiting values to their default values for a port or range of ports.                                                                                                                                                                                                                            | <code>clear arpinspection limit port<br/>port-string</code>                                                                                 |
| To clear all dynamic ARP inspection statistics                                                                                                                                                                                                                                                                          | <code>clear arpinspection statistics</code>                                                                                                 |

## Example Configuration

This section provides two examples, one for a non-routing switch, and one for routing switches.

### Non-Routing Example

The following example configures DHCP snooping and dynamic ARP inspection in a non-routing environment. The example configures VLAN 10 on the switch and then enables DHCP snooping and dynamic ARP inspection on this VLAN. Interfaces are configured as follows:

- Interface ge.1.1, which is connected to a DHCP server, on VLAN 10
- Interface ge.1.2, which is connected to DHCP clients, on VLAN 10

### VLAN Configuration

```
set vlan create 10
clear vlan egress 1 ge.1.1-2
set vlan egress 10 ge.1.2 untagged
```

### DHCP Snooping Configuration

```
set dhcpsnooping enable
set dhcpsnooping vlan 10 enable
set dhcpsnooping trust port ge.1.1 enable
```

## Dynamic ARP Inspection Configuration

```
set arpinspection vlan 10
set arpinspection trust port ge.1.1 enable
```

## Routing Example



**Note:** This example applies only to platforms that support routing.

The following example configures DHCP snooping and dynamic ARP inspection in a routing environment using RIP. The example configures two interfaces on the switch, configuring RIP on both interfaces, assigning each to a different VLAN, and then enabling DHCP snooping and dynamic ARP inspection on them:

- Interface ge.1.1, which is connected to a remote DHCP server, on VLAN 192
- Interface ge.1.2, which is connected to DHCP clients, on VLAN 10

In addition, the default VLAN, VLAN 1, is also enabled for DHCP snooping and dynamic ARP inspection.

Since the DHCP server is remote, the switch has been configured as a DHCP relay agent (with the **ip helper-address** command), to forward client requests to the DHCP server. Therefore, MAC address verification is disabled (with the **set dhcp snooping verify mac-address disable** command) in order to allow DHCP RELEASE packets to be processed by the DHCP snooping functionality and client bindings removed from the bindings database

## Router Configuration

```
router
enable
configure
interface vlan 10
no shutdown
ip address 10.2.0.1 255.255.0.0
ip helper-address 192.168.0.200
ip rip send version 2
ip rip receive version 2
ip rip enable
exit

interface vlan 192
no shutdown
ip address 192.168.0.1 255.255.255.0
ip rip send version 2
ip rip receive version 2
ip rip enable
exit
router rip
exit
```

**VLAN Configuration**

```
set vlan create 10
set vlan create 192
clear vlan egress 1 ge.1.1-2
set vlan egress 10 ge.1.2 untagged
set vlan egress 192 ge.1.1 untagged
```

**DHCP Snooping Configuration**

```
set dhcpsnooping enable
set dhcpsnooping vlan 1 enable
set dhcpsnooping vlan 10 enable
set dhcpsnooping vlan 192 enable
set dhcpsnooping verify mac-address disable
set dhcpsnooping trust port ge.1.1 enable
```

**Dynamic ARP Inspection Configuration**

```
set arpinspection vlan 1
set arpinspection vlan 10
set arpinspection vlan 192
set arpinspection trust port ge.1.1 enable
```

