53-1001583-01
21 June 2010

Brocade Adapters

Administrator's Guide

Supporting HBA models 825, 815, 804, 425, 415

BROCADE

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
1745 Technology Drive
San Jose, CA 95110
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

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

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

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

Document History

Title	Publication number	Summary of changes	Date
Brocade Adapters Administrator’s Guide Supporting HBA models 415, 425, 815, 825	*53-1000881-01*	New document	June 2008
Brocade Adapters Administrator’s Guide Supporting HBA models 825, 815, 804, 425, 415	*53-1001583-01*	Updates to support the HBA model 804 (mezzanine card for the Hewlett Packard Blade server)	June 2010

Contents

About This Document

In this section

How this document is organized

. This document is organized to help you find the information that you want as quickly and easily as possible.

The document contains the following components:

- Chapter 1, “Host Management Overview,” provides a description of the Host Connectivity Manager (HCM) application software, the graphical user interface (GUI), system requirements, and supported operating systems.
- Chapter 2, “Getting Started with HCM Software,” explains how to launch the management software, set security passwords, discover SAN components, and log out.
- Chapter 3, “Host Configuration,” provides the procedures to configure operating parameters (basic and advanced), security authentication, and persistent binding using the Brocade Command Line Utility (BCU) or the GUI.
- Chapter 4, “Monitoring,” describes the HCM monitoring features.
- Chapter 5, “Diagnostics,” describes the non-destructive group of diagnostic commands that can be run from the BCU or the GUI.
- Appendix A, “HCM Dialog Boxes,” lists the fields that are associated with the HCM GUI and provides a definition for each field.
- Appendix B, “Brocade Command Utility,” provides reference information for the Host Connectivity Manager (HCM) commands that can be run from the Brocade Command Line Utility (BCU)
- Appendix C, “HCM Troubleshooting,” provides a summary of HCM navigation problems and workarounds.
- Appendix D, “Glossary and Acronyms,” provides reference information for common terms and acronyms.

Document conventions

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

Text formatting

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

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

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, **switchShow**. In actual examples, command lettercase is often all lowercase. Otherwise, this manual specifically notes those cases in which a command is case sensitive.

Notes, cautions, and warnings

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

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

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

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Key terms

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

For definitions specific to this document, see "Glossary and Acronyms" on page 165.

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

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

Notice to the reader

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

These references are made for informational purposes only.

Corporation	Referenced Trademarks and Products
Microsoft Corporation	Windows Server, Windows XP, Windows Vista
Sun Microsystems, Inc.	Sun, Solaris
Red Hat, Inc.	Red Hat, Red Hat Network, Maximum RPM, Linux Undercover
Novell, Inc.	SuSE Enterprise Server (SLES), Linux
VMware	VMware, ESX Server

Additional information

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

Brocade resources

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

For practical discussions about SAN design, implementation, and maintenance, you can obtain *Building SANs with Brocade Fabric Switches* through:

http://www.amazon.com

White papers, online demos, and data sheets are available through the Brocade Web site at:

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

For additional Brocade documentation, visit the Brocade Web site:

http://www.brocade.com

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

Other industry resources

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

http://www.t11.org

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

http://www.fibrechannel.org

Getting technical help

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

- Adapter model and serial number
- Adapter operating system version
- Error numbers and messages received
- **supportSave** command output (see "debug" on page 135 for details)
- Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions
- Description of any troubleshooting steps already performed and the results
- Serial console and Telnet session logs
- syslog message logs

Related documentation

- *Brocade Adapters Installation and Reference Manual*
- *Brocade Adapters Troubleshooting Guide*
- *Fabric OS Administrator's Guide supporting Fabric OS v6.4.0*
- *Fabric OS Troubleshooting and Diagnostics Guide supporting Fabric OS v6.4.0*
- Data Center Fabric Manager User Manual

Document feedback

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

documentation@brocade.com

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

Chapter

1

Host Management Overview

In this chapter

Host bus adapters

Brocade offers five models of Fibre Channel Host Bus Adapters (HBAs). These models provide reliable, high-performance host connectivity for mission-critical SAN environments. The Brocade HBAs are listed in Table 1.

TABLE 1 Brocade Fibre Channel HBA models

Model Number	Port Speed	Number of Ports
415	4 Gbps maximum[2]	1
425	4 Gbps maximum[2]	2
804	8 Gbps maximum	2
815	8 Gbps maximum[1]	1
825	8 Gbps maximum[1]	2

[1] A 4 Gbps SFP installed in Brocade 815 or 825 HBAs allows 4, 2, or 1 Gbps speed only.
[2] An 8 Gbps SFP installed in Brocade 425 or 415 HBAs allows 2 or 4 Gbps speed only.

Using Brocade HBAs, you can connect your server (host system) to devices on the Fibre Channel SAN. The combined high performance and proven reliability of a single-ASIC design makes these HBAs ideal for connecting hosts to SAN fabrics based on Brocade Fabric or M-Enterprise operating systems.

NOTE
Brocade 804 mezzanine cards connect to the embedded switch modules or embedded interconnect modules on the Blade System chassis by way of an internal backplane and therefore, no optical modules (SFPs) are involved. With the exception of no SFPs, the Brocade 804 mezzanine FC HBA card functions the same as the other Brocade HBAs.

HCM software

The Host Connectivity Manager (HCM) is a management software application for configuring, monitoring, and troubleshooting Brocade HBAs, converged network adapters (CNAs) and FC mezzanine cards in a storage area network (SAN) environment.

The management software has two components:

- The agent, which runs on the host.
- The management console, which is the graphical user interface client used to manage the adapter.

The information in this guide is intended for OEMs, field service personnel, and customers who are installing Brocade hardware and HCM software. HCM can be installed in standalone and HP servers. For instructions about how to install the HCM software, refer to the *Brocade Adapters Installation and Reference Manual.*

You can manage the software on the host or remotely from another host. The communication between the management console and the agent is managed using JSON-RPC over HTTPS.

NOTE
All HCM, utility, SMI-S Provider, boot software, and driver installation packages, as well as the Driver Update Disk (DUD), are described in the *Brocade Adapters Installation and Reference Manual*.

HCM features

Common HBA management software features include the following:

- Discovery using the agent software running on the servers attached to the SAN, which enables you to contact the devices in your SAN.
- Configuration management , which enables you to configure local and remote systems. With HCM you can configure the following items:
  - Brocade 4 Gbps and 8 Gbps HBAs
  - HBA ports (including logical ports, base ports, remote ports, and virtual ports) associated with the local host
- Diagnostics, which enables you to test the adapters and the devices to which they are connected:
  - Link status of each adapter and its attached devices
  - Loopback test, which is external to the adapter, to evaluate the ports (transmit and receive transceivers) and the error rate on the adapter
  - Read/write buffer test, which tests the link between the adapter and its devices
  - FC protocol tests, including echo, ping, and traceroute
- Monitoring, which provides statistics for the SAN components.
- Security, which enables you to specify a CHAP secret and configure authentication parameters.
- Event notifications, which provide asynchronous notification of various conditions and problems through a user-defined event filter.

Tree node pop-up menus

You can use the HCM GUI main menu or the Brocade Command Line Utility (BCU) to configure, monitor, and troubleshoot your SAN components. The instructions for using each feature are detailed in subsequent chapters of this document. For each SAN component, you can optionally right-click its icon and a pop-up menu displays (see Table 2).

TABLE 2 HCM tree pop-up menus

SAN component	Pop-up menu feature
Host	Refresh All Start Polling Update Boot Image Change Agent Password Configure Names Basic Port Configuration Persistent Binding Statistics > Port Statistics Authentication Support Save Tree > Copy | Search | Collapse All | Expand All
Brocade HBA 4 Gbps or 8 Gbps	Refresh Define Name Update Boot Image Basic Port Configuration Persistent Binding Port Statistics Diagnostics Authentication Enable Adapter Tree > Copy | Search | Collapse All | Expand All
Port	Refresh Define Name Port Configuration > Basic | Advanced Virtual Port > Create | Delete Diagnostics FC-SP Enable Port Persistent Binding Statistics > Port | FCP IM Module | Fabric | IOC | QoS Tree > Copy | Search | Collapse All | Expand All
Base Port	Refresh Logical Port Statistics Tree > Copy | Search | Collapse All | Expand All
Device	Refresh Define Name Statistics > Target | FCP IM Tree > Copy | Search | Collapse All | Expand All

Adapter support

The HBAs are supported on the operating systems listed in Table 3.

TABLE 3 Adapter operating system support

Type of adapter	Description of adapter	Operating systems supported
HBA		
BR-415	4 Gbps HBA, 1 port	Linux, Windows, VMware, Solaris
BR-425	4 Gbps HBA, 2 port	Linux, Windows, VMware, Solaris
BR-804	8 Gbps HBA mezzanine card, 2 port	Linux, Windows, VMware
BR-815	8 Gbps HBA, 1 port	Linux, Windows, VMware, Solaris
BR-825	8 Gbps HBA, 2 port	Linux, Windows, VMware, Solaris

For a complete list of supported operating systems, refer to the *Brocade Adapters Installation and Reference Manual*.

For the latest support information, refer to the release notes for your adapter software version.

Chapter

Getting Started with HCM Software

2

In this chapter

HCM software launch

The following procedures describe how to launch the HCM application in Windows and Linux.

- "Launching the application on Windows platforms"
- "Launching the application on Linux platforms"

Launching the application on Windows platforms

After installing the HCM software, locate Brocade HCM on the Windows platform by selecting **Start > Programs > Brocade Adapter Software > Host Connectivity Manager.**

OR

Click the desktop icon to launch the application.

Figure 1 shows the screen that appears when HCM software is first launched.

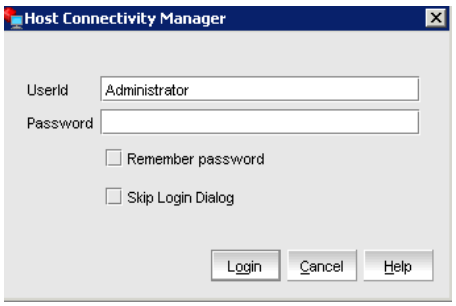


FIGURE 1 HCM Login dialog box

The factory default user ID and password are **Administrator** and **password**. After you log in for the first time, you should change the default password to a new one using the HCM GUI.

Launching the application on Linux platforms

After installing the HCM software, locate Brocade HCM on the Linux platform.

- If using a GNOME shell, double-click the **Host_Connectivity_Manager** icon to launch the application.
- If using a KDE shell, click the **Host_Connectivity_Manager** icon to launch the application.

OR

Start the application from the command prompt using the following commands:

```
suse116208:~ # cd /opt/brocade/adapter/client
suse116208:<installed directory>/adapter/client #
./Host_Connectivity_Manager
```

Remember password

The Login dialog has a check box to remember the password. If you check the **Remember password** check box, you do not need to enter the password the next time you launch the application.

Skip login

Take one of the following actions to manage the Skip Login feature.

- Enable **Skip Login** by checking the **Skip Login Dialog** check box.

  If the **Skip Login** check box is checked, it automatically disables the **Remember password** option.
- Disable **Skip Login** by setting `hba-application.skip-login=false` in the `/data/HBAApplication.properties` file.
- Select the **Skip Login** check box if you do not want the **Login** dialog box to appear the next time the application is started.

Changing an HCM application password

You can change the default password of the application to a different password using the **Change HCM Password** dialog box.

Note the following when you change a password:

- You must validate your user identity by supplying your old password before you can change to a new password. The new password must be different than the old password.
- The password can begin with an alphabetic, numeric, or special character.
- The default minimum and maximum length of the password is 8 and 64 characters. You can configure the password length in the `HBAApplication.properties` file:

  ```
  # min chars for the application password
  password_min=8
  #max chars for the application password
  password_max=64
  ```

- The password is encrypted and stored in the `noitacitnehtua.properties` file.

1. From the Host Connectivity Manager, select **Configure > Change Password > Change Password for HCM User**.

   The **Change HCM Password** dialog box, shown in Figure 2, displays.

FIGURE 2 Change HCM Password dialog box

2. Type the current password for the account. The default user name and password are **Administrator** and **password**.
3. Type the new password of the account.

   The new password must have at least one character different from the old password.
4. Retype the new password in the **Confirm New password** field.
5. Click **OK**.

NOTE
Both the user name and passwords are case-sensitive.

Changing an HCM agent password

You can change the default password of the agent to a different password using the **Change HCM Agent Password** dialog box.

Note the following when you change a password:

- You must validate your user identity by supplying your old password before you can change to a new password. The new password must be different than the old password.
- The password can begin with an alphabetic, numeric, or special character.
- The default minimum and maximum length of the password is 8 and 64 characters. You can configure the password length in the `HBAApplication.properties` file:

```
# min chars for the application password
password_min=8
#max chars for the application password
password_max=64
```

- The password is encrypted and stored in the `noitacitnehtua.properties` file.

1. From the Host Connectivity Manager, click **Configure > Change Password > Change Agent Password**.

   The **Change HCM Agent Password** dialog box, shown in Figure 3, displays.

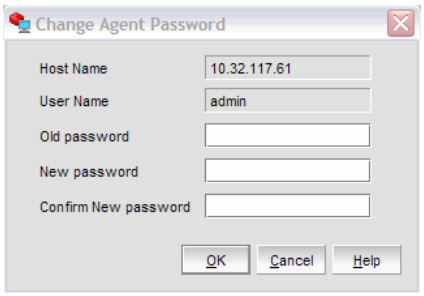


FIGURE 3 Change HCM Agent Password dialog box

2. Type the current password for the account. The default user name and password are **admin** and **password**.
3. Type the new password of the account.

   The new password must have at least one character different from the old password.
4. Retype the new password in the **Confirm New password** field.
5. Click **OK**.

NOTE
Both the user name and passwords are case-sensitive.

Software downgrade using Adapter Software Installer

Although driver and HCM downgrades are not supported, the following procedures are recommended for downgrading between versions 2.1, 2.0, and 1.1 of the Brocade adapter software. If you are not downgrading previous software versions, proceed to HCM software launch.

Downgrading HCM and driver or HCM only

To downgrade HCM and adapter drivers or HCM only, follow these steps, which are detailed in the following designated sections of the *Brocade Adapters Installation and Reference Manual*.

1. Uninstall HCM and drivers or HCM only using procedures detailed under "Software removal using Adapter Software Uninstaller."
2. When a message box displays asking to back up the HCM configuration, click **Yes** and proceed with the software removal. Refer to "HCM configuration data."
3. Install the desired version of the software using "Using the Adapter Software Installer."

   When the "Found Backed up data" message displays prompting you to restore old configurations, select restore the data and continue with the installation.

Downgrading driver only

Uninstall existing drivers using procedures under "Software removal using Adapter Software Uninstaller" in the *Brocade Adapters Installation and Reference Manual*.

Install new drivers using procedures under "Using the Adapter Software Installer" in the *Brocade Adapters Installation and Reference Manual.*

HCM configuration data

HCM configuration data is compatible between version 2.1, 2.0, 1.1, and 1.0 of the Brocade adapter software. Configuration data that is backed up when prompted during software removal with the Adapter Software Uninstaller and when using the HCM Backup dialog box includes the following:

The following application configuration files are backed up in the data directory:

- HBAApplication.properties
- SetupDiscovery.properties
- HbaAliasdb.properties
- log4j.xml
- noitacitnehtua.properties
- Syslog.properties
- Logging.properties

Backing up data after an uninstall

If you uninstall the Brocade HCM software, you are prompted to back up the application configuration data that was created during installation. Be sure to back up configuration data when the backup message displays during uninstallation. You can perform a backup on an as-needed basis.

Following are default locations for HCM configuration data.

- Versions 1.1.0.8 and above - <user home>\HCM\data
- Versions 1.1.0.6 and below - <installation location>\FC HBA\data

To restore the backed-up configuration data when you re-install the HCM, you must manually overwrite the new data directory contents with the backed-up data. This restores your previous settings.

Data restoration

You can use the Restore Data dialog box to restore data that has been previously backed up. The Host Connectivity Manager (HCM) stores the location and version details of the most recently-taken backed up data and automatically points to the location of the data.

NOTE
Use HCM 2.1 or later to restore backed up data. HCM 2.0 and earlier versions do not support the Restore Data feature.

The following data is restored:

- HBA application configuration data (HBAApplication.properties)
- HCM user authentication data (noitacitnehtua.properties)
- Alias Configuration data (HbaAliasdb.properties)
- Setup Discovery data (SetupDiscovery.properties)
- Syslog data (Syslog.properties)
- HCM Logging data (logging.properties and log4j.xml)
- SupportSave

Restoring backed up data

You must use HCM 2.1 or later to restore backed-up data.

1. Select the host, an HBA, or a port from the device tree.
2. Select **Tool > Restore Data** from the main menu.

   The **Restore Data** dialog box, shown in Figure 4, displays.

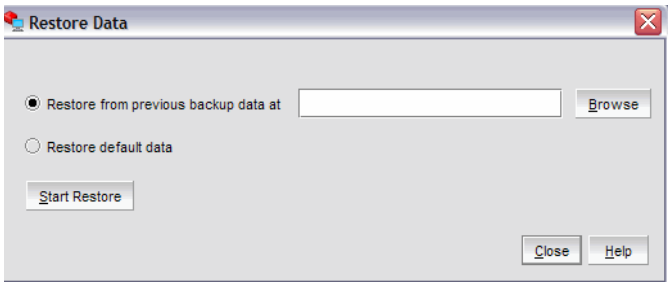


FIGURE 4 Restore Data dialog box

3. Click the **Restore from previous backup data at** button, and then click **Browse** and navigate to where the last backed up file resides.

   OR

   Click the **Restore default data** button. If you click this button, the **Browse** field is grayed out and the last restored data file is automatically retrieved.

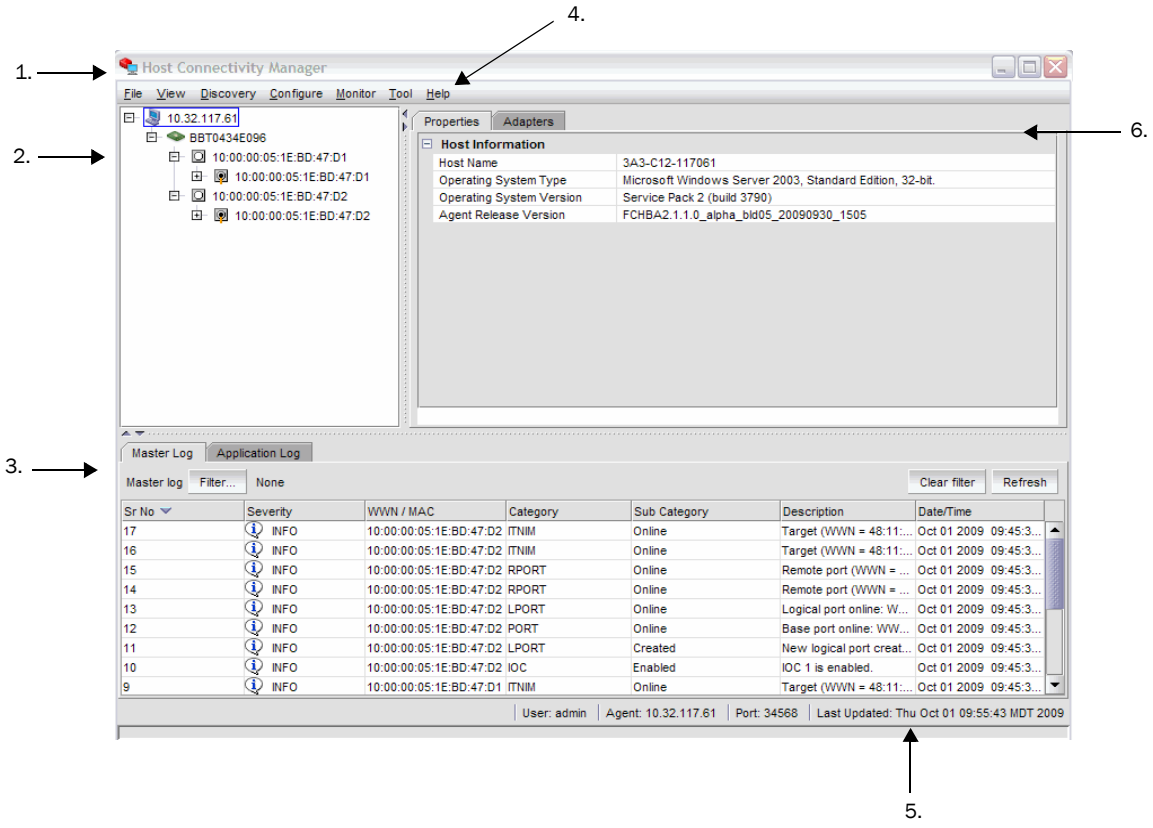
4. Click **Start Restore**.
5. Restart the HCM application for the restoration to take effect.

   The backed up data that you selected is restored.

HCM main window

From the Host Connectivity Manager main window, shown in Figure 5, you can manage all the adapters installed in this computer. Alternatively you can manage adapters installed in remote computers, if the computers are networked. Only one host can be managed at a time; multiple host management is not supported.

Refer to the *Brocade Adapters Installation and Reference Manual* for instructions on how to install both the driver and GUI, the driver only, or the GUI only.



1. Menu bar
2. Device tree window
3. Master Log
4. Online help
5. System information
6. Context view

FIGURE 5 Host Connectivity Manager main window

Legend Help menu

To display the HCM product icons and the event severity icons, select **Help > Legends** from the Host Connectivity Manager.

HCM product icons

On the left side of the Host Connectivity Manager, there is a navigation tree for representing the managed host with adapters and ports. Each tree node has an icon to represent the type of node. If the operational status is offline, link-down, or error, a small red diamond appears on the upper right corner of the icon.

Table 4 shows the product icons that represent the components that HCM manages.

TABLE 4 HCM product icons

Host (agent up)		Remote Port (Initiator) online	
Host (agent down)		Remote Port (Initiator) offline	
HBA online		Remote Port (Target) online	
HBA offline		Remote Port (Target) offline	
Port (with SFP) link up		Base Port (link up)	
Port (with SFP) link down		Base Port (link down)	
Port (without SFP) link up		Virtual Port (online)	
Port (without SFP) link down		Virtual Port (offline)	
Mezzanine card		LUN	
Pre-boot configured device		Beacon Status	

Event severity icons

Table 5 describes the icons that represent the four event types. Event filtering enables you to block events based on user-defined criteria (severity or type of log). Events that have been filtered out do not appear in the Master Log, For information about how to filter events, see "Filtering event log entries" on page 64.

TABLE 5 HCM Master Log icons

Icon	Description
	**Critical-level messages** indicate that the software has detected serious problems that will eventually cause a partial or complete failure of a subsystem if not corrected immediately; for example, a power supply failure or rise in temperature must receive immediate attention.
	**Major messages** represent conditions that do not impact overall system functionality significantly. For example, timeouts on certain operations, failures of certain operations after retries, invalid parameters, or failure to perform a requested operation.
	**Minor messages** highlight a current operating condition that should be checked or it might lead to a failure in the future. For example, a power supply failure in a redundant system relays a warning that the system is no longer operating in redundant mode and that the failed power supply needs to be replaced or fixed.
	**Information-level messages** report the current non-error status of the system components; for example, the online and offline status of a fabric port.

Discovery

Discovery enables you to contact the adapters present in a specified host in your SAN. The setup discovery profile is saved in the `SetupDiscovery.properties` file to remember the history of each host and related attributes of discovered hosts.

When you log in to HCM, the specified host is automatically contacted (discovered) and displayed on the navigation tree. By default, the local host is automatically contacted (discovered) and displayed on the navigation tree. When you configure and turn on discovery, the application discovers Brocade adapters in that host, connected to the SAN.

NOTE
The HCM application enables you to discover Brocade adapters, ports, virtual ports, remote ports, and LUNs using out-of-band discovery only.

Setting up out-of-band discovery for an adapter

When performing out-of-band discovery, you are managing the adapter remotely. The application connects to the agent running on the host server over the IP network and product information is copied back from the Brocade adapter to the server. If you do not configure the application to directly discover the devices, the connections and attached devices may not display correctly.

1. From the Host Connectivity Manager, click **Discovery > Setup**.

   The **Setup for Discovery** dialog box, shown in Figure 6, displays.

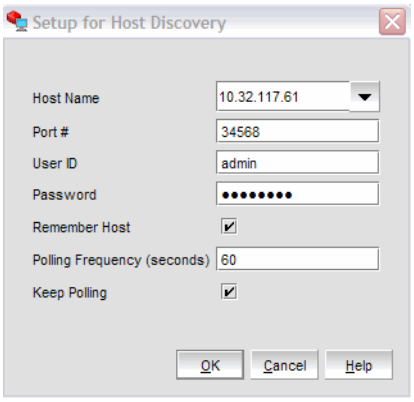


FIGURE 6 Setup for Discovery dialog box

2. From the **Host Name** list, select the host name from where you will discover the adapter.

   For the first time, the Host Name list will contain only the Local host. You must specify the host name or the IP address for discovering the remote servers. Only previously-discovered servers are available in the Host Name list.

3. Type the port number in the **Port Number** text box. The default is 34568.

4. Type in the user ID and password that will authenticate the SAN product with the agent. The default user ID and password are **admin/password**.

   It is recommended you change the agent password on the host for security reasons.

   NOTE
   Click the **Remember Host** check box if you do not want to type it in each time you set up discovery.

5. In the **Polling Frequency (seconds)** text box, specify the value for how frequently the application has to poll for newly discovered devices.

   All parameters related to the adapters that are installed in that server are refreshed each time the poll occurs.

   NOTE
   If the **Keep Polling** check box is checked, polling occurs after the specified polling interval. If the check box is not checked, polling stops.

6. Click **OK**.

Logging off HCM

End the HCM session using one of the following methods:

- From the Host Connectivity Manager, click **File > Exit**.
- Click the **X** in the upper-right corner of the HCM window to close it.

Chapter

Host Configuration

3

In this chapter

Host security authentication

Use the HCM GUI or the Brocade command line utility (BCU) to display the authentication settings and status. There are five well-known DH groups; however, only DH-CHAP group 0, called NULL DH, is supported in this release.

NOTE
Security authentication is not supported on Solaris platforms.

Configuring security authentication using HCM (Host and HBA)

You can access the **Fibre Channel Security Protocol Configuration** dialog box by selecting the Host, an HBA, or an HBA port from the device tree.

NOTE
Fibre Channel Security Protocol (FC-SP) is not available for Solaris platforms.

1. Select the appropriate device based on how you want to configure security authentication:
   - From the host level, select the host from the device tree.
   - From the HBA level, select the adapter from the device tree.
   - From an HBA port, select a port from the device tree.

2. Select **Configure > Authentication** from the main menu, or perform the appropriate following step to open the security authentication dialog box:

   - From the host level, right-click the host and select **Authentication** from the list.

     The **Fibre Channel Security Protocol Configuration** (host level) dialog box displays, as shown in Figure 7.

   - From the adapter level, right-click the adapter and select **Authentication** from the list.

     The **Fibre Channel Security Protocol Configuration** (adapter level) dialog box displays. This dialog box is identical to the **Fibre Channel Security Protocol Configuration** (host level) dialog box.

   - From the adapter port level, right click a port and select **FC-SP > Authentication** from the list.

   The **Fibre Channel Security Protocol Configuration** dialog at the host level displays.

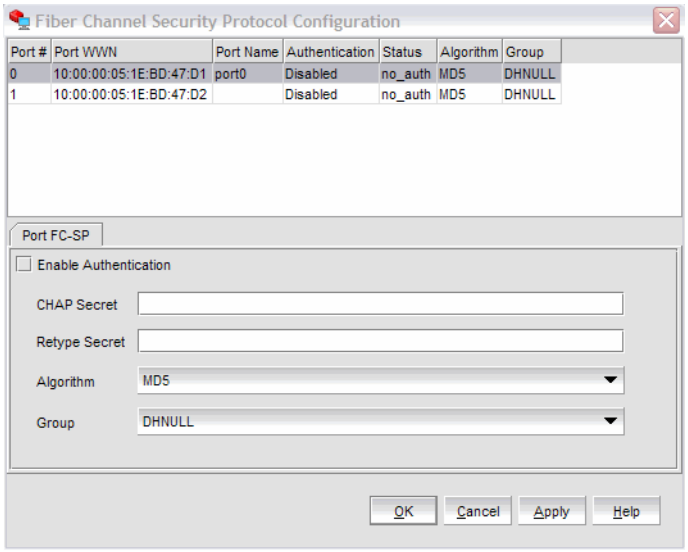


FIGURE 7 **Fibre Channel Security Protocol Configuration - host-level dialog box**

3. Configure the following parameters on the **Port Security Authentication** tab:
   a. Select the **Enable Authentication** check box to enable or disable the authentication policy.

      If authentication is enabled, the port attempts to negotiate with the switch. If the switch does not participate in the authentication process, the port skips the authentication process.

   b. Type and retype the secret.

      The maximum length of the secret is 63 bytes. The default secret for each interface is its port world wide name (PWWN) without the colons; for example, `0102030405060708`. Select the algorithm type from the list:

      - **MD5** - A hashing algorithm that verifies a message's integrity using Message Digest version 5.
      - **SHA1** - A secure hashing algorithm that computes a 160-bit message digest for a data file that is provided as input.
      - **MD5SH1** - Similar to the MD5 hashing algorithm, but used for DH-CHAP authentication.
      - **SHA1MD5** - Similar to the SHA1 hashing algorithm, but used for DH-CHAP authentication.

   c. Select **DHNULL** as the group value (this is the only group that is supported).
4. Click **Apply** to apply the changes.
5. Click **OK** to save the changes and close the dialog box.

Configuring security authentication using the BCU

Enter the following commands to display or configure security authentication for the ports:

- bcu auth --**algo** <*port_id*> <*md*|*sha1*|*ms*|*sm*>
- bcu auth --**policy** <*port_id*> {*on*|*off*}
- bcu auth --**secret** <*port_id*> "*secret_string*"
- bcu auth --**show** <*port_id*>
- bcu auth --**stats** <*port_id*>
- bcu auth --**statsclr** <*port_id*>

Refer to "auth" on page 128 for details about these commands.

Buffer credits

Buffer-to-buffer credit flow control is implemented to limit the amount of data a port sends, based on the number and size of the frames sent from that port. This scheme allows Fibre Channel to be self-throttling, thereby allowing it to establish a reliable connection without the need to accommodate dropped frames due to congestion. Buffer credit limits between each device and the fabric are communicated at the time of fabric login. One buffer credit allows a device to send one frame of data (typically 1 or 2 KB). Buffer credits cannot be configured on an adapter.

The default BB Credit is 1. The baseline for the calculation is one credit per kilometer at 2 Gbps. This yields the following values for 10 km:

- 5 credits per port at 1 Gbps
- 10 credits per port at 2 Gbps
- 20 credits per port at 4 Gbps
- 40 credits per port at 8 Gbps

Refer to the "Extended Fabrics concepts and planning" section of the *Fabric OS Administrator's Guide* for detailed information about buffer credits.

Basic port configuration

For each port, you can configure the following parameters using the **Basic Port Configuration** dialog box, the Brocade Command Line utility (BCU), or both. Table 6 lists the features and configuration options.

TABLE 6 Basic port configuration options

Port configuration parameter	Configurable using HCM	Configurable using the BCU	For more information
Port logging level	Yes	Yes	"Port logging level"
Configure speed	Yes	Yes	"Port speed"
Frame data field size	Yes	Yes	"Frame data field size"
Persistent Binding Note: The persistent binding option is available on Windows platforms only.	Yes	Yes	"Persistent binding"
QoS	Yes	Yes	"QoS"
Path Time Out Note: Path time out value (pathtov) is valid for firmware versions 2.0 and higher. It is not supported on the Solaris operating system.	Yes	Yes	"Path time out"
Target Rate Limiting	Yes	Yes	"Target rate limiting"

Opening the Basic Port Configuration dialog box

You can access the **Basic Port Configuration** dialog box, shown in Figure 8, by selecting the Host, an HBA, or an HBA port from the device tree.

NOTE
There are slight changes in HCM's **Basic Port Configuration** dialog box, depending on the operating system.

1. Select a device from the device tree.
2. Select **Configure > Basic Port Configuration** from the main menu.

   The **Basic Port Configuration** dialog box displays.

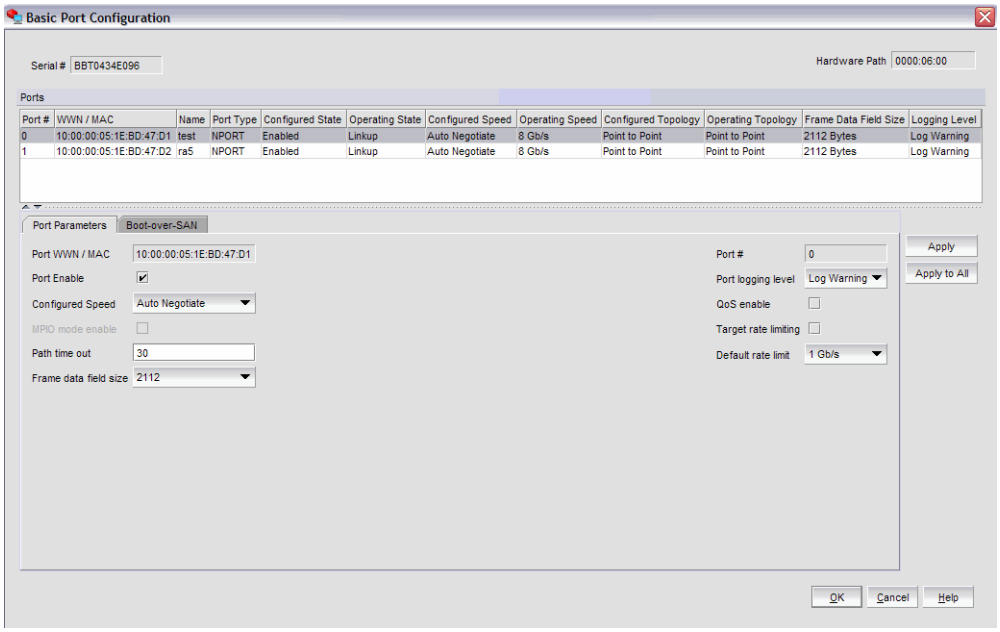


FIGURE 8 **Basic Port Configuration dialog box - Windows, Linux, and VMware**

Port logging level

The number of messages logged by the host depends on the predetermined logging level. Although the adapter might generate many messages, only certain types of messages are logged based on the specified logging level.

Configuring the port logging level using HCM

1. Select **Configure > Basic Port Configuration** from the Host Connectivity Manager.

   The **Basic Port Configuration** dialog box displays.

2. Select a value from the **Port Logging Level** list.

   Supported values are Log Critical, Log Error, Log Warning, Log Info, and Log Invalid.

3. Click **Apply** to apply the changes.
4. Click **OK** to save the changes and close the window.

Configuring the port logging level using the BCU

Enter the following command to set the logging level on the port.

bcu log –**level** <*port_id*> [<*level*>] [-m <fw|ha1|fcs|drv|aen|all>]

Refer to "log" on page 147 for details about this command.

Port speed

Port speed is the maximum amount of data that can pass through the port at a given second. The unit of measurement is in gigabits per second (Gbps). The available speed options depend on the HBA's speed and the port's SFP. Auto-negotiate is the recommended setting and it is the default.

Speed options for the 4 Gbps HBA (425 and 415) and the mezzanine card (804) are 1 Gbps, 2 Gbps, 4 Gbps, and 8 Gbps. The 8 Gbps HBA supports the 1 Gbps speed at the driver level, but it does not support 1 Gbps in a BIOS/BOS configuration.

Configuring the port speed using HCM

1. Select **Configure > Basic Port Configuration** from the Host Connectivity Manager.

   The **Basic Port Configuration** dialog box displays.

2. Select a value from the **Configured Speed** list.
3. Click **Apply** to apply the changes.

   A port disable/enable configuration dialog box displays, confirming the configured speed, which will take effect when the port is disabled or enabled.

4. Click **Yes** to continue, or **No** to cancel the operation.
5. Click **OK** to close the window.

Configuring the port speed using the BCU

Enter the following command to set the port speed.

bcu port –**speed** <*port_id*> [<*speed*>]

Refer to "port" on page 151 for details about this command.

Frame data field size

Buffer credits determine the maximum amount of frame data. If the number of buffer credits is not large enough to handle the link distance and speed, performance can be severely limited.

See "Buffer credits" on page 20 for information about buffer credits.

Specifying the maximum frame size using HCM

1. Select **Configure > Basic Port Configuration** from the Host Connectivity Manager.

   The **Basic Port Configuration** dialog box displays.

2. Select the frame size from the **Frame Data Field Size** list. Options include 512, 1024, 2048, 2112 Mbps and auto. The default value is 2112.
3. Click **Apply** to apply the change.
4. Click **OK** to close the window.

Configuring the frame data field size using the BCU

The **dfsize** command sets the ports maximum receive data field size. If you do not specify a value, the driver default receive buffer size displays, which is 2112.

NOTE
The new receive data field size takes effect when the port is re-enabled.

Enter the following command to set the frame data field size.

bcu port –**dfsize** <*port_id*> [<*dfsize*>]

Refer to "port" on page 151 for details about this command.

Persistent binding

Persistent binding enables you to permanently assign a system SCSI target ID to a specific FC device. Persistent binding can be achieved by binding to world wide port name (WWPN), world wide node name (WWNN), or device ID (DID).

You can access the **Persistent Binding** dialog box by selecting the Host or an HBA from the device tree.

Enabling and disabling persistent binding using HCM

Persistent binding can be enabled or disabled from the HCM GUI using the following steps:

1. Launch the **Basic Port Configuration** dialog box at the port level.
2. Check or uncheck the **Persistent Binding** check box in the **Basic Port Configuration** dialog box.

Enabling and disabling persistent binding using the BCU

Target persistent binding enables target port world wide name binding to a persistent target ID for the OS stack. Using the -list operand, you can query the list of mappings from the persistent binding module.

Enter the following commands to configure target persistent binding:

- bcu pbind --**list** <*port_id*> [<*pwwn*>]
- bcu pbind --**clear** <*port_id*>

Refer to "pbind" on page 150 for details about this command.

QoS

Quality of Service (QoS) works in conjunction with the QoS feature on Brocade switch F_Ports. The Fabric operating system (FOS) provides a mechanism to assign traffic priority (high, medium, or low) for a given source and destination traffic flow. By default, all flows are marked as medium.

This feature is supported only on 8 Gbps HBA ports installed on specific switch models that use Fabric OS 6.2 and later. The following licenses need to be installed on the switch connected to each HBA port (edge switch):

- Adaptive Networking (AN) license
- Server Application Optimization (SAO) license

To determine if these licenses are installed on the connected switch, execute the Fabric OS **licenseshow** command. Refer to the *Fabric OS Administrator's Guide* for detailed information about QoS.

Configuring QoS on the switch side using the BCU

On the switch side, you can create QoS zones using the PWWNs that correspond to devices in a source/destination traffic flow. You need a Server Application Optimization (SAO) license installed on the switch to enable QoS. In addition, an Adaptive Networking (AN) license is required on the switch to enable QoS on the switch ports.

You enable or disable QoS settings on ports with the **portCfgQos** command. Refer to the *Fabric OS Administrator's Guide* for details about this command on the switch side.

Configuring QoS on the HBA side using the BCU

There are three possible QoS states:

- Enabled, online - QoS is established with the switch.
- Enabled, offline - QoS negotiation failed and QoS was not established with the switch. Possible reasons for failure could be the license is not installed on the switch or QoS is not enabled on the port.
- Disabled.

NOTE
You must first enter the `bcu port --disable <port_id>` command, followed by the `bcu port --enable <port_id>` command, before the `bcu qos --enable` or `bcu qos --disable` commands take effect.

Enter the following commands to enable or disable QoS support on the HBA side:

- bcu qos –**enable** <*port_id*>
- bcu qos –**disable** <*port_id*>
- bcu qos –**query** <*port_id*>
- bcu qos –**stats** <*port_id*>
- bcu qos –**statsclr** <*port_id*>

Refer to "qos" on page 155 for details about this command.

Path time out

With path time out values (TOV), you can either force an immediate failover (by setting the TOV to 0) or you can specify a delay in seconds (1-60 seconds). The default TOV is 30.

Specifying path time out using HCM

1. Select **Configure > Basic Port Configuration** from the Host Connectivity Manager.

   The **Basic Port Configuration** dialog box displays.

2. Type a value in the **Path Time Out** field.
3. Click **OK** to close the window.

Specifying path time out using the BCU

Enter the following command to specify the optional path time out value in seconds (1 to 60). The default TOV is 10 seconds. A value of 0 is not allowed from the BCU.

bcu fcpim –**pathtov** <*port_id*> tov

Refer to "fcpim" on page 143 for details about this command.

Target rate limiting

The target rate limiting feature is used to minimize congestion at the adapter port caused by a slow drain device operating in the fabric at a slower speed. A remote port's operating speed is determined from the fabric, and then the information is used to throttle the transmitted traffic rate to that remote port. Traffic destined to the remote port is limited to its current operating speed.

Limiting the data rate to slower targets ensures that there is no buffer-to-buffer credit back-pressure between the switch due to a slow-draining target.

Enabling and disabling rate limiting on the adapter side using HCM

Target rate limiting is supported only when the adapter port is connected to the fabric. Therefore, target rate limiting is not supported when the port is directly connected with another device.

1. Select **Configure > Basic Port Configuration** from the Host Connectivity Manager.

   The **Basic Port Configuration** dialog box displays.

2. Enable the Target Rate Limiting feature by clicking the corresponding check box.
3. Select the default rate limit from the list. Options include 1 Gbps, 2 Gbps, and 4 Gbps; the default is 2 Gbps.
4. Click **OK** to close the window.

Enabling and disabling rate limiting on the adapter side using the BCU

Enter the following commands to enable or disable rate limiting on the adapter side:

NOTE
You must first enter the `bcu port --disable <port_id>` command, followed by the `bcu port --enable <port_id>` command, before the `bcu ratelim --enable` or `bcu ratelim --disable` commands take effect.

- bcu ratelim --**enable** <*port_id*>]
- bcu ratelim --**disable** <*port_id*>
- bcu ratelim --**query** <port_id>
- bcu ratelim --**defspeed** <port_id> [<1|2|4>]

Refer to "ratelim" on page 156 for details about this command.

Boot over SAN

Boot over SAN configuration using the **Basic Port Configuration** dialog box is enabled on all platforms if the HCM version is 1.1 or higher.

The Boot over SAN feature allows you to target remote boot devices (LUNs on SAN storage arrays) from which to boot the host system. When the host's operating system and adapter driver are installed on the remote device, the adapter BIOS and user-configurable boot instructions stored in adapter flash memory allow the host to boot from the device.

NOTE
Various operating systems require you to follow specific guidelines to enable servers to boot from a SAN. Understanding these requirements is key to a successful deployment of a boot over SAN environment.

Boot LUNs are identified to adapter ports using the BIOS Configuration Utility and BCU commands. These utilities also allow you to enable or disable BIOS for booting the host system over SAN, set boot options, and set the port speed. Refer to the *Brocade Adapters Installation and Reference Manual* for instructions.

BIOS boot over SAN provides the ability for x86 and x86_64 systems to perform booting of the OS installed on the SCSI disk connected over the Fibre Channel SAN.

The maximum number of supported adapters is limited to 16 and the maximum targets and LUNs that are displayed during discovery is limited to 256.

After you have configured boot devices using the BIOS Configuration Utility, you can enable or disable BIOS for Boot over SAN, set boot options, and set port speed using the HCM GUI. All configuration information is stored in flash memory.

Configuring Boot over SAN

The boot-LUN table lists the vendor information, LUN capacity, and whether the LUNs are accessible. These fields are not editable.

You can access the **Boot-over-SAN** dialog box by selecting the Host, an adapter or a physical port from the device tree.

1. Select **Configure > Basic Port Configuration** from the Host Connectivity Manager.

   The **Basic Port Configuration** dialog box displays.

2. Click the **Boot-over-SAN** tab.

   The **Boot-over-SAN** dialog box, shown in Figure 9, displays.

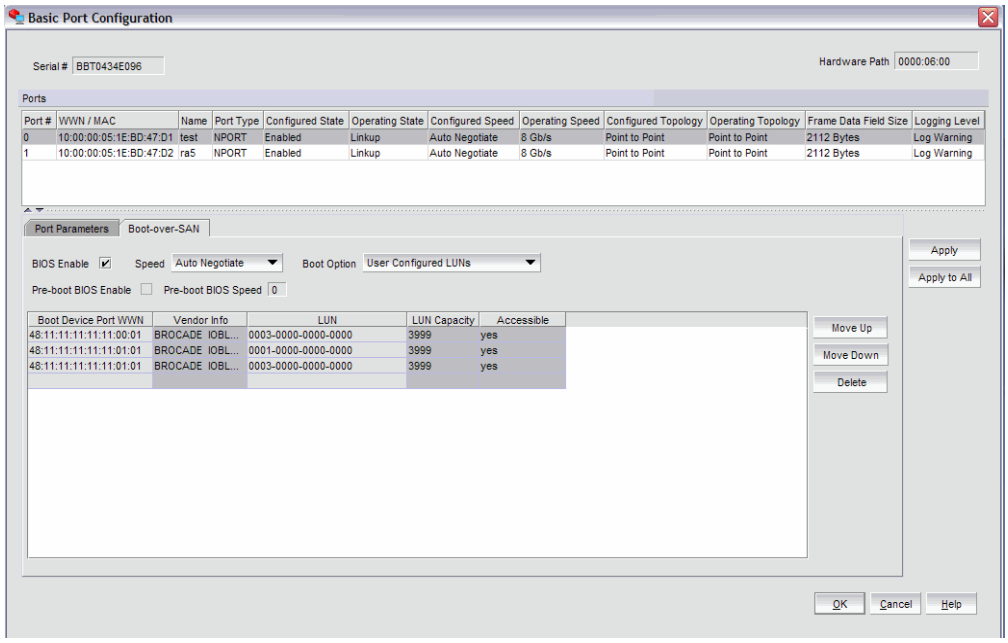


FIGURE 9 Boot-over-SAN dialog box

3. Click the **BIOS Enable** check box to enable Boot over SAN.
4. From the **Boot Option** list, select one of the following:
   - **Auto Discovered from Fabric** - Enables Boot over SAN using boot LUN information stored in the fabric. This is the default setting.
   - **First Visible LUN** - Enables Boot over SAN from the first discovered LUN in the SAN.
   - **User Configured LUNs** - Allows the user to select and prioritize the remote target and LUN for booting over SAN.
5. Select the Boot Device Port WWN row in the table, then click the up and down arrows to move the row up or down in the table. The host will attempt to boot from the first LUN in the table, and then move on to succeeding LUNs.
   - You can delete a row using the **Delete** button under the arrows.
   - Click the **Boot Device Port WWN** and **LUN** fields to physically enter boot LUNs to the table. These LUNs must be visible to the adapter to be accessible as boot LUNs.
6. Click **OK**.

   The Vendor Info, LUN Capacity, and Accessible status that correspond to the selected boot device and LUN display automatically.

Pre-boot configuration

Any parameters flagged with pre-boot were configured using a blade system management application. You cannot use HCM to create or modify a pre-boot configuration. If the port has been pre-boot enabled:

- The BIOS Enable option is disabled.
- The pre-boot configured LUNs in the LUN column are displayed as <LUN wwn> (Pre-boot), as shown in Figure 9. The maximum number of user-configured LUNs supported is four, and the maximum number of pre-boot-configured LUNs is eight.
- The configuration changes take affect after the next reset.

Configuring fabric-based boot LUN discovery

Use the following steps to configure fabric-based boot LUN discovery.

1. Set the adapter's BIOS configuration to auto-discovery using one of the following interfaces:
   - Brocade BIOS Configuration Utility

     Adapter Settings > Boot LUN > Auto Discover
   - HCM

     Refer to "Configuring Boot over SAN" on page 28 for instructions.
   - BCU

     bios --enable <port_id> -o auto
2. Enter the following BCU command to provide the zone name and zone members to use as operands in the Fabric OS zonecreate command.

   bcu boot --**blunZone** -c <cfg> -p <port_wwn> -r <rport_wwn> -l <lun_id | lun#>

   Refer to "boot" on page 133 for details about this command.
3. Configure the zone on the switch using the Fabric OS **zoneCreate** command. Refer to the *Brocade Adapters Installation and Reference Manual* or the *Fabric OS Administrator's Guide* for more information about creating zones.

Boot image update

You can update a boot image at the host level or at the adapter level.

At the host level, if the HCM version is lower than 2.1, the **Upload Boot Image** menu is enabled only when one HBA is visible. If the agent version is 2.1 and higher, the **Upload Boot Image** menu is always enabled if at least one adapter is visible and will update the image to all visible adapters.

Uploading the boot image using HCM

1. Download the boot code (brocade_adapter_boot_fw_v2-1-1-0) from www.brocade.com/hba to a folder on your local drive.
2. Launch HCM.
3. Right-click a host or adapter from the device tree and select **Upload Boot Image** from the list.
   - Right-clicking a host downloads the boot image to all adapters that are installed on the host.
   - Right-clicking an adapter downloads the boot image to the selected adapter only.

   The **Upload Boot Image** dialog box displays.
4. Click the **Browse** button and navigate to the location of the boot image.
5. Select the boot image and click **Open**.

   The selected file downloads. If an error occurs during the downloading process, an error message displays.

Updating the boot image using the BCU

Enter the following command to update the boot image.

bcu boot --**update** [adapter_id] <image_file> [-a]

Refer to "boot" on page 133 for details about this command.

Virtual port configuration

Virtual ports (V_Ports) appear to the hosts as physical ports in the data network. One or more virtual ports are assigned to each host, and a host can access storage at a virtual port only if the virtual port has been assigned to the host.

Virtual port restrictions

- You cannot create a V_Port that already exists in the **Names** dialog box. If you need to re-create a V_Port that has been deleted through an interface other than the currently-managing HCM or the V_Ports deleted on Linux servers reboot, you must first manually remove the V_Port's WWN from the **Names** dialog box in HCM. If you do not manually remove the V_Port from HCM, an error message displays that the V_Port already exists. See "Removing a name entry" on page 40 for instructions on how to manually remove a V_Port.
- The HCM GUI should post an error message for duplicate VPorts (detected in the Vports.db file) and prompt the user to remove the duplicate, but it does not. Duplicate world wide names are not restricted when the BCU is used to create V_Ports. Do not use the BCU for virtual port management, because it does not handle duplicate V_Port world wide names. Instead, use only the HCM GUI to manage vPorts.

Creating a virtual port

You create virtual ports on HBA ports only; virtual ports are not supported on an adapter. Virtual ports are not supported for VMware and Solaris agents.

1. Select a physical HBA port from the device tree.
2. Select **Configure > Virtual Port > Create** from the main menu.

   OR

   Right-click the physical port and select **Virtual Port > Create** from the list.

   The **Virtual Port Creation** dialog box, shown in Figure 10, displays. The following fields are system-generated:

   - Physical port world wide name.
   - Virtual port world wide name - This WWN must be unique.
   - Virtual node world wide name - The system returns the default node WWN, which is the physical port node WWN.

NOTE
By default, the **Use auto-generated** check box is selected and the **Generate Again** button is enabled. You can still edit the **Virtual Port WWN** field if **Use auto-generated** is selected.

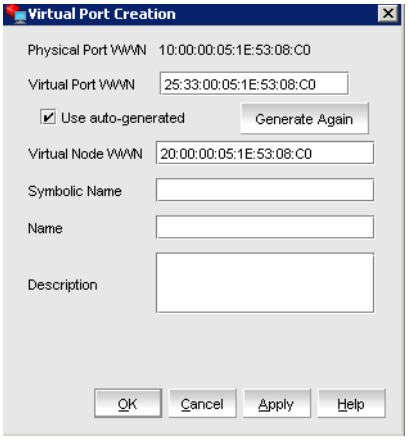


FIGURE 10 Virtual Port Creation dialog box

3. (*Optional*). Provide a symbolic name for the virtual port.
4. (*Optional*). Provide an alias name for the virtual port. By creating an alias, you can assign a familiar name to a device or group multiple devices into a single name. This can simplify cumbersome data entry and allows an intuitive naming structure.
5. (*Optional*). Enter descriptive information about the virtual port into the **Description** field.
6. Click **OK** to apply the changes and close the window.

Deleting a virtual port

If the maximum number of virtual ports have already been created, the option to create virtual ports using HCM is disabled.

NOTE
Pre-boot-created virtual ports are not labeled. If the virtual port is pre-boot-created, the **Delete** check box is disabled.

1. Select a virtual port from the device tree.
2. Select **Configure > Virtual Port > Delete** from the main menu.

   OR

   Right-click the virtual port and select **Virtual Port > Delete** from the list.

   A warning message displays, asking for confirmation.
3. Click **OK** to continue.

   The **Virtual Port Deletion** dialog box displays.

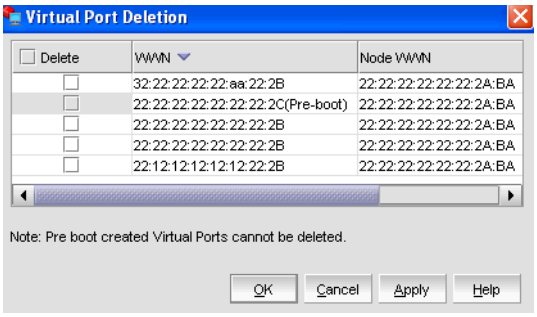


FIGURE 11 Virtual Port Deletion dialog box

4. Click the check box that corresponds to one or multiple virtual ports you want to delete, and click **OK**.

HCM logging levels

You can set the log level for the following modules:

- Agent communication log, where all messages are exchanged between the HCM GUI application and the HCM agent.
- HCM debug log, where messages are logged locally.

If you do not set an HCM log level, DEBUG, which is the default, is used.

Configuring the HCM logging level using HCM

1. Select **Configure >HCM Logging Levels** from the Host Connectivity Manager.

   The **Configure HCM Logging Levels** dialog box, shown in Figure 12, displays.

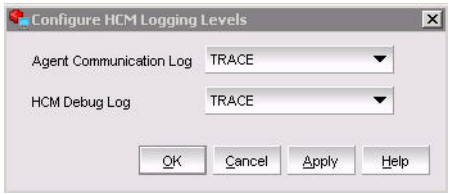


FIGURE 12 Configure HCM Logging Levels dialog box

2. From both the **Agent Communication Log** and the **HCM Debug Log** lists, select one of the following:
   - Trace
   - Debug, the most verbose and the default
   - Info
   - Warning
   - Error
   - Fatal, which is the least verbose.
3. Click **Apply** to apply the change.

Advanced port configuration

You can access the **Advanced Port Configuration** dialog box by selecting an HBA port from the device tree.

For each port, you can configure the following parameters using the **Advanced Port Configuration** dialog box, the Brocade Command Line utility (BCU), or both. Table 7 lists the features and configuration options.

TABLE 7 Advanced port configuration options

Port configuration parameter	Configurable using HCM	Configurable using the BCU
Interrupt Control Coalesce	Yes	Yes
Interrupt Control Latency	Yes	Yes
Interrupt Control Delay	Yes	Yes

Opening the Advanced Port Configuration dialog box

1. Select an HBA port from the device tree.
2. From the Host Connectivity Manager, select **Configure > Port Configuration > Advanced.**

   The **Advanced Port Configuration** dialog box, shown in Figure 13, displays.

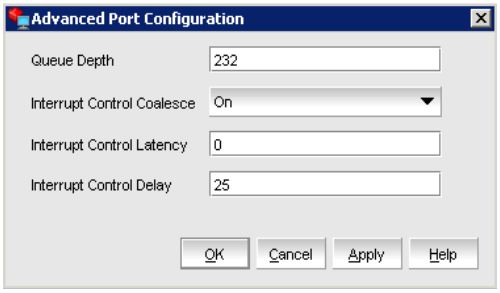


FIGURE 13 Advanced Port Configuration dialog box

Interrupt Control Coalesce

Interrupt control coalescing allows the system to optimize CPU utilization by varying the number of interrupts generated. Increasing the latency monitor timeout value should result in a lower interrupt count and less CPU utilization, which may result in higher throughput.

You can configure the following interrupt control coalescing parameters per port:

- Interrupt delay time - The host interrupt generation is delayed by the specified duration to coalesce multiple I/O interrupt events into one. Increasing this value results in fewer interrupts per multiple interrupt events.
- Interrupt latency timer - This value helps to minimize I/O latency by avoiding host interrupt generation to have to wait until the interrupt delay has expired for an I/O throughput.

Configuring the Interrupt Control Coalesce using HCM

1. Select a port from the device tree.
   - From the Host Connectivity Manager, select **Configure > Advanced Port Configuration.**

     The **Advanced Port Configuration** dialog box displays.

     OR
   - Right-click a port and select **Port Configuration > Advanced**.
2. Set the latency and delay values:
   - Select **On** from the **Interrupt Control Coalesce** list.

     NOTE
     Interrupt Control Coalesce is **On** by default.
   - Specify the latency monitor timeout value in microseconds, if coalesce is set to on. Latency timeout values supported are 0-225 microseconds for all HBAs, including the Brocade 804 mezzanine card. Setting the latency timeout value to 0 disables the latency monitor time out interrupt.
   - Specify the delay timeout value in microseconds, if coalesce is set to on. Delay timeout values supported are 0-1125 microseconds for all HBAs, including the Brocade 804 mezzanine card. Setting the delay timeout value to 0 disables the latency monitor time out interrupt.
3. Click **OK**.

Name configuration

The Host Connectivity Manager allows you to configure names as a method of providing familiar, simple names to world wide names for adapters, ports, virtual ports, and remote ports in the SAN. (A logical port can be a base port or a virtual port.) Only unique names are allowed.

NOTE
You can access the **Define Names** dialog box by right-clicking an adapter, port, remote port, or Virtual Port. You can access the **Configure Names** dialog box by selecting an HBA, an HBA port, or a Virtual Port from the device tree.

You can perform the following name tasks using either the Configure Names dialog or the Define Names dialog:

- Associate a name that represents an adapter, port, virtual port, or remote port. Note the following points about names:
  - Among all adapters, two cannot have duplicate names.
  - Among all the ports, two cannot have duplicate names.
  - A port and adapter can have the same name.
  - You cannot associate a name for a storage device.
  - Name changes on remote ports and virtual ports are sent to the *.properties file local to the HCM application but are not sent to the agent.
- Add a detached WWN and an associated name with Type and operational status as Unknown.
- Remove or disassociate a name from a WWN.

Dual role changes

Dual role types were introduced in HCM release 1.1 for situations where an Initiator WWN acts as a Target. In HCM release 2.0, the design was changed to use a MAC or WWN + Type combination, enabling you to set your own name to the port (Initiator) as well as to a remote port (Target).

Since HCM release 2.1, the dual role type has been eliminated, so if you import a data file from an HCM release 2.0 or earlier which has a Dual Role type, the WWN is imported as an "Unknown" type and the application log displays "Dual Role" type is not supported.

If the name you imported already exists in the **Configure Names** dialog box, the **Fix Duplicates** dialog box displays, showing the duplicated names. Refer to "Importing duplicated names" on page 43 for more information.

Name validation

Note the following when you define a name:

- The name cannot begin with a number.
- The name cannot begin with an underscore (_) or hyphen (-), however an underscore or hyphen character is allowed within the name; for example, name1_name-2.
- No special characters are allowed, except for an underscore or hyphen.
- The maximum length of the name is 15 characters.
- The maximum length of the description is 80 characters.

Defining a name

The **Define Name** dialog box, shown in Figure 14, enables you to assign a name to an existing world wide name (WWN) or media access control (MAC) address.

1. Select an adapter from the device tree.
2. Select **Configure > Define Names** from the Host Connectivity Manager.

   OR

   Right-click a device from the device tree and select **Define Names**.

   The **Define Name** dialog box displays.

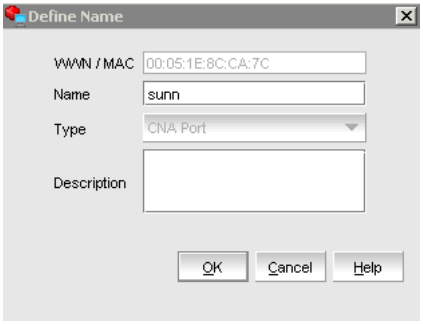


FIGURE 14 Define Name dialog box

3. Enter a meaningful name for the selected adapter or port.

   NOTE
   Tye type of device is displayed in the **Type** field. The drop-down list is disabled.

4. Enter a description of the device.
5. Click **OK**.

Editing the name fields

Only the name, the world wide name (WWN), and the description fields are editable. Depending on the component, the following occurs when you edit the name fields:

- Name changes on the adapter and ports are sent to the agent and stored in the *.properties file.
- Name changes on remote ports and virtual ports are sent to the *.properties file local to the HCM application but are not sent to the agent.

1. Select a host, adapter, or port from the device tree.
2. Select **Configure > Names** from the Host Connectivity Manager.

   OR

   Right-click a device from the device tree and select **Configure > Names**.

The **Configure Names** dialog box, shown in Figure 15, displays all the discovered and detached (undiscovered) names.

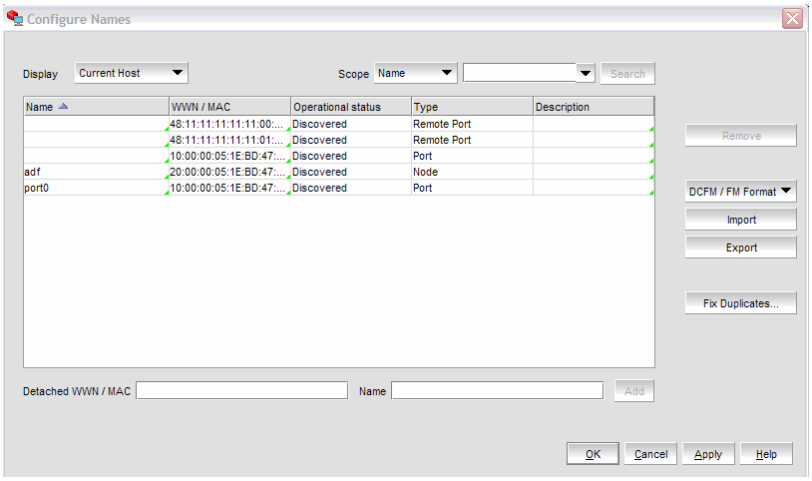


FIGURE 15 Configure Names dialog box

3. Select a row and edit the name, the WWN, and the description, as needed.
4. Click **OK**.

Adding name entries

You can add up to 2000 names which are then stored in the `HbaAliasdb.properties` file. The entries persist during reboot.

1. Select an HBA, an HBA port, or a Virtual Port from the device tree.
2. Select **Configure > Names** from the Host Connectivity Manager.

   OR

   Right-click a device from the device tree and select **Configure Names.**
3. Type a name that represents an adapter, port, or storage device into the **Name** field.
4. Type a valid WWN that corresponds to the name. Valid WWW types are as follows:
   - Node
   - Port
   - Remote Port
   - V_Port
   - Unknown
5. Click **OK** to close the window.

   The new component is added to the **Name** list.

Removing a name entry

The Remove functionality clears the name and description values of a selected detached WWN.

1. Select an HBA, an HBA port, or a Virtual Port from the device tree.
2. Select **Configure > Names** from the Host Connectivity Manager.

   OR

   Right-click a device from the device tree and select **Configure > Names**.

   The **Configure Names** dialog box displays all the names available at the host.
3. Select one of the following from the **Display** list:
   - Current Host
   - All WWNs
   - Only Nodes
   - Only Ports
   - Only V_Ports
   - Only Remote Ports

   A list of names for the devices you selected displays.
4. Select a device to highlight it and click the **Remove** button to remove the discovered device from the list.

   The **Remove** button clears the names of the discovered WWN and the entire row of the detached (undiscovered) WWN.
5. Click **OK** to close the window.

Exporting the properties for a WWN

You can export the properties for a world wide name in .csv, *.properties, or .txt file format.

1. Select an HBA, an HBA port, or a Virtual Port from the device tree.
2. Select **Configure > Names** from the Host Connectivity Manager.

   OR

   Right-click a device from the device tree and select **Configure > Names**.

   The **Configure Names** dialog box displays.
3. Select one of the following from the **Display** list:
   - Current Host
   - All WWNs
   - Only Nodes
   - Only Ports
   - Only L_Ports
   - Only V_Ports
   - Only Remote Ports

4. Click the **Export** button.

   The **Save** dialog box displays. You can save the properties file in .txt, .csv, or .properties format.

5. Name the file, and click **Save**.
6. Click **OK** to close the window.

Importing the properties for a WWN

Complete the following steps to import WWN properties.

1. Select **Configure > Names** from the Host Connectivity Manager.

   OR

   Right-click a device from the device tree and select **Configure Names**.

   The **Configure Names** dialog box displays.

2. Select one of the following from the **Display** list:
   - Current Host
   - All WWNs
   - Only Nodes
   - Only Ports
   - Only Remote Ports
3. Click the **Import** button.

   The **Open** dialog box displays.

4. Navigate to the location of the *.properties file from which you will import properties for the selected device.
5. Name the properties file, and click **Open**.
6. Click **OK** to close the window.

Importing properties in EFCM format

You can use this procedure to import properties in Enterprise Fabric Connectivity Manager (EFCM) format.

1. In the **Configure Names** dialog box, select **EFCM Format** and then select **Import**.
2. Navigate to the location of the *.properties file from which you will import properties for the selected device.

   The format appears as follows.

```
# Names Export File V 1.0 : DO NOT DELETE / MOVE / MODIFY THIS LINE
# For each row in the file the name should be followed by an '='
# Column Format: WWN=Name=Type =Description
# EFCM Names file Format [ Delimiter '=' ]
#########################################################################
200000051e536b20=s=Node=
200000051e536b43=bfa0=Node=
100000051e536b20=a=Port=
100000051e536b44=bfa0_port1=Port=
100000051e536b43=bfa0_port0=Port=
```

3. Click **OK**.

Importing properties in DCFM or FM format

You can use this procedure to import properties in Data Center Fabric Manager (DCFM) or Fabric Manager (FM) format.

1. In the **Configure Names** dialog box, select **DCFM/FM Format** and then select **Import**.
2. Navigate to the location of the *.properties file from which you will import properties for the selected device.

   The format appears as follows:

```
# Names Export File V 1.0 : DO NOT DELETE / MOVE / MODIFY THIS LINE
# For each row in the file the name should be followed by an ','
# Column Format: WWN,Name,Type ,Description
# FM Names file Format [ Delimiter ',' ]
#########################################################################
200000051e536b20,s,Node,
200000051e536b43,bfa0,Node,
100000051e536b20,a,Port,
100000051e536b44,bfa0_port1,Port,
100000051e536b43,bfa0_port0,Port,Adding a name and a WWN
```

3. Click **OK**.

Importing duplicated names

The **Duplicated Names** dialog box, shown in Figure 16, displays when you import a file with a duplicate name.

1. Select **Configure > Names** from the Host Connectivity Manager.

   OR

   Right-click a device from the device tree and select **Configure Names**.

   The **Configure Names** dialog box displays.

2. Import a file with duplicate names in the **Configure Names** dialog box.

   The **Duplicated Names** dialog box displays.

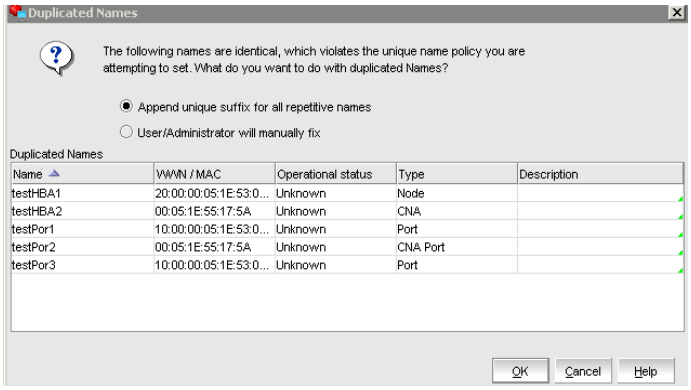


FIGURE 16 Duplicated Names dialog box

3. Determine which method you will use to fix the name policy violation, and click the appropriate button.

   - **Append unique suffix for all repetitive names** - Click to instruct the software to add incremental numbers to fix the duplicated names.
   - **User Administrator will manually fix** - Change duplicate names using the procedure in "Editing the name fields" on page 38.

4. Click **OK**.

NPIV

N-Port ID Virtualization (NPIV) enables a single Fibre Channel protocol port to appear as multiple, distinct ports. NPIV provides separate port identification within the fabric for each operating system image (partition) behind the port, as if each operating system image had its own unique physical port.

Each NPIV device has a unique virtual port ID (PID), port WWN, and node WWN. The virtual port has the same properties as an N_Port and is therefore capable of registering with all services of the fabric. In other words, multiple virtual devices emulated by NPIV appear no different than regular devices connected to a non-NPIV port. The maximum number of virtual PIDs for an N_Port on a FC switch is 255.

NPIV is available at the physical port level or at the virtual fabric level. If virtual fabric ports are detected, then you cannot configure NPIV parameters at the physical port level. If virtual fabric ports are deleted on the switch port side, the NPIV parameters can then be configured at the physical port level. No settings are available for V_Ports from basic port configuration.

Chapter

4

Monitoring

In this chapter

Performance monitoring

The Host Connectivity Manager (HCM) **Port Statistics** window enables you to monitor the performance of the adapter and the traffic between the adapter and the LUNs. You can use the information to isolate and troubleshoot areas that impact application performance.

Table 8 lists the port statistics that are monitored by component. Refer to Appendix A, "HCM Dialog Boxes" for a description of each statistics field.

TABLE 8 Statistics monitored by component

Component	Statistics monitored
Local host	• Port
HBA	• Port
HBA port	• Port • FCP IM Module • Fabric • IOC • QoS
Logical port and remote port	• Logical port
Virtual port	• Logical port • Virtual port
Device* *No statistics are available for LUNs	• Remote port > Target statistics • Remote port > FCP IM statistics

Polling frequency rate

The faster the polling rate, the more quickly the HCM GUI receives indications from the host. However, faster polling rates consume more of your system's CPU and network resources and can therefore slow the system.

Controlling the polling frequency rate

To control port statistics polling, do one of the following from any of the **Statistics** dialog boxes.

1. Click the **Start Polling** check box to manually poll the port statistics.
2. Type the polling rate in the **Polling Frequency in Seconds** field. The range is between 5 and 3600 seconds. The default is 5 seconds.
3. Click the **Stop Polling** check box to stop port statistics polling.
4. Check the **Keep Running Data** check box to see the trend.

Resetting statistics

1. Click the **Reset** button on any of the **Statistics** dialog boxes.

   A warning dialog box, shown in Figure 17, displays.

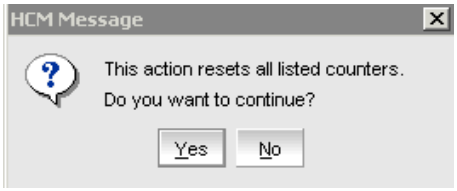


FIGURE 17 Reset statistics warning

2. Click **Yes**.

   All of the statistics are reset to **0**.

Master log

Event monitoring enables early fault detection and isolation on a selected adapter. When applicable events occur during adapter operation, the adapter driver generates event messages. These messages are captured in your host system logs. These messages are also captured in an agtEvent.log file by the HCM agent and displayed in the HCM master log. Note that message display may differ in your host system log and the HCM master log; however, messages will most likely contain the following information:

- Message ID
- Description
- Severity level
- Event category
- Cause of event
- Recommended action
- Date and time event occured

Message details are also contained in HTML files, which load into your system when you install the adapter driver. You can view these HTML files using any internet browser application. Refer to the *Brocade Adapters Troubleshooting Guide* for details of all driver event messages.

NOTE
To avoid processing of older events in first-time event discovery, an event will be considered for processing if it has occurred within the last 20 seconds, or not greater than the discovery interval. The agent and the HCM GUI application must be running in the same time zone and at the right time.

The **Master Log Properties** dialog box, described in Table 9, displays a list of all events that have occurred. See Table 5 on page 14 for a description of the event severities.

You can filter the events based on the user-defined criteria shown in Figure 18.

TABLE 9 Master Log fields

Field	Description
Filter button	Click to launch the **Master Log Filter** dialog box.
Clear Filter button	Click to clear the master log filter option set.
Sr No column	Displays a numbering sequence in ascending order.
Severity column	Displays the event severity (informational, minor, major, or critical).
WWN/MAC column	Displays the world wide name (WWN) or the media access control (MAC) address of the device on which the event occurred.
Category column	Displays the category of event, based on one of the following categories: • Adapter • Port • LPort • RPort • ITNIM • Audit • IOC
Subcategory column	Displays the subcategory of the main category.
Description column	Displays a brief description of the event.
Date/Time column	Displays the date and time when the event occurred.

Filtering event log entries

Event filtering enables you to block events based on user-defined criteria (severity or type of log). Events that have been filtered out do not appear in the Master Log

1. Click the **Filter** button in the **Master Log** section of the bottom pane.

   The **Master Log Filter** dialog box displays.

2. Filter the events using one or a combination of the criteria shown in Figure 18.

NOTE
The Category is the type of event. The categories are listed in Table 9.

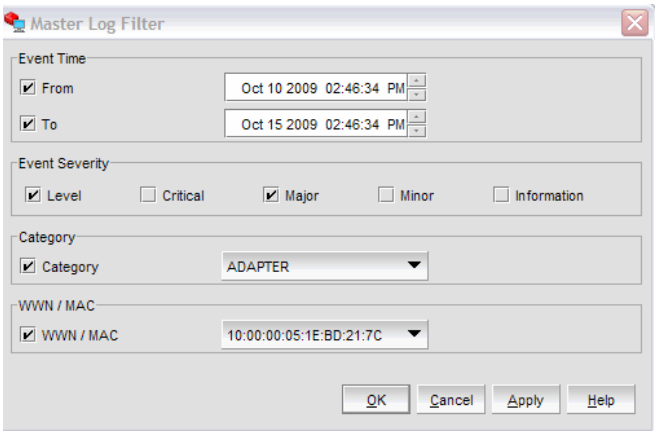


FIGURE 18 Master Log Filter dialog box

3. Click **Apply** to save your changes, or click **Cancel** to exit the window.

   OR

   Click **OK** to save the changes and exit the window.

Application log

The HCM application log, shown in Figure 19, displays all application-related informational and error messages, as well as the following attributes:

- Date and time the message occurred
- Severity of the message
- Description of the message
- The agent IP address

NOTE
Run-time memory information is logged in the application log whenever a supportSave is triggered from HCM or when the **About** dialog box is launched in HCM.

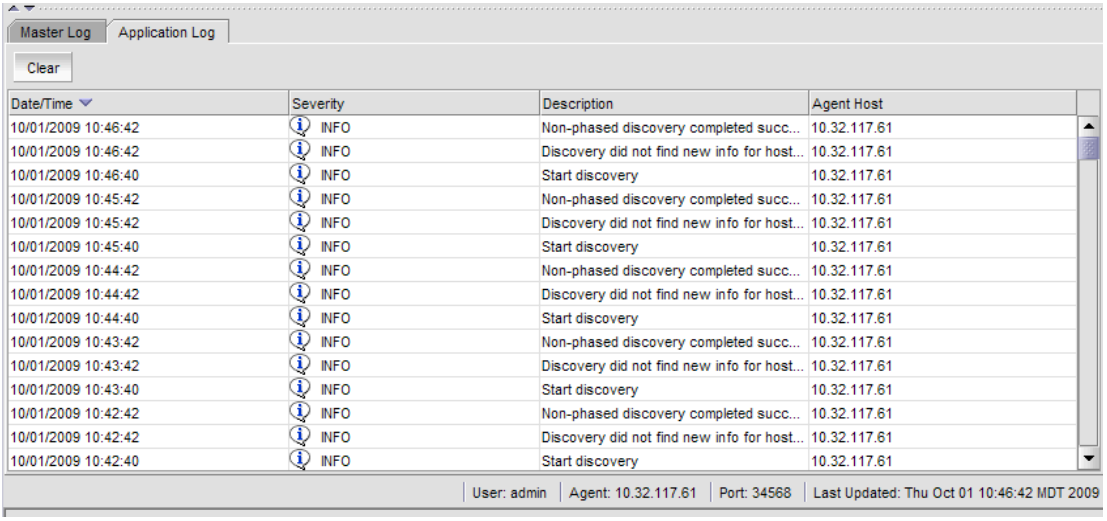


FIGURE 19 HCM Application Log

Syslog support

Syslog forwarding is the process by which you can configure the Host Connectivity Manager (HCM) agent to send Syslog messages to other computers through port 514. You can configure the HCM agent to forward events to a maximum of three Syslog destinations. These events will display in the operating system logs.

The HCM stores all the received events from the driver in the agtEvent.log file. By default, the location is `/opt/hcmagent/log/hbaEvents.log` in Linux and Solaris systems.

NOTE
VMware ESX 3.5 and 4.0 blocks the Syslog outgoing port 514 by default. Therefore, you must configure the firewall if you use VMware ESX 3.5 or 4.0 and plan to use Syslog Host Configuration feature in DCFM or if you access HCM through DCFM. See "Syslog host configuration using VMware" on page 52 for more information.

Opening the Syslog Server Configuration dialog box

1. Select the host, an adapter, or a port from the device tree.
2. Select **Configure > Syslog** from the main menu.

   The **Syslog Server Configuration** dialog box, shown in Figure 20, displays.

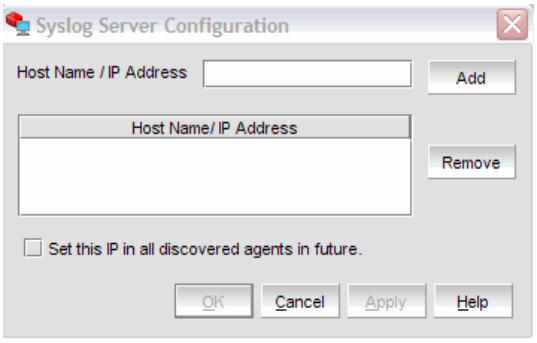


FIGURE 20 **Syslog Server Configuration dialog box**

Registering a host server

You can register up to three Syslog destinations on managed Fabric OS devices.

1. Select **Configure > Syslog** from the main menu.

   The **Syslog Server Configuration** dialog box displays.
2. Enter the host name or IP address of the destination device into the **Host Name/IP Address** field.
3. Click **Add** to register the host as a Syslog destination.
4. Click **OK** to close the dialog box.

Removing a host server

1. Select **Configure > Syslog** from the main menu.

   The **Syslog Server Configuration** dialog box displays.
2. Enter the host name of the destination device into the **Hostname** field.
3. Enter the IP address of the destination device into the **IP Address** field.
4. Click **Remove** to remove the host as a Syslog destination.
5. Click **OK** to close the dialog box.

Syslog host configuration using VMware

VMware ESX 3.5 and 4.0 blocks the Syslog outbound port 514 by default. Therefore you must configure the firewall to allow outgoing port 514 for Syslog if you plan to use the Syslog host configuration feature in DCFM or if you access HCM through DCFM.

Use the following procedure if the outgoing UDP port 514 is blocked by the VMware ESX firewall.

1. Restart the HCM Agent if the firewall settings on port 514 change in VMware.
2. Use the following command to open port 514:

   ```
   esxcfg-firewall -o 514,udp,out,syslog
   ```
3. Use the following command to block outgoing traffic through port 514:

   ```
   esxcfg-firewall -c 514,udp,out,syslog
   ```

Chapter

5

Diagnostics

In this chapter

Diagnostics using the BCU

The purpose of diagnostic commands is to evaluate the integrity of the system hardware. Be sure to disable the port before running any type of port diagnostics. In addition, it is advisable that you do not perform other operations on the adapter while running HCM or BCU diagnostics.

NOTE
You must disable the port prior to executing the loopback test. You must disable the adapter prior to executing the memtest.

diag commands

The **diag** commands shown in Table 10 monitor hardware components and can be performed while the system is running (they are non-disruptive). Refer to "diag" on page 137 for command details.

NOTE
The **sfpshow** and **beacon** commands are not applicable for Brocade 804 mezzanine cards.

TABLE 10 Fibre Channel diag commands

Command	Description
beacon	Blinks the appropriate port LED for physical identification. Beaconing can occur at the port or the link level. End-to-end (E2E) beaconing is a software feature that can be enabled on Brocade 8 Gbps HBAs to allow the local HBA to flash (beacon) and also cause the connected Fibre Channel switch port to uniquely beacon. Refer to the *Brocade Adapters Installation and Reference Guide* for details on E2E beaconing patterns.
loopback	Tests the data path from the IOC to the desired network loopback port (internal, serdes, external) and back. This is an offline diagnostic test.
memtest	Tests the adapter's memory blocks.
pciloopback	Checks the communications path between the host and the IO Controller (IOC).
queuetest	Tests the CPE/RME queue.
sfpshow	Displays small form factor pluggable (SFP) information.
tempshow	Displays the temperature of the adapter.

fcdiag commands

Fibre Channel diagnostics include the tests shown in Table 11. Refer to "fcdiag" on page 141 for details about this command.

TABLE 11 Fibre Channel diagnostic tests

Command	Description
fcping	Determines the basic connectivity between the Fibre Channel network points and monitors and measures network latency.
fctraceroute	Reports on a SAN path, including node hops and latency data.
fcecho	Sends an FC Echo Extended Link Services (ELS) request to a remote port.
linkbeacon	Blinks the LED light of the remote port of the link.
scsitest	Tests the SCSI components.

Diagnostics using HCM

The purpose of diagnostic commands is to evaluate the integrity of the system hardware. Be sure to disable the port(s) before running any type of port diagnostics. In addition, it is advisable that you do not perform other operations on the adapter while running HCM or BCU diagnostics.

NOTE
When you invoke a test on an adapter, you can run diagnostics for one or both ports within the selected adapter.

Running a hardware-level test using HCM

1. Select an adapter or an adapter port from the device tree.
2. Select **Configure > Diagnostics** from the main menu.

   OR

   Right-click the component and select **Diagnostics** from the list

   The **Diagnostics** dialog box, shown in Figure 21, is displayed.

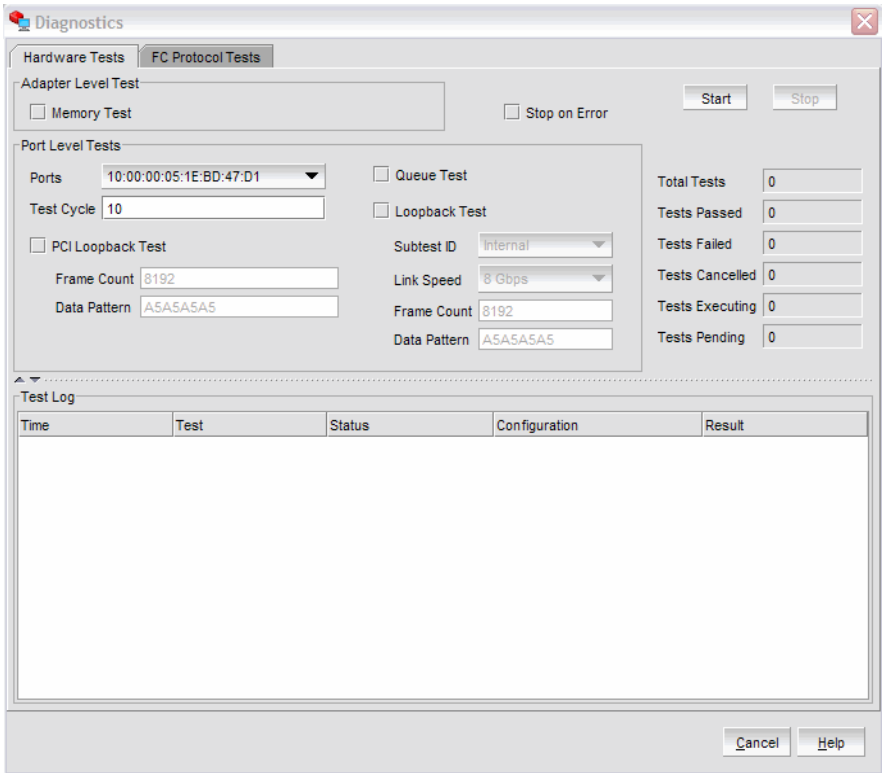


FIGURE 21 Hardware-level diagnostics tests dialog box

3. Click the check box that corresponds to the port test you are running.
4. Specify the parameters based on parameter information found in Table 12.

NOTE
Click the **Stop on Error** check box if you want the test to stop running if an error occurs.

5. Click **Start** to run the test.

Hardware-level test parameters

TABLE 12 Hardware-level test parameters

Hardware-level test	Parameter	Test Options
Memory test **NOTE:** During the test, IOC will be disabled.	None	You can enable or disable this test. Regardless of test cycle set value, the Memory Test will run only once.
PCI loopback test	Frame Count	Integer from 0 - 4,294,967,295. The default value is 8192.
	Data Pattern	Default value is A5A5A5A5.
	Test Cycle	The number of times the test runs. The default value is 10.
Port loopback test **NOTE:** For an External Loopback test, you must plug in the loopback connector. For a Brocade 804 mezzanine card, a pass-through module is required for an External Loopback test.	Subtest ID	• Internal • External • Serdes
	Link Speed	2, 4, and 8 Gbps
	Frame Count	Integer from 0 - 4,294,967,295. The default value is 8192.
	Test Cycle	The number of times the test runs. The default value is 10.
	Data Pattern (hexadecimal)	Default value is A5A5A5A5.
Queue test Sends a health check message from host to firmware through message queues memory mapped over the PCI.	You can enable or disable this test.	Queue number from 0-3. Because HCM only allows you to enable or disable the queue test (and not specify an integer), all the queues will be tested.

Running a Fibre Channel protocol-level test using HCM

There are three protocol-level tests:

- Echo test, which sends an FC Echo ELS to a remote port.
- FC ping test, which requests the management server to test the connectivity with a given remote port (without zoning restrictions). Not supported in Solaris operating systems.
- FC traceroute test, which requests to enumerate the route between two given end points. Not supported in Solaris operating systems.

To run one of the protocol-level tests, use the following procedure.

1. Select an adapter or port from the device tree.
2. Select **Configure > Diagnostics** from the main menu.

   OR

   Right-click the component and select **Diagnostics** from the list.

   The **Diagnostics** dialog box, shown in Figure 22, displays.
3. Click the **FC Protocol Tests** tab.

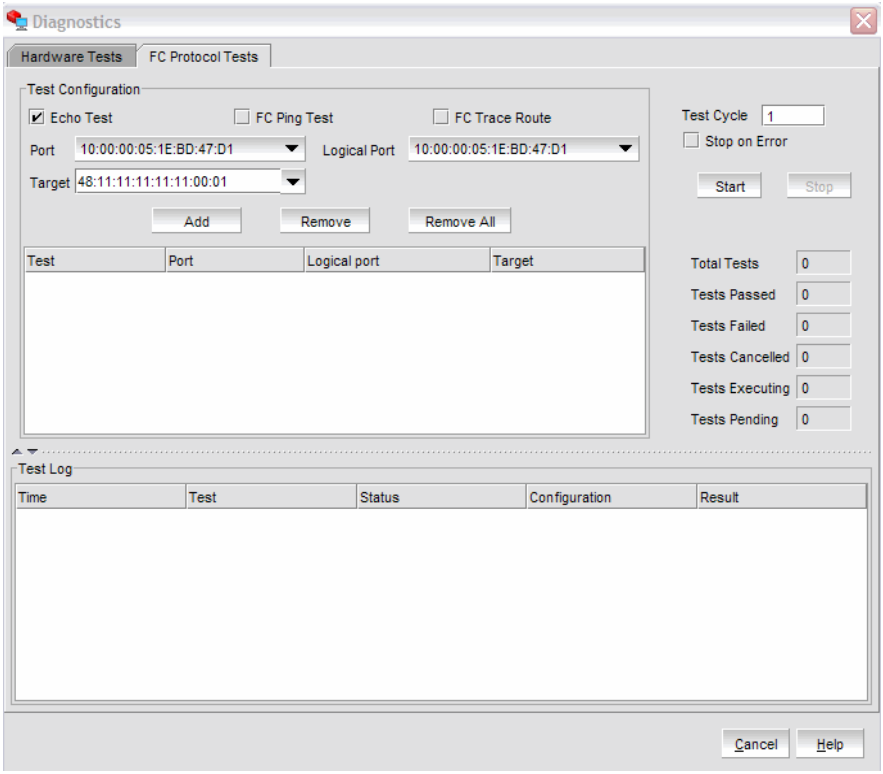


FIGURE 22 **Protocol-level diagnostic tests dialog box**

4. Click the check box that corresponds to the protocol test you are running.
5. Select a port, target, and logical port from the lists, and click **Add** to add it to the test table.
6. Define how many times the test runs by specifying the test cycle number. The default test cycle number is 1.
7. Click **Start** to run the test.

Displaying test log details

1. Select **Configure > Diagnostics** from the Host Connectivity Manager.
2. Run any diagnostic test.
3. Select and double-click a row of the test results in the bottom pane.

   The **Test Log** Details dialog box, shown in Figure 23, displays.

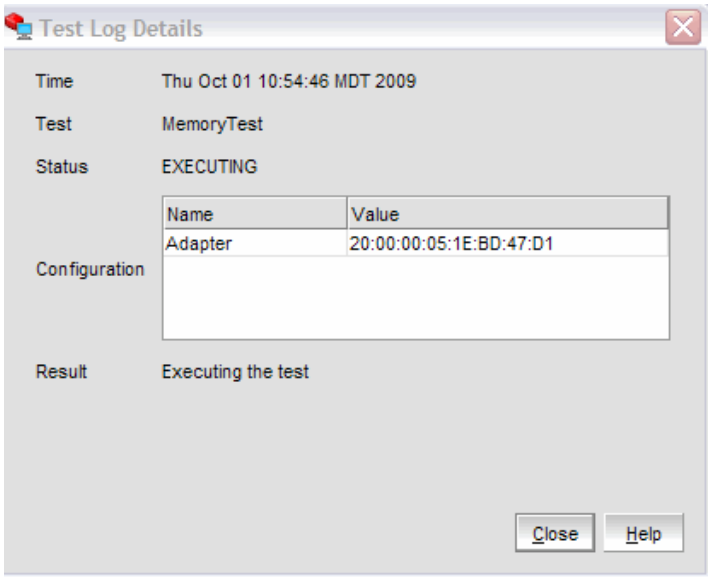


FIGURE 23 Test Log Details for Echo Test dialog box

Beaconing

Beaconing is a continuous signaling of error conditions on a LAN. Beaconing can occur either on the port or on one or both sides of the link (known as end-to-end beaconing). Link end-to-end beaconing provides a mechanism to start beaconing on both the adapter side and the switch side.

NOTE
Port beaconing is not supported on the Brocade 804 mezzanine card.

Configuring beaconing using HCM

You can configure beaconing from an HBA port.

1. Select an HBA port from the device tree.
2. Select **Configure > Beacon** from the Host Connectivity Manager.
3. Click either the **Port** check box or the **Link** check box to enable the feature.

Configuring beaconing using the BCU

Enter the following command to blink the appropriate port LED for physical identification.

bcu diag --**beacon** <*port_id*> {*on* | *off*} [-t <*secs*>]

where:

duration — Blinks the local port for the specified number of seconds. The default is 0, which means infinite blinking.

Refer to "diag" on page 137 for details about this command.

Enter the following command to blink the appropriate link for physical identification.

bcu fcdiag --**linkbeacon** <*port_id*> {*on*|*off*}

Refer to "fcdiag" on page 141 for details about this command.

SFP management

The **Port SFP** dialog box enables you to display the properties that are associated with a selected small form-factor pluggable (SFP) transceiver.

Displaying SFP information using the BCU

Enter the following command to view the SFP information. If the firmware detects a non-Brocade SFP, the port is disabled.

bcu diag –**sfpshow** <*port_id*>

Refer to "diag" on page 137 for details about this command.

Displaying SFP information using HCM

NOTE
Brocade 804 mezzanine cards connect to the embedded switch modules or embedded interconnect modules on the Blade System chassis by way of an internal backplane and therefore, the SFP properties do not apply to the Brocade 804 mezzanine card.

1. Select a port in the device tree.
2. Click the **SFP** tab in the right pane.

   The **SFP Properties** panel, shown in Figure 23, displays.

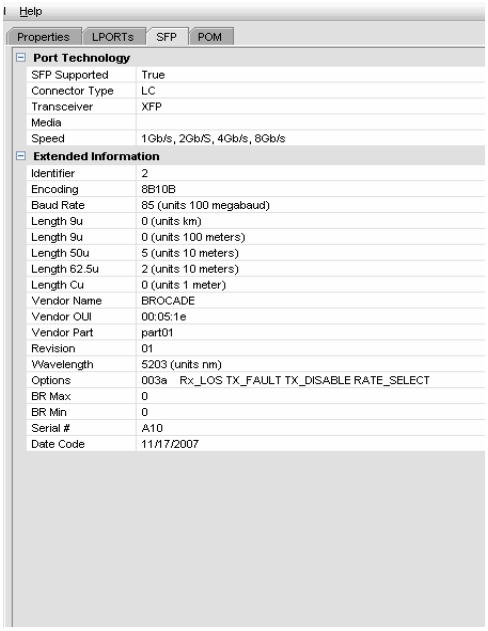


FIGURE 24 SFP Properties panel

Details about the port technology and extended link are described in "SFP Properties panel" on page 107.

Debugging

The following **debug** commands capture all the support information needed to diagnose suspected system issues:

- **portlog**

  Displays the log of FC frames and other main control messages that were sent out and received.

- **portlogclear**

  Clears the port's frame log.

- **portlogctl**

  Enables or disables the portlog.

Refer to "debug" on page 135 for details about these commands.

supportSave

The supportSave command collects debug information needed from the driver. You can collect supportSave information using the **bfa_supportsave** command or through the Data Center Fabric Manager (DCFM). HCM supportSave contains driver, agent, and HCM-related information.

NOTE
Before collecting data using the supportSave feature, you may want to disable auto-recovery on the host system. This is because when adapters are reset after an auto-recovery from a failure, traces initiated before the failure can be lost or overwritten.

The captured debug information can be saved to the local filesystem and then sent to the supplier for further investigation. The information that is captured is detailed in Table 13.

TABLE 13 supportSave categories

supportSave level	Captured information
System (or Host)	HCM GUI-related engineering logs Events Configuration files Operating-specific information Environment information Data.xml file Vital CPU, memory, network resources HCM Agent (logs, configuration) Driver logs (bfa_supportSave output) Install logs Core files

The default location to where supportSave output is saved is under the IP address of the host from which it was collected, relative to the HCM installation directory, as follows:

USER HOME\HCM\data\10.32.116.1\supportsave

For example:

C:\Users\Administrator\HCM\data\10.32.116.1\supportsave

supportSave collection sources

Table 14 lists the sources from which you can gather supportSave information.

TABLE 14 supportSave collection sources

Source of supportSave information	supportSave information collected
BFA based supportSave[1]	Driver-related logs and config files
Browser-based supportSave	Driver-related logs and config files Agent log/config files
HCM-based supportsave	Agent log and config files HCM GUI log and config files

[1] bcu debug does not support the bcu debug --supportsave command. See "supportSave collection using a command prompt" on page 63 for more information.

Automatic statistics collection

The port statistics log file is collected as part of the supportSave activity.

Port statistics collection occurs every eight hours and will be logged in to a rolling file under the `/log/` directory. There are a maximum of five backup files and each file has a 100 KB size limit. A new backup file overwrites the oldest file.

supportSave collection using HCM

There are two ways to trigger a supportSave collection using the HCM GUI, explained in this section. You can also gather supportSave information for the adapter using the DCFM application. For information about supportSave using DCFM, refer to the *Data Center Fabric Manager User Manual*.

1. Select **Tool > Support Save** from the Host Connectivity Manager.

   OR

   Right-click a host from the device tree and select **Support Save** from the list.

   NOTE
   If the agent is up, it will use the advanced configuration. If there is no agent, it will use the basic configuration.

   After the supportSave operation completes, the following message is displayed:

   Support Save Completed and is located at

   `<HCM HOME Dir>/data/localhost/supportSave_Basic_<file_name>.zip`

2. Click **OK** to close the dialog box.

supportSave collection on a port crash event

If the port crashes and triggers a port crash event, support save data is collected at a system-wide level. An application log message is generated with the following message:

```
Port Crash Support Save Completed
```

Port crash events have a CRITICAL severity and you can view the details in the Master Log and Application Log tables in HCM. For more information, refer to "Master log" on page 47 and "Application log" on page 50.

supportSave collection using a command prompt

The **bcu debug** command does not support the **bcu debug –supportsave** command. The **bfa_supportsave** command, however, supports the following options:

- **bfa_supportsave** - To create and save the supportsave at /tmp.
- **bfa_supportsave_dir** - To create and save the supportsave under <dir>.
- **bfa_supportsave <dir> <ss_file_name>** - To create and save the supportsave under <dir> as the file name <ss_file_name>. If <ss_file_name> already exists, it will be overwritten.

supportSave collection using a browser

You can use an Internet browser (Internet Explorer 6 or higher or Firefox 2.0 or higher) to collect and transfer supportSave information for the driver and the HCM agent.

Use a browser if you do not have root access, if you do not have access to file transfer methods such as FTP and SCP, or you do not have access to the Host Configuration Manager (HCM) or the Data Center Fabric Manager (DCFM).

1. Open an Internet browser and type the following URL:

   `https://localhost:34568/JSONRPCServiceApp/SupportSaveController.do`

   In this URL, *localhost* is the IP address of the server from which you want to collect the bfa_supportSave information.

2. Type the agent's credentials using the factory default settings, `admin` and `password`.

   The **File Download** dialog box displays, prompting you to save the `supportSaveController.do` file.

3. Click **Save** and navigate to the location where you want to save the bfa_supportSave file.

4. Rename the `supportSaveController.do` file as a zip file, using .zip as the extension. Use IZArc or winzip to unpack the file and analyze the contents.

Appendix

HCM Dialog Boxes

A

In this appendix

A In this appendix

Authentication Statistics dialog box

The **Authentication Statistics** dialog box enables you to display statistical information related to transmitted and received DH-CHAP attempts for a selected port.

Opening the dialog box

1. Select an HBA port from the device tree.
2. Select **Configure > FC_SP > Authentication Statistics** from the Host Connectivity Manager.

Fields and components

Field	Description
Date	The date the statistics were run.
Failures	The number of times security authentication failed.
Successes	The number of times security authentication succeeded.
Tx Auth Rjts	The number of rejected transmitted Fibre Channel authentication attempts.
Tx Auth Negs	The number of transmitted Fibre Channel authentication negotiation attempts.
Tx Auth Dones	The number of completed Fibre Channel authentication negotiation attempts.
Tx DHCHAP Challenges	The number of transmitted DH-CHAP challenge attempts.
Tx DHCHAP Replies	The number of transmitted DH-CHAP replies.
Tx DHCHAP Successes	The number of times a transmitted Fibre Channel authentication attempt was successful.
Rx Auth Rjts	The number of rejected received Fibre Channel authentication attempts.
Rx Auth Negs	The number of received Fibre Channel authentication negotiation attempts.
Rx Auth Dones	The number of completed received Fibre Channel authentication attempts.
Rx DHCHAP Challenges	The number of received DH-CHAP challenge attempts.
Rx DHCHAP Replies	The number of received DH-CHAP replies.
Rx DHCHAP Successes	The number of times a received DH-CHAP challenge was successful.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Configuring security authentication using HCM (Host and HBA)"
- "Port Statistics dialog box"
- "Polling frequency rate"
- "Resetting statistics"
- "Performance monitoring"

Backup dialog box

The **Backup** dialog box allows you to create a backup of data and configuration files.

Opening the dialog box

Select any device from the device tree and select **Tool > Backup Data** from the Host Connectivity Manager.

Fields and components

Field	Description
Output Directory text box	Enter the location of the directory in which you want to back up the data and configuration files.
Browse button	Click to browse to the location of the backup directory.
Start Backup button	Click to instruct the system to back up the data and configuration files to the designated location.
Close button	Click to close and exit the **Backup** dialog box.

Base Port Properties panel

The **Base Port Properties** panel enables you to display the properties that are associated with the base port.

Opening the properties panel

1. From the device tree, select a base port.
2. In the right pane, click the **Base Port Properties** tab.

Fields and components

Field	Description
Base Port	Indicates whether the port is a base port (true or false).
Fabric Name	The name of the Fabric associated with the base port.
FC Address	The Fibre Channel address of the base port.
Node WWN	The world wide name of the device.
Port WWN	The world wide name of the base port.
Roles	The role of the base port; for example, FCP Initiator.
State	Indicates whether the base port is online or offline.
Switch IP Address	The IP address of the switch.
Symbolic Name	The symbolic name associated with the base port.

Change HCM Password dialog box

The **Change HCM Password** dialog box enables you to change an existing password for the application.

Opening the dialog box

Select **Configure > Change HCM Password** from the Host Connectivity Manager.

Fields and components

Field	Description
User Name	Type your user name.
Old password	Type your existing password.
New password	Type a new password.
Confirm New password	Confirm your new password by retyping it.

Using the dialog box

Refer to the following topic for specific procedures using this dialog box:

- "Changing an HCM application password"

Change HCM Agent Password dialog box

The **Change HCM Agent Password** dialog box enables you to change an existing password for the host.

Opening the dialog box

Select **Configure > Change Password > Change Agent Password** from the Host Connectivity Manager.

Fields and components

Field	Description
Host Name	Displays the IP address of the host.
User Name	Type your user name.
Old password	Type your existing password.
New password	Type a new password.
Confirm New password	Confirm your new password by retyping it.

Using the dialog box

Refer to the following topic for specific procedures using this dialog box:

- "Changing an HCM application password"

Configure Names dialog box

The **Configure Names** dialog box enables you to add a world wide name and an associated name for an adapter, port, or storage device that is not yet discovered. You can also remove a device from the Name display list and import from or export properties to a file.

Opening the dialog box

1. Select any device from the device tree.
2. Select **Configure > Names** from the Host Connectivity Manager.

Fields and components

Field	Description
Display list	Select a discovered host from the list. **Current Host** is the default.
Name	The name for all configured devices. **NOTE:** You can also search for a name by typing the name into the text box and clicking **OK**.
Scope list	The type of name; options include the Name itself or the WWN. After you have selected the type of name from the Scope list, type the name or WWN into the corresponding text box.
WWN/MAC	The world wide name for all configured devices. **NOTE:** You can also search for a name by typing the world wide name into the text box and clicking **OK**.
Operational Status	The operational status of the WWN/MAC (for example, Discovered).
Type	The type of device; for example, Node or Port.
Description	Displays a description of the device.
Remove button	Select a device to highlight it, then click the Remove button to remove the discovered device from the list.
Import	Click to import properties from a properties file for a selected device.
Export	Click to save properties to a properties file for a selected device.
Add button	For undiscovered devices, type in the name of the port's name or the WWN and click the **Add** button to add it to the Display list.
DCFM/FM format list	Select from the list to import properties in DCFM (Data Center Fabric Manager), FM (Fabric Manager), or EFCM (Enterprise Fabric Connectivity Manager) format.
Fix Duplicates button	Click to fix any duplicate names.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Name configuration"
- "Adding name entries"
- "Removing a name entry"
- "Exporting the properties for a WWN"
- "Importing the properties for a WWN"

Define Name dialog box

The **Define Name** dialog box enables you to assign a name to an existing world wide name.

Opening the dialog box

1. Right-click on an HBA or a port in the device tree.
2. Type a name that represents the adapter or port.

   NOTE
   The WWN and the Type are not editable.

3. Click **OK** to apply the change and close the window.

   The new component is added to the **Name** list.

Fields and components

Field	Description
WWN/MAC	The world wide name for the device.
Name	Enter a meaningful name for the device.
Type	The type of device; for example, Node or Port.
Description	Enter a description of the device.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Name configuration"
- "Adding name entries"
- "Removing a name entry"
- "Exporting the properties for a WWN"
- "Importing the properties for a WWN"

Duplicated Names dialog box

The **Duplicated Names** dialog box enables you to display configured names that are redundant.

Opening the dialog box

The **Duplicated Names** dialog box displays when you import a file with a duplicate name.

1. Select **Configure > Names** from the Host Connectivity Manager.

   OR

   Right-click a device from the device tree and select **Configure Names**.

   The **Configure Names** dialog box displays.

2. Import a file with duplicate names in the **Configure Names** dialog box.

   The **Duplicated Names** dialog box displays.

Fields and components

Field	Description
Append unique suffix for all repetitive names button	Click to automatically add an incremental number to a duplicate name.
User/Administrator will manually fix button	Click if you want to manually fix a duplicate name.
Name	The port number with which the duplicated name is associated.
WWN/MAC	The world wide name or media access control address with which the duplicated name is associated.
Operational Status	The operational status of the duplicate WWN (for example, Discovered).
Type	The type of device; for example, Node or Port.
Description	A description of the duplicate name.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Name configuration"
- "Adding name entries"
- "Removing a name entry"
- "Exporting the properties for a WWN"
- "Importing the properties for a WWN"

Event Properties dialog box

The **Event Properties** dialog box displays the properties associated with a selected event from the Master Log.

Opening the dialog box

1. Click the **Master Log** tab, located on the bottom pane of the Host Connectivity Manager.

   A master summary of events on all discovered devices is displayed.

2. Double-click an event.

Fields and components

Field	Description
Date/Time	The date when the event occurred.
Time	The time when the event occurred.
Severity	The event severity (informational, minor, major, or critical).
WWN/MAC	The world wide name (WWN) or media access control (MAC) of the device on which the event occurred.
Event ID	An identifier that corresponds to the event.
Category	The category of event; for example, Rport or ITNIM.
Description	A brief description of the event.
Root Cause	The root cause of the event.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Master log"
- "Event severity icons"
- "Filtering event log entries"

Fabric Statistics dialog box

The **Fabric Statistics** dialog box enables you to view statistics on a selected Fabric.

Opening the dialog box

1. Select a port from the device list.
2. Select **Monitor > Statistics > Fabric Statistics** from the Host Connectivity Manager.

Fields and components

Field	Description
Keep Running Data check box	Click to continue running statistical data. This is useful if you want to see a trend.
Polling Frequency in Seconds text box	Type a number for polling frequency. The range is between five and 3600 seconds and the default is five seconds.
Start Polling button	Click to manually poll the V_Port statistics.
Reset button	Click to reset all of the statistics to 0.
Date	The date the Fabric statistics were run.
Num FLOGIs sent	The number of Fabric logins sent.
FLOGI response errors	The number of Fabric login response errors.
FLOGI accept errors	The number of times Fabric login attempts are accepted.
FLOGI accepts received	The number of times Fabric logins are received.
FLOGI rejects received	The number of times Fabric login attempts are rejected.
Unknown responses for FLOGI	The number of unknown Fabric login responses.
Allocation waits prior to sending FLOGI	The number of delayed Fabric login allocations.
FLOGIs received	The number of times Fabric logins are received.
Incoming FLOGIs rejected	The number of times Fabric logins are rejected.
Internal fabric online notification sent to other modules	The number of internal notifications for Fabrics that are online that are sent to other modules.
Internal fabric offline notification sent to other modules	The number of internal notifications for Fabrics that are offline that are sent to other modules.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Port Statistics dialog box"
- "Polling frequency rate"
- "Resetting statistics"
- "Performance monitoring"

FCP IM Statistics dialog box

The **FCP IM Statistics** dialog box enables you to display Fibre Channel Protocol Input Method (FCP IM) statistical information for initiators and targets.

Opening the dialog box

Select **Monitor > Statistics > Remote Port Statistics > FCP IM Statistics** from the Host Connectivity Manager.

OR

Right-click a remote port from the device tree and select **FCP IM Statistics**.

Fields and components

Field	Description
Date	The date and time of the most recent reset.
RPort Onlines	The number of online R_Ports.
RPort Offlines	The number of offline R_Ports.
PRLI Sent	The number of process login (PRLI) requests sent.
Fcxp Alloc Waits	The number of FCXP allocation waits.
PRLI Rsp Errors	The number of process login (PRLI) response errors.
PRLI Rsp Accepts	The number of process login (PRLI) response accepts.
PRLI Responses Parse Error	The number of process login (PRLI) response parse errors.
PRLI Rejects	The number of process login (PRLI) rejected requests.
Number of Times Timeouts Detected	The number of timeouts detected.
Second Level Error Recovery	The number of errors recovered.
Num Times in Initiator Mode	The number of times the RPort has been in initiator mode.
HAL Online Events	The number of hardware abstraction layer (HAL) online events.
HAL Offline Events	The number of hardware abstraction layer (HAL) offline events.
HAL Create Events	The number of hardware abstraction layer (HAL) create events.
HAL Delete Events	The number of hardware abstraction layer (HAL) delete events.
HAL Create Completions	The number of hardware abstraction layer (HAL) create completions.
HAL Delete Completions	The number of hardware abstraction layer (HAL) delete completions.
HAL SLER Events	The number of hardware abstraction layer (HAL) sequence layer error recovery (SLER) events.
HAL IOC Down Events	The number of hardware abstraction layer (HAL) IOC Down events.
HAL IO Cleanup Completions	The number of hardware abstraction layer (HAL) I/O cleanup completions.
HAL Task Management Commands	The number of hardware abstraction layer (HAL) task management commands.

Field	Description
HAL TM Firmware Responses	The number of hardware abstraction layer (HAL) task management firmware responses.
HAL TM Successes	The number of hardware abstraction layer (HAL) task management successes.
HAL TM Failures	The number of hardware abstraction layer (HAL) task management failures.
HAL TM Related IO Cleanups	The number of hardware abstraction layer (HAL) TM-related I/O cleanups.
HAL TM Firmware Queue Resumed	The number of times the hardware abstraction layer (HAL) task management firmware queue is resumed.
HAL TM Affected by IOC Down Events	The number of times hardware abstraction layer (HAL) task management is affected by IOC down events.
HAL TM Affected by ITN Offline	The number of times hardware abstraction layer (HAL) task management is affected when ITN is offline.
HAL TM Offline Cleanup Completions	The number of hardware abstraction layer (HAL) task management offline cleanup completions.
HAL IO Requests	The number of hardware abstraction layer (HAL) I/O requests.
HAL IO Completions	The number of hardware abstraction layer (HAL) I/O completions.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Port Statistics dialog box"
- "Polling frequency rate"
- "Resetting statistics"
- "Performance monitoring"

FCP IM Module Statistics dialog box

The **FCP IM Module Statistics** dialog box enables you to display statistical information for each initiator target nexus (ITN).

Opening the dialog box

Select **Monitor > Statistics > FCP IM Module Statistics** from the Host Connectivity Manager.

OR

Right-click a port from the device tree and select **Statistics > FCP IM Module Statistics**.

Fields and components

Field	Description
Keep Running Data check box	Click to continue running statistical data. This is useful if you want to see a trend.
Polling Frequency in Seconds text box	Type a number for polling frequency. The range is between five and 3600 seconds and the default is five seconds.
Start Polling button	Click to manually poll the FCP IM Module statistics.
Reset button	Click to reset all of the statistics to 0.
Date	The date and time of the most recent reset.
Total number of IOs	The total number of I/O operations on the port.
NO IO contexts	Number of I/O context requests.
IO waiting for CQ space	The number of I/Os waiting for circular queue space.
IO abort requests	The number of I/O abort requests.
NO task management contexts	Number of task management I/O context requests.
IO completions with OK status	The number of I/O operations that completed successfully.
IO underrun (good)	The number of successful firmware I/O underrun operations.
IO overrun (good)	The number of successful firmware I/O overrun operations.
Aborted IO requests	The number of aborted I/O requests.
IO selection timeouts	The number of I/O selection timeout occurrences.
IO protocol errors	The number of I/O protocol errors.
IO timeouts	The number of times an I/O timed out.
IO SBC-3 protection errors	Number of SCSI block data protection errors for SBC-3 (SCSI Block Command 3)
IO aborted by TM requests	The number of I/Os that were aborted because of target mode requests.
IO retry for SQ error recovery	The number of I/O retries for sequence level error recovery.
Delayed freeing of IO resources	The number of times I/O resource freeing was delayed.
IO with non-good SCSI status	The number of I/Os with SCSI status of non-good.
Host IO abort requests	The number of times the host aborted I/O requests.

Field	Description
IO comp with unknown tags	The number of I/Os with unknown tags.
IO implicitly aborted	The number of times an I/O was implicitly aborted.
IO aborted due to TM commands	The number of I/Os that were aborted because of target mode commands.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Port Statistics dialog box"
- "Polling frequency rate"
- "Resetting statistics"
- "Performance monitoring"

Fibre Channel Security Protocol Configuration dialog box

The **Fibre Channel Security Protocol Configuration** dialog box enables you to define security authentication on selected ports.

Opening the dialog box

Select **Configure > Authentication** from the main menu, or perform the appropriate following step to open the security authentication dialog box:

- From the host level, right-click the host and select **Authentication** from the list.

  The **Fibre Channel Security Protocol Configuration** (host level) dialog box displays.

- From the adapter level, right-click the adapter and select **Authentication** from the list.

  The **Fibre Channel Security Protocol Configuration** (adapter level) dialog box displays. This dialog box is identical to the **Fibre Channel Security Protocol Configuration** (host level) dialog box.

- From the adapter port level, right click a port and select **FC-SP > Authentication** from the list.

  The **Fibre Channel Security Protocol Configuration** dialog at the host level displays.

Fields and components

Field	Description
Port #	The port number (0 or 1) for which you are configuring security authentication.
Port WWN	The world wide name of the port for which you are configuring security authentication.
Port Name	The name of the port (for example, Port 0 or Port 1) for which you are configuring security authentication.
Authentication	Check to enable port security authentication.
Status	Indicates whether authentication is used.
Algorithm	The configured algorithm. Options include MD5, SHA1, MD5SHA1, SHAMD5.
Group	Indicates the DH group value. DHNULL (group 0) is the only option.
Enable Authentication check box	Check to enable FC-SP authentication on the selected device.
CHAP Secret	Type the CHAP secret.
Retype Secret	Retype the CHAP secret to confirm.
Algorithm list	Select the type of algorithm. Options include the following: • **MD5** - A hashing algorithm that verifies a message's integrity using Message Digest version 5. • **SHA1** - A secure hashing algorithm that computes a 160-bit message digest for a data file that is provided as input. • **MD5SH1** - Similar to the MD5 hashing algorithm, but used for DH-CHAP authentication. • **SHA1MD5** - Similar to the SHA1 hashing algorithm, but used for DH-CHAP authentication.

Field	Description
Group list	The DHNULL (group 0) is the only option available in the list.
Apply button	Click to apply the FC-SP settings.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Configuring security authentication using HCM (Host and HBA)"
- "Port Statistics dialog box"
- "Polling frequency rate"
- "Resetting statistics"
- "Performance monitoring"

Hardware Tests Diagnostics dialog box

The **Port Tests diagnostics** dialog box enables you to run tests on the port and to configure parameters such as link speed and frame count.

Opening the dialog box

1. Select an HBA or HBA port from the device tree.
2. Select **Configure > Diagnostics** from the Host Connectivity Manager.
3. Click the **Hardware Tests** tab.

Fields and components

Field	Description
Memory Test check box	Check to run a Memory test on the port.
Ports list	Select a port from the list.
PCI Loopback Test check box	Check to run a PCI Loopback test on the port.
Data Pattern	Type a data pattern. The default value is A5A5A5A5.
Test Cycle text box	Specify the number of times the test runs. The default value is 100.
Loopback Test check box	Check to run a Loopback test on the port.
Queue Test check box	Check to run a Queue test on the port.
Subtest ID list	Select a subtest from the list. The default is Internal.
Link Speed list	Select a link speed from the list.
Frame Count	Type a frame count. The default value is 8192.
Stop on Error check box	Check to flag the system to stop running the test if an error occurs.
Test Log table	Displays the time the test was run, the status of the test, and the result of the test.
Start button	Click to run the selected test.
Stop button	Click to stop all pending tests.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- “Configuring beaconing using HCM”
- “supportSave collection sources”

HBA Properties panel

The **HBA Properties** panel enables you to display the properties that are associated with a selected 4 Gbps or 8 Gbps Brocade HBA or mezzanine card.

Opening the properties panel

1. Select an HBA in the device tree.
2. Click the **Properties** tab in the right pane.

Fields and components

Field	Description
HBA Parameters	
Node WWN	The adapter node's world wide name.
Name	The name representing the adapter.
Operating Status	Whether the HBA is enabled or disabled.
Manufacturer	The company that manufactured the HBA.
Model Description	The description of the HBA.
Max Speed Supported	The maximum speed supported on the HBA; for example, 8 Gbps.
# of Ports	The number of ports associated with the HBA.
OEM info	Information about the original equipment manufacturer.
Card Type	The HBA card type; for example, FC.
Chip Revision	The revision level of the chip.
Hardware Path	The hardware path of the HBA.
Serial #	The serial number of the HBA.
Temperature	The temperature of the HBA, displayed in Celsius and Fahrenheit.
Driver Parameters *It is possible to have multiple pairs of driver information, based on the number and types of drivers installed.*	
Driver Name	The name of the host adapter driver.
Driver Version	The version level of the host adapter driver.
Firmware Parameters	
Firmware Version	The version level of the firmware.
BIOS Version	The version level of the BIOS.
PCI Registers	
Vendor ID	The identifier of the PCI Register's vendor.
Device ID	The device ID of the PCI Register.
Subsystem ID	The ID of the PCI subsystem.
Subsystem Vendor ID	The ID of the PCI subsystem vendor.

Field	Description
Current # of Lanes	The number of PCI lanes, in Gbps, each way between the PCI slot and the adapter.
Initial Negotiated # of Lanes	The set number of PCI lanes that were initially negotiated.
PCIe Generation	The number of times the PCI Register is generated.
OEM Vital Product Data (VPD) Information	
OEM	The name of the original equipment manufacturer.
Part #	The OEM part number of the HBA.
EDC	The engineering date code (HP only), displayed as A-YYWW, where A is the revision, YY is the year minus 1960, and WW is the week of the release. For example, A-4832 is Revision A, week 32 of 2008.
MDC	The manufacturing date code (HP only), displayed as YYWW, where YY is the year minus 1960 and WW is the week of manufacturing. For example, 4915 is the 15th week of 2009.
PW	The power rating (HP only). The value, 10 W, is the same for all adapters.
EC level	The engineering change level for the card, represented by alphanumeric characters.
FRU #	The OEM FRU number of the HBA.
Serial #	The OEM serial number of the HBA.
Product Description	The OEM product description of the HBA.
Vendor Data	Displays information that is specific to the HBA vendor.

IOC Statistics dialog box

The **IOC Statistics** dialog box enables you to view statistics related to the input/output controller (IOC).

Opening the dialog box

1. Select a physical port of the HBA from the device tree.
2. Select **Monitor > Statistics > IOC Statistics** from the Host Connectivity Manager.

Fields and components

Field	Description
Keep Running Data check box	Click to continue running statistical data. This is useful if you want to see a trend.
Polling Frequency in Seconds text box	Type a number for polling frequency. The range is between five and 3600 seconds and the default is five seconds.
Start Polling button	Click to manually poll the IOC statistics.
Reset button	Click to reset all of the statistics to 0.
IOC Driver: Mailbox Interrupt	The number of mailbox interrupts on the IOC driver.
IOC Driver: Start Events	The number of start events on the IOC driver.
IOC Driver: Stop Events	The number of stop events on the IOC driver.
IOC Driver: Enable Events	The number of enable events on the IOC driver.
IOC Driver: Disable Events	The number of disable events on the IOC driver.
IOC Driver: Heartbeat Failures	The number of heartbeat failures on the IOC driver.
IOC Driver: Firmware Boots	The number of firmware boots on the IOC driver.
IOC Driver: Statistics Timeouts	The number of statistics timeouts on the IOC driver.
Firmware IO: host IO aborts	The number of host IO aborts in the firmware.
Firmware IO: host IO Cleanup	The number of host IO cleanup attempts in the firmware.
Firmware IO: IO timeouts in f/w	The number of IO timeouts in the firmware.
Firmware IO: Frames parsed by f/w	The number of frames parsed by the firmware.
Firmware IO: data frames	The number of data frames in the firmware.
Firmware IO: fcp rsp frames	The number of FCP responses on the firmware IO.
Firmware IO: xfer_rdy_frames	The number of transfer ready frames.
Firmware IO: BLS ACC frames	The number of BLS ACC frames on the firmware IO.
Firmware IO: target abort frames	The number of aborted target frames on the firmware IO.
Firmware IO: unknown frames	The number of unknown frames on the firmware IO.
Firmware IO: itn CISC updated on rsp	The number of CISCs updated on response.
Firmware IO: itn CISC updated on data	The number of CISCs updated on data.
Firmware IO: itn CISC updated on xfer ready	The number of updates that occurred on xfer_rdy.

Field	Description
Firmware IO: data frames DMA'd by f/w	The number of data frames dropped by the firmware.
Firmware IO: frames dropped by f/w	The number of times the firmware dropped frames.
Firmware IO: FCP data frames lost	The number of FCP data frames lost.
Firmware IO: RO set in xfr_rdy	The number of RO set in xfr_rdy events on the firmware IO.
Firmware IO: xfer_rdy_000 error	The number of xfer_rdy_000 errors on the firmware IO.
Firmware IO: xfer_rdy_unknown_error	The number of xfer_rdy_unknown errors on the firmware IO.
Firmware IO: IO ABTS time out	The number of ABTS timeouts on the firmware IO.
Firmware IO: ITN SLER initiated	
Firmware IO: REC timeouts	The number of receive timeouts on the firmware IO.
Firmware IO: error REC	The number of errors received on the firmware IO.
Firmware IO: REC rsp invalid	The number of invalid receive responses.
Firmware IO: seqr IO abort	The number of sequential IO aborts.
Firmware IO: seq IO retry	The number of sequential retries on the firmware IO.
Firmware IO: FCP RSP - wrong IO state	The number of times responses were in the wrong IO state.
Firmware IO: wait for seq initiative	The number of sequential initiative waits on the firmware IO.
Firmware IO: FCP RSP_underrun	The number of IO response underruns.
Firmware IO: FCP RSP_underrun for write	The number of IO response underruns during write operations.
Firmware IO: FCP RSP_underrun err	The number of IO response underrun errors.
Firmware IO: FCP RSP_invalid residue	The number of invalid residue responses.
Firmware IO: FCP RSP_overrun	The number of overrun responses on the firmware IO.
Firmware IO: FCP RSP_overrun err	The number of overrun response errors on the firmware IO.
Firmware IO: FCP RSP - protocol err	The number of response protocol errors on the firmware IO.
Firmware IO: FCP RSP_sense data err	The number of response sense data errors on the firmware IO.
Firmware IO: FCP RSP - conf requested	The number of RSP_conf requests on the firmware IO.
Firmware IO: target initiated IO abort	The number of RSP_target initiated IO aborts.
Firmware IO: IOH EDTOV timer event	The number of Error Detect Time Out events.
Firmware IO: IOH FCP RSP excp event	The number of FCP response exception events on the firmware IO.
Firmware IO: IOH FCP conf event	The number of FCP conf events on the firmware IO.
Firmware IO: IOH multi-frm rsp event	The number of multi-frame response events on the firmware IO.
Firmware IO: IOH hit class2 event	The number of hit class2 events on the firmware IO.
Firmware IO: IOH miss other event	The number of other events missed on the firmware IO.
Firmware IO: IOH Seq count error event	The number of seq count error events on the firmware IO.
Firmware IO: IOH length error event	The number of length error events on the firmware IO.
Firmware IO: IOH seq length error event	The number of IOH seq length error events during firmware IO.
Firmware IO: IOH data oor event	The number of IOH data events that are out of range during firmware IO.

Field	Description
Firmware IO: IOH RO OOO event	The number of IOH RO events that are out of range during firmware IO.
Firmware IO: IOH CPU owned event	The number of CPU-owned events during firmware IO.
Firmware IO: IOH unex frame event	The number of unexpected frames on the firmware IO.
Firmware IO: IOH Error Interrupt	The number of interrupted errors on the firmware IO.
Firmware Port: Port FPG Interrupt	The number of firmware port FPG interrupts.
Firmware Port: FPG Level 0 Interrupts	The number of firmware port FPG Level 0 interrupts.
Firmware Port: FPG 0 Caused Interrupts	The number of firmware port FPG 0 caused interrupts.
Firmware Port: FPG Interrupts Other	The number of other firmware port FPG interrupts.
Firmware Port: FPG Interrupts Other Ignored	The number of other firmware port FPG interrupts that were ignored.
Firmware Port: FPG Signal Lost	The number of firmware port FPG lost signals.
Firmware Port: FPG Signal Regained	The number of firmware port FPG regained signals.
Firmware Port: FPG Sync Lost	The number of times loss of sync on the firmware port has occurred.
Firmware Port: FPG Sync Timeout	The number of times sync timeout on the firmware port has occurred.
Firmware Port: FPG Sync Regained	The number of synchronizations that were regained on the firmware port.
Firmware Port: FPG DIV2 Overflow	The number of DIV2 overflow events on the firmware port.
Firmware Port: FPG DIV2 Underflow	The number of DIV2 underflow events on the firmware port.
Firmware Port: FPG EFIFO Overflow	The number of Elastic FIFO (EFIFO) overflow events on the firmware port.
Firmware Port: FPG EFIFO Underflow	The number of Elastic FIFO (EFIFO) underflow events on the firmware port.
Firmware Port: FPG IDLE Primitives	The number of IDLE primitive events on the firmware port.
Firmware Port: FPG LRR Primitives	The number of Link Reset Responsive (LRR) primitive events on the firmware port.
Firmware Port: FPG LR Primitives	The number of Link Reset (LR) primitive events on the firmware port.
Firmware Port: FPG OLS Primitives	The number of Offline Sequence (OLS) primitive events on the firmware port.
Firmware Port: FPG NOS Primitives	The number of Not Operational (link has failed) primitive events on the firmware port.
Firmware Port: FPG LIP Primitives	The number of Loop Initialization (LIP) primitive events on the firmware port.
Firmware Port: FPG ARBFO Primitives	The number of ARBFO primitive events on the firmware port.
Firmware Port: FPG MRK Primitives	The number of MRK primitive events on the firmware port.
Firmware Port: PHYSM Module Inserts	The number of module inserts in the Physical Port State Machine (PHYSM).
Firmware Port PHYSM Module Extracts	The number of module extracts in the Physical Port State Machine (PHYSM).

Field	Description
Firmware Port PHYSM Module Invalid Events	The number of invalid events in the Physical Port State Machine (PHYSM).
Firmware Port: FPG Unknown Primitives	The number of unknown primitive events on the firmware port.
Firmware Port: PHYSM Module Validation Ignored	The number of times Physical Port State Machine (PHYSM) module validation was ignored.
Firmware Port: PHYSM Laser Faults	The number of laser fault events on the Physical Port State Machine (PHYSM).
Firmware Port SNSM: HWSM Success	The number of Hardware State Machine (HWSM) successes for the firmware port speed negotiation state machine (SNSM).
Firmware Port SNSM: HWSM Failures	The number of Hardware State Machine (HWSM) failures for the firmware port speed negotiation state machine (SNSM).
Firmware Port SNSM: HWSM Timeouts	The number of Hardware State Machine (HWSM) timeouts for the firmware port speed negotiation state machine (SNSM).
Firmware Port SNSM: SWSM Success	The number of speed negotiation state machine (SNSM) successes.
Firmware Port SNSM: SWSM Timeouts	The number of speed negotiation state machine (SNSM) timeouts.
Firmware Port SNSM: Error Resets	The number of error resets on the speed negotiation state machine (SNSM).
Firmware Port SNSM: Signal Loss Count	The signal loss count on the speed negotiation state machine (SNSM).
Firmware Port SNSM: Sync Loss Count	The synchronization loss count on the speed negotiation state machine (SNSM).
Firmware Port LKSM: HWSM Success	The number of LKSM and Hardware State Machine (HWSM) successes.
Firmware Port LKSM: HWSM Failures	The number of LKSM and Hardware State Machine (HWSM) failures.
Firmware Port LKSM: HWSM Timeouts	The number of LKSM and Hardware State Machine (HWSM) timeouts.
Firmware Port LKSM: SWSM Success	The number of LKSM and SWSM successes.
Firmware Port LKSM: SWSM Failures	The number of LKSM and SWSM failures.
Firmware Port: LKSM: Busy Buffer Failures	The number of LKSM failures on the firmware port because of a busy buffer.
Firmware Port LKSM: SWSM Timeouts	The number of LKSM and SWSM timeouts on the firmware port.
Firmware Port LKSM: Buffer Wait State Entries	The number of buffer wait state entries on the firmware port.
Firmware Port LKSM: Link Failures	The number of link failures on the firmware port.
Firmware Port LKSM: Prim Sequence Protocol Errors	The number of primitive sequence protocol errors on the firmware port.
Firmware Port LKSM: LRs Unexpected	The number of unexpected Link Resets (LRs).
Firmware Port LKSM: LRRs Unexpected	The number of unexpected Link Reset Responsive (LRR) occurrences.

Field	Description
Firmware Port LKSM: LR TX Started	The number of Link Reset (LR) transmissions started on the firmware port.
Firmware Port LKSM: LRR TX Started	The number of Link Reset Responsive (LRR) transmits started on the firmware port..
Firmware Port LKSM: NOS TX Started	The number of Not Operational transmissions that were started.
Firmware Port LKSM: OLS TX Started	The number of Offline Sequence (OLS) transmits started on the firmware port.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Port Statistics dialog box"
- "Polling frequency rate"
- "Resetting statistics"
- "Performance monitoring"

Logical Port Statistics dialog box

The **Logical Port Statistics** dialog box enables you to display statistics that are related to a selected logical port.

Opening the dialog box

Select **Monitor > Statistics > Logical Port Statistics** from the Host Connectivity Manager

OR

Right-click a logical port (LPORT) from the device tree and select **Logical Port Statistics**.

Fields and components

Field	Description
Date	The date and time of the most recent reset.
ns_plogi_rsp_err	The number of Name Server response errors.
ns_plogi_sent	The number of Name Server port logins sent.
ns_plogi_acc_err	The number of Name Server port login accept errors.
ns_plogi_accepts	The number of times Name Server port logins are accepted.
NS command Rejects	The number of Name Server port login rejects.
ns_plogi_unknown_rsp	The number of unknown Name Server port login response errors.
ns_plogi_alloc_wait	The number of delayed Name Server port login response errors.
NS command retries	The number of name server command retries.
NS command timeouts	The number of name server command timeouts.
ns_rspnid_sent	The number of times the Name Server Register Symbolic Port Name identifier was sent.
ns_rspnid_accepts	The number of times the Name Server Register Symbolic Port Name identifier was accepted.
ns_rspnid_rsp_error	The number of Name Server Register Symbolic Port Name identifier response errors.
ns_rspnid_rejects	The number of Name Server Register Symbolic Port Name identifier rejects.
ns_rspnid_alloc_wait	The number of Name Server Register Symbolic Port Name identifier allocations.
ns_rftid_sent	The number of Name Server Register FC4 Type identifier requests sent.
ns_rftid_accepts	The number of times the system accepted Name Server Register FC4 Type identifier requests.
ns_rftid_rsp_err	The number of Name Server Register FC4 Type identifier response errors.
ns_rftid_rejects	The number of times the system rejected Name Server Register FC4 Type identifier requests.

Field	Description
ns_rftid_alloc_wait	The number of delayed Name Server Register FC4 Type identifier allocations.
ns_gidft_sent	The number of times a Name Server Get all Port ID request for a given FC4 type is sent.
ns_gidft_accepts	The number of times a Name Server Get all Port ID request for a given FC4 type is accepted.
ns_gidft_rsp_err	The number of response errors associated with a Name Server Get all Port ID request for a given FC4 type.
ns_gidft_rejects	The number of times a Name Server Get all Port ID request for a given FC4 type is rejected.
ns_gidft_unknown_rsp	The number of unknown responses associated with a Name Server Get all Port ID request for a given FC4 type.
ns_gidft_alloc_wait	The number of delayed Name Server Get all Port ID requests for a given FC4 type allocations.
MS command retries	The number of MS command retries.
MS command timeouts	The number of times an MS command timed out.
ms_plogi_sent	The number of port login requests sent.
ms_plogi_rsp_err	The number of response errors associated with a ms port login.
ms_plogi_acc_err	The number of ms port login accept errors.
ms_plogi_accepts	The number of ms port login accepts.
ms_plogi_unknown_rsp	The number of ms port login unknown responses.
ms_plogi_alloc_wait	The number of delayed ms plogin allocations.
Num of RSCN Received	The number of Registered State Change Notifications received.
Num port id format RSCN	The number of Registered State Change Notifications received by Port ID.
unsolicited recv frames	The number of received frames that were unsolicited.
dropped received frames	The number of received frames that were dropped.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Port Statistics dialog box"
- "Polling frequency rate"
- "Resetting statistics"
- "Performance monitoring"

LPORT Properties panel

The **LPORT Properties** panel enables you to display the properties that are associated with a logical port.

Opening the properties panel

1. From the device tree, select a physical port.
2. Click the **LPORTs Properties** tab in the right pane.

Fields and components

Field	Description
Base Port	Indicates whether the logical port is used as the base port.
FC Address	The Fibre Channel address of the logical port.
Node WWN	The adapter's world wide name.
Port WWN	The port's world wide name.
Roles	The role of the logical port; for example, FCP Initiator.
State	Displays whether the logical port is online or offline.
Switch IP Addr	The switch's IP address.
Switch NWWN	The switch node's world wide name.
Symbolic Name	The symbolic name associated with the logical port.

Master Log tab

The **Master Log** enables you to display a list of all events that have occurred.

Opening the Master Log

Click the **Master Log** tab, located on the bottom pane of the Host Connectivity Manager.

A master summary of events on all discovered devices is displayed.

Fields and components

Field	Description
Filter button	Click to launch the **Master Log Filter** dialog box.
Sr No column	Displays a numbering sequence in ascending order.
Severity column	The event severity (informational, minor, major, or critical).
WWN/MAC column	The world wide name or the media access control (MAC) address of the device on which the event occurred.
Category column	The event categories are as follows: • ADAPTER - Events pertaining to the adapter. • IOC - Events pertaining to the IO Controller. • IP over FC - Events pertaining to IP over Fibre Channel. • VLAN - Events pertaining to a virtual LAN. • PORT - Events pertaining to a physical port. • LPORT - Events pertaining to a specific logical port (one logical port always exists per physical port). • RPORT - Events pertaining to a specific remote port (could be an initiator or target). • ITNIM - Events pertaining to an initiator-target nexus. • RSVD - Reserved. • AUDIT - Audit events.
Subcategory column	The subcategory of the main event; for example, offline, online, disabled, or enabled.
Description column	Displays a brief description of the event.
Date/Time column	The date and time when the event occurred.
Clear Filter button	Click to clear the Master Log filter.
Refresh button	Click to refresh the screen.

Using the Master Log

Refer to the following topics for specific procedures using this dialog box:

- "Master log"
- "Event severity icons"
- "Filtering event log entries"

Master Log Filter dialog box

The **Master Log Filter** dialog box enables you to filter the events you receive by time, severity, category, or world wide name.

Opening the dialog box

1. Select the **Master Log** tab, located at the bottom pane of the Host Connectivity Manager,
2. Click the **Filter** button.

Fields and components

Field	Description
Event Time	Type in a From and To value to represent the time during which events will be logged.
Event Severity	Select one or all of the following values: Critical, Major, Minor, Information.
Category	Select an event category, for example, Rport or ITNIM, from the list.
WWN/MAC	Select a world wide name (WWN) or media access control (MAC) address from the list.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Master log"
- "Event severity icons"
- "Filtering event log entries"

Persistent Binding dialog box

The **Persistent Binding** dialog box enables target port world wide name binding to a persistent target ID for the OS stack. You can view the **Persistent Binding** dialog box at the host level, the adapter level, or the port level.

Opening the dialog box

1. Select a device that supports persistent binding from the device tree.

   Devices that support persistent binding include the local host, the adapter, and the port.

2. Select **Configure > Persistent Binding**.

Fields and components

Field	Description
At the host or HBA level	
Serial Number	The serial number of the host or HBA.
Hardware Path	The hardware path of the host or HBA.
Port #	The port number of the host or HBA.
Port WWN	The port's world wide name.
Name	The port name; for example, Port 0 or Port 1.
Persistent Type	The type of binding; for example, Port WWN.
Target Name	The SCSI target name.
Remote Port WWN	The world wide name of the remote port.
SCSI Target ID	The SCSI target identifier.
At the port level	
HBA Node	The world wide node name of the HBA node (the WWN of the mezzanine node for the Brocade 804).
HBAport	The world wide name of the HBA port (the WWN of the mezzanine port for the Brocade 804).
Persistent type	The type of binding; for example, Port WWN.
Target Name	The SCSI target name.
Remote Port WWN	The world wide name of the remote port.
SCSI Target ID	The SCSI target identifier.

Using the dialog box

Refer to the following topic for specific procedures using this dialog box:

- "Basic port configuration"

Port Properties panel

The **Port Properties** panel enables you to display the properties that are associated with a selected HBA port.

Opening the properties panel

1. Select a port in the device tree.
2. Click the **Properties** tab in the right pane.

Fields and components

Field	Description
Port Parameters	
Port #	The port number: 0 or 1.
Port WWN	The port's world wide name.
Node WWN	The adapter's world wide name.
Factory Port WWN	The factory-assigned port world wide name.
Factory Node WWN	The factory-assigned adapter world wide name.
Name	The name that is manually assigned to the port.
FC Address	The port's Fibre Channel address.
Media	Type of media software; for example, 8G-sw.
Port Type	The port type; for example, N_Port.
Configured Port State	Indicates whether the port is enabled or disabled.
Operating Port State	Indicates whether the link is online or offline.
Supported Classes	The types of classes that are supported on the port; for example, Class-3.
Configured Speed	The configured port speed.
Operating Speed	The speed at which the port is operating. The unit of measurement is in gigabits per second (Gbps). The available speed options depend on the HBA's speed and the port's SFP. Auto-negotiate is the recommended setting and it is the default. For the 4 Gbps HBA (425 and 415) and the mezzanine card (804), speed options are 1 Gbps, 2 Gbps, 4 Gbps, and 8 Gbps. The 8 Gbps HBA (825, 815) does not support the 1 Gbps speed.
Max Speed Supported	The maximum speed that is supported on the port, which is 8 Gbps.
Operating Topology	The topology setting at which the port is operating.
Receive BB Credits	The maximum number of receive buffers.
Transmit BB Credits	The maximum number of transmit buffers.
IOC ID	The I/O controller's identifier.
Hardware Path	The hardware path of the port.

Field	Description
Frame Data Field Size	The frame size, in byres, of the port. The default is 2112. Select auto to set the frame data field size automatically.
# of Lports	The number of logical ports in the configuration.
Port Log	Indicates whether port logging is enabled or disabled.
Operating Parameters	
Path Time Out	The value between 0 and 60 that specifies the time out session. The default value is 30.
Logging Level	The port logging level. Values include Log Critical, Log Error, Log Warning, Log Info, and Log Invalid.
Target Rate Limit	Indicates whether target rate limiting is on or off.
Default Rate Limit	Select the target rate limit from the list. Options include 1 Gbps (the default), 2 Gbps, and 4 Gbps.
FC-SP Parameters	
Authentication	Indicates whether FC-SP authentication is on or off.
Status	The status of Fibre Channel Security Protocol (FC-SP) authentication.
Algorithm	The configured authentication algorithm.
Group	The DH Group (DH Null, group 0, is the only option).
Error Status	The health status of the Fibre Channel Security Protocol (FC-SP) parameters.
QoS Parameters	
Configured QoS State	Indicates whether QoS is enabled or disabled.
Operating QoS State	Indicates whether QoS is online or offline.
Total BB Credit	The total number of receive buffers.
Priority Levels	QoS priority levels. Values include High, Medium, and Low.

Using the property panel

Refer to the following topics for specific procedures using this dialog box:

- "Configuring the port speed using HCM"
- "Specifying the maximum frame size using HCM"
- "Specifying path time out using HCM"
- "Configuring the HCM logging level using HCM"
- "Enabling and disabling persistent binding using HCM"
- "Enabling and disabling rate limiting on the adapter side using HCM"

Port Statistics dialog box

The **Port Statistics** dialog box enables you to monitor the performance of the adapter and the traffic between the adapter and the LUNs. You can use the information to isolate and troubleshoot areas that affect application performance.

Opening the dialog box

Select **Monitor > Statistics > Port Statistics** from the Host Connectivity Manager.

Fields and components

Field	Description
Keep Running Data check box	Click to continue running statistical data. This is useful if you want to see a trend.
Polling Frequency in Seconds text box	Type a number for polling frequency. The range is between five and 3600 seconds and the default is five seconds.
Start Polling button	Click to manually poll the V_Port statistics.
Reset button	Click to reset all of the statistics to 0.
Date	The date and time of the most recent reset.
Port WWN	The world wide name of the port about which statistics are displayed.
Seconds since stats is reset	The number of seconds since the port statistics reset (the counter returns to 0).
Tx frames	The number of total transmitted Fibre Channel frames across all protocols and classes.
Tx words	The number of total transmitted Fibre Channel words across all protocols and classes.
Tx LIP	The number of loop initialization (LIP) transmit events.
Tx NOS	The number of not operational (link has failed) transmit events.
Tx OLS	The number of transmitted Offline Sequence (OLS) events.
Tx LR	The number of link reset (LR) transmit events.
Tx LRR	The number of transmitted Link Reset Response (LRR) events.
Rx frames	The number of total received Fibre Channel frames across all protocols and classes.
Rx words	The number of total received Fibre Channel words across all protocols and classes.
Rx LIP	The number of loop initialization (LIP) receive events.
Rx NOS	The number of not operational (link has failed) receive events.
Rx OLS	The number of received Offline Sequence (OLS) events.
Rx LR	The number of link reset (LR) receive events.
Rx LRR	The number of received Link Reset Response (LRR) events.

Field	Description
Rx CRC err frames	The number of frames that have been received in error.
Rx CRC err good EOF frames	The number of received frames with good end of frames (EOF)s.
Rx undersized frames	The number of undersized received frames.
Rx oversized frames	The number of oversized received frames.
Rx frames with bad EOF	The number of received frames with end of frame (EOF) errors.
Errored frames	The number of frames received in error.
Dropped frames	The number of frames that were lost due to a lack of host buffers available.
Link Failure (LF) Count	The number of times a link error has occurred.
Loss Of sync count	The number of times loss of sync has occurred.
Loss Of signal count	The number of times loss of signal has occurred.
Primitive sequence protocol err.	The number of primitive sequence protocol errors.
Invalid ordered sets	The number of ordered sets that are invalid.
Encoding err non frame_8b10b	The encoding non-frame error.
Encoding err frame_8b10b	The number of 8b/10b encoding errors recorded.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Port Statistics dialog box"
- "Polling frequency rate"
- "Resetting statistics"
- "Performance monitoring"

Protocol Tests dialog box

The **Protocol Tests** dialog box enables you to run diagnostic tests on Fibre Channel components.

Opening the dialog box

1. Select **Configure > Diagnostics** from the Host Connectivity Manager.
2. Click the **FC Protocol Tests** tab.

Fields and components

Field	Description
Echo Test check box	Check to run an Echo Test on the selected port.
FC Ping Test check box	Check to run an FC Ping Test on the selected port.
FC Trace Route check box	Check to run an FC Traceroute on the selected port.
Add button	Click to add a selected port, logical port, or target to the test list.
Remove button	Click to remove a selected port, logical port, or target from the test list.
Remove All button	Click to remove all ports, logical ports, and targets from the test list.
Test Cycle text box	Specify the number of times the test runs. The default value is 100.
Test Log table	Displays the time the test was run, type of test run, status of the test, configuration, and the results.
Port list	Select a port on which the test will be run from the list.
Target list	Select a target on which the test will be run from the list.
Logical Port list	Select a logical port on which the test will be run from the list.
Stop on Error check box	Check to flag the system to stop running the test if an error occurs.
Start button	Click to run the selected test.
Stop button	Click to stop all pending tests.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- “Configuring beaconing using HCM”
- “supportSave collection sources”

QoS Statistics dialog box

The **QoS Statistics** dialog box enables you to view statistics related to Quality of Service (QoS).

Opening the dialog box

Select **Monitor > Statistics > QoS Statistics** from the Host Connectivity Manager.

Fields and components

Field	Description
Date	The date and time of the most recent reset.
QoS Flogi sent	The number of QoS Fabric login (Flogi) requests sent.
QoS Flogi Acc received	The number of QoS Fabric login (Flogi) accept requests received.
QoS Flogi rejects received	The number of QoS Fabric login (Flogi) rejects received.
QoS Flogi retries	The number of QoS Fabric login (Flogi) retries.
QoS ELP received	The number of ELPs successfully received.
QoS ELP Accepted	The number of ELPs (Exchange Link Parameters) accepts sent.
QoS ELP rejected	The number of ELPs rejected.
QoS ELP dropped	The number of ELPs dropped.
QoS RSCN received	The number of Registered State Change Notifications (RSCN) received.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Port Statistics dialog box"
- "Polling frequency rate"
- "Resetting statistics"
- "Performance monitoring"

Remote Port Properties panel

The **Remote Port Properties** panel enables you to display the properties that are associated with the remote port.

Opening the properties panel

1. From the device tree, select a remote port (target or initiator).
2. Click the **Remote Port Properties** tab in the right pane.

NOTE
If it is a target port, there are two tabs in the right pane: **Properties** and **LUNs**.

Fields and components

Field	Description
Port WWN	The world wide name of the device's port.
Node WWN	The world wide name of the device.
Symbolic Name	The symbolic name associated with the remote port.
Name	The name associated with the device.
FC Address	The remote port's Fibre Channel address.
Device Type	The type of device associated with the remote port; for example, Disk.
Target Rate Limiting Enforced	Indicates whether target rate limiting is used on the remote device.
QoS Priority	The QoS priority level, which ranges between 0 (best effort) to 7 (the highest priority).
Bus #	The unique identifying number for each PCI bus, assigned during system initialization.
Target ID	The identifier of the target device.

Restore dialog box

You can use the **Restore Data** dialog box to restore data that has been previously backed up. The Host Connectivity Manager (HCM) stores the location and version details of the most recently-taken backed up data and automatically points to the location of the data.

NOTE
Use HCM 2.1 or later to restore backed up data. HCM 2.0 and earlier versions do not support the Restore Data feature.

The following data is restored:

- HBA application configuration data (HBAApplication.properties)
- HCM user authentication data (noitacitnehtua.properties)
- Alias Configuration data (HbaAliasdb.properties)
- Setup Discovery Data (SetupDiscovery.properties)
- Syslog Data (Syslog.properties)
- HCM Logging Data (logging.properties and log4j.xml)
- SupportSave

Opening the dialog box

1. Select a host, an HBA, or a port from the device tree.
2. Select **Tool > Restore Data** from the main menu.

   The **Restore Data** dialog box displays.

Fields and components

Field	Description
Restore from previous backup data button	Click to enable the **Browse** button, which enables you to locate the last backed-up file.
Browse button	Click to navigate to where the last backed-up file resides.
Restore default data button	If you click this button, the **Browse** text field is grayed out and the last restored data file is automatically retrieved.
Start Restore button	Click to restore the backed up data that you selected.

SFP Properties panel

The **SFP Properties** panel enables you to display the properties that are associated with a selected small form-factor pluggable (SFP) transceiver.

NOTE
Brocade 804 mezzanine cards connect to the embedded switch modules or embedded interconnect modules on the Blade System chassis by way of an internal backplane and therefore, no optical modules (SFPs) are involved. With the exception of no SFPs, the Brocade 804 mezzanine FC HBA card functions the same as the other Brocade HBAs.

Opening the properties panel

1. Select a port in the device tree.
2. Click the **SFP** tab in the right pane.

NOTE
Only Brocade-branded SFPs are supported with the 8 Gbps FC HBA.

Fields and components

Field	Description
Port Technology	
SFP Supported	The name of the supported SFP.
Connector Type	The type of port connector; for example, LC. SC, or Cu (copper cable).
Transceiver	The type of transceiver; for example, XFP or GBIC.
Media	The type of media for the transceiver; for example, single mode.
Speed	The port speed. Options for the 8 Gbps HBA (825 and 815) are 2 Gbps, 4 Gbps, and 8 Gbps (1 Gbps not supported). Port speed options for the 4 Gbps HBA (425 and 415) and the mezzanine card (804) are 1 Gbps, 2 Gbps, 4 Gbps, and 8 Gbps.
Extended Information	
Identifier	The identifier for the extended link.
Encoding	Displays how the extended link is encoded, for example, 8B10B.
Baud Rate	The transmission rate, roughly equivalent to the number of bits per second.
Length 9u	The length of the single-mode fiber optic cable, used in situations where gigabit performance is not required (for distances greater than 100 meters).
Length 50u	The length of the fiber optic cable (for distances greater than 10 meters).
Length 62.5u	The length of the fiber optic cable (for distances greater than 10 meters).

Field	Description
Length Cu	The length of the copper cable (for distances greater than 1 meter, where optimum performance is required).
Vendor Name	The vendor of the extended link.
Vendor OUI	The vendor's organizational unique identifier (OUI).
Vendor Part	The part number of the extended link.
Revision	The revision level of the extended link.
Wavelength	The wavelength translation, which enables longer reach through lower attenuation.
Options	Displays details about the transceiver; for example, the type of port connector, type of transceiver, and enable/disable status.
BR Max	The upper bit rate limit at which the SFP transceiver meets its specifications.
BR Min	The lower bit rate limit at which the SFP transceiver meets its specifications.
Serial #	The serial number of the SFP.
Date Code	The date the SFP was manufactured.
Refresh button	Click to refresh the screen.

Syslog Server Configuration dialog box

The **Syslog Server Configuration** dialog box enables you to configure the host connectivity manager (HCM) to send Syslog messages to other computers through port 514. You can configure the HCM agent to forward events to a maximum of three Syslog destinations.

Opening the dialog box

1. Select the host from the device tree.
2. Select **Configure > Syslog** from the main menu.

Fields and components

Field	Description
Host name / IP Address text box	Enter the host name or IP address of the destination device.
Set this IP in all discovered agents in future check box	Click to set the device as a Syslog destination in all future discovered agents.
Add button	Click to register the host as a Syslog destination.
Remove button	Click to remove the host as a Syslog destination.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Syslog support"
- "Registering a host server"
- "Removing a host server"

Target Statistics dialog box

The **Target Statistics** dialog box enables you to display statistical information for a selected remote port (R_Port).

Opening the dialog box

Select **Monitor > Statistics > Remote port statistics > Target Statistics** from the Host Connectivity Manager.

OR

Right-click a remote port and select **Target Statistics**.

Fields and components

Field	Description
Date	The date and time of the most recent reset.
offlines	The remote ports that are offline.
onlines	The remote ports that are online.
RSCN	The number of Fibre Channel Registered State Change Notifications (RSCNs) received.
PLOGI sent	The number of times port logins (when two node ports in the SAN establish a connection between each other) occur.
PLOGI accepts	The number of times port logins are accepted.
PLOGI timeouts	The number of times port logins time out.
PLOGI failed	The number of times port logins fail.
PLOGI rejects	The number of times port logins are rejected.
PLOGI received	The number of times port logins are received.
PRLI received	The number of times PRLIs are received.
ADISC sent	The number of discover address (ADISC) requests sent.
ADISC accepts	The number of times discover address (ADISC) requests are accepted.
ADISC failed	The number of times discover address (ADISC) requests fail.
ADISC rejects	The number of times discover address (ADISC) rejects.
ADISC received	The number of times discover address (ADISC) requests are received.
ADISC rejected	The number of times discover address (ADISC) requests are rejected.
LOGO sent	The number of times logouts occur.
LOGO accepts	The number of times logouts are accepted.
LOGO failed	The number of times logouts fail.
LOGO rejected	The number of times logouts are rejected.

Field	Description
LOGO received	The number of times logouts are received.
RPSC received	The number of Report Port Speed Capabilities (RPSC) requests received.
RPSC rejects	The number of Report Port Speed Capabilities (RPSC) requests rejected.
RPSC sent	The number of Report Port Speed Capabilities (RPSC) requests sent.
RPSC accepts	The number of Report Port Speed Capabilities (RPSC) requests accepted.
RPSC failed	The number of failed Report Port Speed Capabilities (RPSC) requests
uninit: create events	The number of hardware abstraction layer (HAL) uninit create events.
uninit: exception events	The number of hardware abstraction layer (HAL) uninit exception events.
created: online events	The number of hardware abstraction layer (HAL)-created online events.
created: delete events	The number of hardware abstraction layer (HAL)-created delete events.
created: IOC Down	The number of times hardware abstraction layer (HAL)-created I/O controllers were down.
created: exception events	The number of hardware abstraction layer (HAL)-created exception events.
fw create: f/w responses	The number of hardware abstraction layer (HAL) firmware-create responses.
fw create: delete events	The number of hardware abstraction layer (HAL) firmware-created delete events.
fw create: offline events	The number of hardware abstraction layer (HAL) firmware created offline events.
fw create: IOC down	The number of times hardware abstraction layer (HAL) firmware-created I/O controllers were down.
fw create: exception events	The number of hardware abstraction layer (HAL) firmware-created exception events.
online: offline events	The number of hardware abstraction layer (HAL) online and offline events.
online: delete events	The number of hardware abstraction layer (HAL) online delete events.
online: IOC down events	The number of hardware abstraction layer (HAL) online IOC down events.
online: exception events	The number of hardware abstraction layer (HAL) online exception events.
fw delete: fw responses	The number of hardware abstraction layer (HAL) fw Delete f/w responses.
fw delete: delete events	The number of hardware abstraction layer (HAL) fw Delete Delete events.

Field	Description
fw delete: IOC down events	The number of hardware abstraction layer (HAL) fw Delete IOC down events.
fw delete: exception events	The number of hardware abstraction layer (HAL) fw Delete Exception events.
offline: delete events	The number of hardware abstraction layer (HAL) Offline Delete events.
offline: online events	The number of hardware abstraction layer (HAL) Offline Online events.
offline: IOC down events	The number of hardware abstraction layer (HAL) offline IOC down events.
offline: exception events	The number of hardware abstraction layer (HAL) offline exception events.
delete: fw events	The number of hardware abstraction layer (HAL) delete f/w events.
delete: IOC down events	The number of hardware abstraction layer (HAL) Delete IOC down events.
delete: exception events	The number of hardware abstraction layer (HAL) delete exception events.
delete pend: fw responses	The number of hardware abstraction layer (HAL) delete pend f/w responses.
delete pend: IOC downs	The number of hardware abstraction layer (HAL) delete pending IOC downs.
delete pend: exceptions	The number of hardware abstraction layer (HAL) delete pending exceptions.
off-pending: fw responses	The number of hardware abstraction layer (HAL) off-pending f/w responses.
off-pending: deletes	The number of hardware abstraction layer (HAL) off-pending deletes.
off-pending: IOC downs	The number of hardware abstraction layer (HAL) off-pending IOC downs.
off-pending: exceptions	The number of hardware abstraction layer (HAL) off-pending exceptions.
IOC down: offline events	The number of hardware abstraction layer (HAL) IOC down offline events.
IOC down: delete events	The number of hardware abstraction layer (HAL) IOC down delete events.
IOC down: online events	The number of hardware abstraction layer (HAL) IOC down online events.
IOC down: exceptions	The number of hardware abstraction layer (HAL) IOC down exception events.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Port Statistics dialog box"
- "Polling frequency rate"
- "Resetting statistics"
- "Performance monitoring"

Test Log Details dialog box

The **Test Log Details** dialog box enables you to view details about a selected port or protocol test.

Opening the dialog box

1. Select **Configure > Diagnostics** from the Host Connectivity Manager.
2. Run any diagnostic test.
3. Select and double-click a row of the test results in the bottom pane.

Fields and components

Field	Description
Time	The date and time the test was run.
Test	The name of the test.
Status	The status of the test, for example, executing or pending.
Configuration	The name of the test component and its corresponding value. For example: • Adapter world wide name • Data pattern • Frame count • Port world wide name
Result	The test result, for example, test started or test complete.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Running a hardware-level test using HCM"
- "Running a Fibre Channel protocol-level test using HCM"

Virtual Port Creation dialog box

The **Virtual Port Creation** dialog box enables you to create a new virtual port from a physical port.

Opening the dialog box

1. Select a physical port from the device tree.
2. Select **Configure > Virtual Port > Create** from the main menu.

   OR

   Right-click the physical port and select **Virtual Port > Create** from the list.

Fields and components

Field	Description
Physical Port WWN	Displays the world wide name for the physical port.
Virtual Port WWN text box	Enter a unique world wide name for the virtual port. The default node WWN is the physical port node WWN. You must manually change it to a unique WWN for the virtual port.
Use auto-generated check box	Click to auto-generate the virtual port world wide name. By default, auto-generate is selected.
Generate Again button	Click to regenerate the virtual port WWN and the virtual node WWN.
Virtual Node WWN text box	Enter a unique world wide name for the virtual node. The default node WWN is the physical port node WWN. You must manually change it to a unique WWN for the virtual port.
Symbolic Name text box	Enter the symbolic name associated with the virtual port.
Name text box	Enter the name for the virtual port.
Description text box	Enter a description for the virtual port.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Virtual port configuration"
- "Creating a virtual port"
- "Deleting a virtual port"

Virtual Port Deletion dialog box

The **Virtual Port Deletion** dialog box enables you to delete an existing virtual port.

Opening the dialog box

1. Select a virtual port from the device tree.
2. Select **Configure > Virtual Port > Delete** from the main menu.

   OR

   Right-click the virtual port and select **Virtual Port > Delete** from the list.

   A warning message displays, asking for confirmation.
3. Click **OK** to continue.

NOTE
You cannot delete the base port.

Fields and components

Field	Description
Deletion check box	Check to select the virtual port to be deleted.
WWN	The virtual port's world wide name.
Node WWN	The virtual node's world wide name.
Symbolic Name	The symbolic name that is associated with the virtual port.
Delete Selected button	Click to delete the selected virtual port.
Delete All button	Click to delete all virtual ports that are displayed.
Cancel button	Click to abort the operation.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Virtual port configuration"
- "Creating a virtual port"
- "Deleting a virtual port"

Virtual Port Properties panel

The **Virtual Port Properties** panel enables you to display the properties that are associated with a virtual port.

Opening the properties panel

Select a virtual port from the device tree and click the **Properties** tab.

Fields and components

Field	Description
Port WWN	The port's world wide name.
Node WWN	The adapter's world wide name.
Fabric Name	The name of the Fabric associated with the virtual port.
FC Address	The Fibre Channel address of the virtual port.
State	Indicates whether the virtual port is online or offline.
Roles	The role of the virtual port; for example, FCP Initiator.
Base Port	Indicates whether the virtual port is used as the base port.
Symbolic name	The switch's symbolic name.
Switch IP address	The switch's IP address.
Preboot Created	Indicates whether preboot was created on the virtual port (True or False).

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Virtual port configuration"
- "Creating a virtual port"
- "Deleting a virtual port"

Virtual Port Statistics dialog box

The **Virtual Port Statistics** dialog box enables you to view statistical information related to a selected virtual port.

Opening the dialog box

1. Select a virtual port from the device tree.
2. Select **Monitor > Statistics > Virtual Port Statistics** from the Host Connectivity Manager.

Fields and components

Field	Description
Keep Running Data check box	Click to continue running statistical data. This is useful if you want to see a trend.
Polling Frequency in Seconds text box	Type a number for polling frequency. The range is between five and 3600 seconds and the default is five seconds.
Start Polling button	Click to manually poll the V_Port statistics.
Reset button	Click to reset all of the statistics to 0.
Date	The date and time of the most recent reset.
FDISCs Sent	The number of Fabric discoveries sent.
FDISCs Accepts	The number of times the system accepts Fabric discoveries.
FDISC Retries	The number of times a Fabric discovery is attempted.
FDISC Req Timeouts	The time that is required for a Fabric discovery.
FDISC RSP Errors	The number of Fabric discovery response errors.
FDISC Bad Accepts	The number of bad accepts.
FDISC Rejects	The number of times the system rejects Fabric discoveries.
FDISC Unknown Rsps	The number of unknown Fabric discovery occurrences.
FDISC Alloc Waits	The number of delayed Fabric discovery allocations.
LOGOs Sent	The number of times logouts occur.
LOGO Accepts	The number of times logouts are accepted.
LOGO Rejects	The number of times logouts are rejected.
LOGO Rsp Errors	The number of logout response errors.
LOGO Unknown RSPs	The number of unknown logout occurrences.
No NPIV Support	Indicates if there is no NPIV support.
Fabric Offlines	The number of fabrics that are offline.
Fabric Onlines	The number of fabrics that are online.
Fabric Cleanups	The number of fabric cleanups.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box:

- "Port Statistics dialog box"
- "Polling frequency rate"
- "Resetting statistics"
- "Performance monitoring"

Appendix

Brocade Command Utility

B

In this appendix

About the BCU

This appendix provides reference documentation for the Brocade Command Line Utility (BCU) supporting the Brocade Fibre Channel components.

BCU runs in two modes:

- Direct mode, where you type the command at the command prompt. For example:

  `bcu port --topology <port_id> <auto|p2p>`

- Shell mode, accessed using the bcu shell; for example, `bcu> port --topology <port_id> <auto|p2p>`.
  - To access the shell mode, type `bcu shell`.
  - To exit out of shell mode, type `exit`.

All the commands in this appendix are shown in the direct mode. For example:

`bcu port --topology <port_id> <auto|p2p>`

To list all the commands and subcommands, type the following command:

`bcu --help`

To check the CLI and Driver version number, type the following command:

`bcu --version`

BCU commands

The following table lists the Brocade Command Line Utility (BCU) commands alphabetically that are available for configuring the devices in a SAN environment that use a Brocade adapter.

Command	Operands	Synopsis
bcu --help		Lists all available sub-commands.
bcu <sub_command> --help		Lists all details about the specific subcommand.
Adapter commands		
bcu adapter	--list	
	--name	<serial-no> <adapter-name>
	--query	<ad_id>
	--enable	<ad_id>
	--disable	<ad_id>
Authentication commands		
bcu auth	--show	<port_id>
	--policy	<port_id> <on | off>
	--reinit	<port_id>
	--algo	<port_id> <md5 | sha1 | ms | sm>
	--secret	<port_id> “secret string”
	--stats	<port_id>

	--statsclr	<port_id>
BIOS commands		
bcu bios	--query	<port_id>
	--enable	<port_id> [-s *speed*] [-o *auto*|flash|firstlun] [-p *pos*] {-b pwwn,lun}*
	--disable	<port_id>
Boot commands		
bcu boot	--blunZone	-c <cfg> -p <port_wwn> -r <rport_wwn> -l <lun_id | lun#>
	--update	[adapter_id] <image_file> [-a]
Debug commands		
bcu debug	--portlog	<port_id>
	--portlogclear	<port_id>
	--portlogctl	<port_id> <enable | disable>
Diagnostic commands *Note: The sfpshow and beacon diagnostic tests are not available on the Brocade 804 mezzanine card.*		
bcu diag	--sfpshow	<port_id>
	--tempshow	<ad_id>
	--beacon	<port_id> {on | off} [<duration>]
	--pciloopback	<port_id> [-p <pattern>] [-c <frame_count>]
	--loopback	<port_id> [-t <loopback_type>] [-s <speed>] [-c <frame_count>] [-p <pattern>]
	--memtest	<port_id>
	--queuetest	<port_id> [-q <queue_num>]
Driver configuration commands *Note: Driver configuration commands are supported only on Windows operating systems.*		
bcu drvconf	--key	<key_name>
	--val	<value>
	Possible key_name and value ranges are: • key = bfa_ioc_queue_depth, value range [>0] default = 2048 • key = bfa_lun_queue_depth, value range [>0] default = 32 • key = ioc_auto_recover, value range [0-1] default = 1 • key = rport_del_timeout, value range [>0] default = 90 • key = msix_disable, value range [0-1] default = 1	
FC diagnostic commands		
bcu fcdiag	--fcping	<port_id> <rpwwn> [-l lpwwn]
	--fctraceroute	<port_id> <rpwwn> [-l lpwwn]
	--fcecho	<port_id> <rpwwn> [-l lpwwn]
	--linkbeacon	<port_id> {on|off}
	--scsitest	<port_id> <rpwwn> [-l lpwwn]
FCP initiator mode commands		

bcu fcpim	--query	<port_id> rpwwn [-l <lpwwn>]
	--stats	<port_id> <rpwwn. [-l <lpwwn>]
	--statsclr	<port_id> <rpwwn. [-l <lpwwn>
	--qdepth	<port_id> <q_depth_value>
	--modstats	<port_id>
	--modstatsclr	<port_id>
I/O Controller (IOC) commands (Storage)		
bcu ioc	--stats	<port_id>
	--statsclr	<port_id>
	--enable	<port_id>
	--disable	<port_id>
	--query	<port_id>
	--intr	<port_id> <-coalesce | c> {on | off} [<-l <usecs>] [-d <usecs>]
I/O Controller (IOC) commands (Networking)		
bcu ioceth	--stats	<port_id>
	--statsclr	<port_id>
bcu ethioc	--enable	<port_id>
	--disable	<port_id>
	--query	<port_id>
Log commands		
bcu log	--level	<port_id> [<Critical|Error|Warning|Info>] [-m <fw|hal|fcs|drv|aen|all>]
Logical port (lport) commands		
bcu lport	--list	<port_id>
	--query	<port_id> [-l <lpwwn>]
	--stats	<port_id> [-l <lpwwn>]
	--statsclr	<port_id> [-l <lpwwn>]
Port commands (physical port)		
bcu port	--list	
	--name	<port_id> [port_name]
	--enable	<port_id>
	--disable	<port_id>
	--stats	<port_id>
	--statsclr	<port_id>
	--query	<port_id>
	--topology	<port_id> {auto | p2p}
	--speed	<port_id> <speed>

	--dfsize	<port_id> [dfsize]
Target persistent binding commands *Note: Target persistent binding is available in Windows operating systems only.*		
bcu pbind	--list	<port_id> [<pwwn>]
	--clear	<port_id>
QoS commands		
bcu qos	--enable	<port_id>
	--disable	<port_id>
	--query	<port_id>
	--stats	<port_id>
	--statsclr	<port_id>
Target rate limiting commands		
bcu ratelim	--enable	<port_id>
	--disable	<port_id>
	--query	<port_id>
	--defspeed	<port_id> [<1|2|4>]
Remote port (rport) commands		
bcu rport	--list	<port_id> [-l <lpwwn>]
	--query	<port_id> <rpwwn> [-l <lpwwn>]
	--stats	<port_id> <rpwwn> [-l <lpwwn>]
	--statsclr	<port_id> <rpwwn> [-l <lpwwn>]
	--osname	<port_id> [-l <lpwwn>]
Virtual port (vport) commands *Note: vport commands are not supported on Solaris platforms.*		
bcu vport	--create	<port_id> <vpwwn> [-n <vnwwn>] [-s <sname>]
	--delete	<port_id> <vpwwn>
	--query	<port_id> <vpwwn>
	--stats	<port_id> <vpwwn>
	--statsclr	<port_id> <vpwwn>

adapter

Displays and sets adapter parameters. The adapters are HBA models 415, 425, 804, 815, and 825.

NOTE
When trunking is enabled, multiple physical ports are trunked together to form a logical Fibre Channel port.

Synopsis

bcu adapter --**enable** <*ad_id*>

bcu adapter --**disable** <*ad_id*>

bcu adapter --**list**

bcu adapter --**name** <*serial-no*> <*adapter-name*>

bcu adapter --**query** <*ad_id*>

Description

Displays and sets commands that apply to the physical adapter. There can be one or more PCI functions per adapter, which are referred to as *ports*. Each port exposes a logical Fibre Channel port, which typically equates to a physical Fibre Channel port.

Operands

When invoked without operands, this command displays the usage.

--**enable**	Enables the adapter.
ad_id	Specifies the ID of the adapter you want to enable.
--**disable**	Disables the adapter.
ad_id	Specifies the ID of the adapter you want to disable.
--**list**	Lists all adapters in the system. For each adapter in the system, a brief summary line is displayed.
--**name**	Displays or specifies the name of the adapter. The adapter name can be identified either by serial number or by adapter index. Note: Use an empty string (“ “) to clear a previous adapter name. Adapter names are stored persistently.
serial-no	Specifies the serial number or the ID of the adapter for which you want to display information.
adapter-name	Specifies the adapter name. The name can include up to 15 characters, must begin with a letter, can consist of letters, digits, hyphens, and underscore characters, but must not contain spaces. This operand is optional; if you do not specify an adapter name, the current adapter name displays.
--**query**	Queries or displays adapter information.
ad_id	Specifies the ID of the adapter for which you want to query.

Example

```
bcu adapter –list

AD # NP   HW-path      Type   Model-Info    Serial-num    Name
1    2    0000:01:00   FC     Brocade-825   ALX0301D062   - -
2    2    0000:09:00   FC     Brocade-825   ALX0411D01K   - -

bcu adapter –query 1
Example:# bcu adapter –query 1
Adapter Information:
       card type - FC
       model info: Brocade-825
       OEM info: N/A
       num ports: 2
       max speed: 8 Gbps
       chip revision: Rev-B
       hw path: 16:00
       Serial Num: ALX0301D062
       name:
PCI Information:
        vendor id:      0x1657
        device id:      0x0013
        ssid:           0x0014
        ssvid:          0x1657
        PCIe Gen: Gen 1
        PCIe lanes:     8 (Initial number of lanes = 8)
Flash Information:
        status: good
        fw version: FCHBA2.0.0.0
        bios version: brocade_adapter_boot_fw_v2-0-0-0


Flash Information:
        status: good
        fw version: FCHBA2.0
        bios version: FCHBA2.0

bcu adapter --name 1 emc-fab3_ad5
        adapter BRCD1234567’s name set to emc_fab3_ad5

bcu adapter --name 1
        adapter BRCD1234567’s name is emc_fab3_ad5
```

See Also “ioc”, “port”

auth

Enables authentication configuration on a per-port basis and the ability to display authentication status and statistics.

Synopsis

bcu auth --**algo** <*port_id*> <*md*|*sha1*|*ms*|*sm*>

bcu auth --**policy** <*port_id*> {*on*|*off*}

bcu auth --**reinit** <*port_id*>

bcu auth --**secret** <*port_id*> "*secret_string*"

bcu auth --**show** <*port_id*>

bcu auth --**stats** <*port_id*>

bcu auth --**statsclr** <*port_id*>

Description

Configure and display authentication settings and status.

Operands

--**algo** Sets the authentication algorithm.

port_id Specifies the ID of the port for which you want to display information.

md|*sha1*|*ms*|*sm*

- **MD5** - A hashing algorithm that verifies a message's integrity using Message Digest version 5. MD5 produces a 128-bit digest and is the required authentication mechanism for LDAP v3 servers.
- **SHA1** - A secure hashing algorithm that computes a 160-bit message digest for a data file that is provided as input.
- **MD5SH1** - Similar to the MD5 hashing algorithm, but used for DH-CHAP authentication
- **SHA1MD5** - Similar to the SHA1 hashing algorithm, but used for DH-CHAP authentication

--**policy** Turns authentication on or off. By default, the authentication policy is disabled. If authentication is enabled, the port attempts to negotiate with the switch. If the switch side does not participate in the authentication process, the port skips the authentication process. If the switch participates in the authentication and authentication fails, the port is placed in a link down state.

port_id Specifies the ID of the port for which you want to set the authentication policy.

on|*off* Specifies the state of the authentication policy: "policy 2/1 on" means authentication is turned on, "policy 2/1 off" means authentication is turned off.

--**reinit** Restarts the authentication on the port.

port_id Specifies the ID of the port for which you want to restart authentication.

--**secret** Sets the shared secret.

Note: You cannot clear the secret.

port_id Specifies the ID of the port for which you want to set the shared secret.

secret string	Specifies the secret string. The maximum length of the secret is 63 bytes. The default secret for each interface is its pwwn without the colons; for example, 0102030405060708.
–show	Displays the authentication settings and current status.
port_id	Specifies the ID of the port for which you want to display information.
–stats	Displays the authentication statistics.
port_id	Specifies the ID of the port for which you want to display information.
–statsclr	Clears the authentication statistics.
port_id	Specifies the ID of the port for which you want to clear statistical information.

Example Here is an example of the output when authentication is successful:

```
bcu auth –show 1/0
```

port	Port Status	Auth	Hash Type	Group Type
1/0	Linkdown	success	MD5	DH-NULL

Here is an example of the output when authentication failed:

```
bcu auth –show 1/0
```

port	Port Status	Auth	Hash Type	Group Type
1/0	Linkdown	failed	MD5	DH-NULL

Here is an example of the output when authentication is not enabled:

```
bcu auth –show 1/0
```

port	Port Status	Auth	Hash Type	Group Type
1/0	Linkup	no_auth		

```
bcu auth –policy 2/1 on
Authentication turned on

bcu auth –policy 2/1 off
Authentication turned off

bcu auth –secret 5/0 “mypasswd”
Authentication secret set

bcu auth –stats 4/1
successes: 1
failures: 0

auth_rx_stats:
auth_rjts: 0
auth_negs: 0
auth_dones: 0
dhchap_challenges: 2
dhchap_replies: 0
dhchap_successes: 1
```

```
auth_tx_stats:
auth_rjts: 0
auth_negs: 2
auth_dones: 0
dhchap_challenges: 0
dhchap_replies: 2
dhchap_successes: 0

auth –statsclr 4/1
Successfully cleared auth stats
```

See Also None

bios

Enables the basic input/output system (BIOS) in preparation for Boot Over SAN. The BIOS is the firmware code that, when first powered on, is a type of boot loader.

NOTE
Refer to the *Brocade Adapters Installation and Reference Manual* for more information about configuring BIOS.

Synopsis

bcu bios --**query** <*port_id*>

bcu bios --**enable** <*port_id*> [-*s speed*] [-*o auto*|*flash*|*firstlun*] [-*p pos*] {-*b pwwn,lun*}*

bcu bios --**disable** <*port_id*>

Description

You must enable BIOS to support boot over SAN for a port. If disabled, the host system cannot boot from Fibre Channel disk drives. BIOS must be enabled on only one adapter port per host in order to boot from SAN. The default setting for the boot BIOS is enabled.

The port ID can be any of the following:

- Adapter ID
- Port ID
- Port WWN
- Port name
- Port hardware path

Operands

--**query** Queries the boot-over-SAN configuration.

port_id Specifies the ID of the port for which you want to display information.

--**enable** Enables the boot over SAN configuration.

port_id Specifies the ID of the port for which you want to set the port's boot from SAN attributes.

s *speed* Specifies the port speed as auto-negotiate.

o *auto*|*flash*|*firstlun*

Specifies the following options for obtaining boot LUN information:

- auto - Enables auto-discovery. When enabled, the boot LUN identification is provided by the fabric.
- flash - The adapter obtains the boot LUN information from flash memory. Values are saved to flash when you configure them and save them through the BIOS Configuration Utility, HCM, and BCU.
- firstlun - The host boots from the first LUN visible to the adapter that is discovered in the fabric.

p *pos* Specifies the position for storing the boot LUN information in the -b pwwn, lun operand. The range is 0-3. The LUN information specified in position 0 is used first to boot from SAN, then information specified for positions 1, 2, and 3.

b *pwwn,lun*	Specifies the host boots from the LUN information defined by the target port world wide name (PWWN) and LUN value (lun*). Specify the PWWN as a colon-separated value and the LUN as a 64-bit decimal value. The LUN must be the same LUN that you bound to the port using the storage system's management or configuration utility.
–**disable**	Disables boot over SAN for the specified port, if enabled.
port_id	Specifies the ID of the port for which you want to disable the boot over SAN configuration.

Example

```
bcu bios –query 1/0
boot over SAN: enabled
port speed: Auto
Boot luns obtained from the flash
boot lun 0:
       target wwn: 50:00:1f:e1:50:10:eb:da
       lun: 0001-0000-0000-0000

Pre-boot Configuration:
       Speed: 2/4/8/Auto for 8G cards
       BIOS: Enabled/Disabled
       Number of boot luns: 8
       Boot LUN 0 : <Target's WWN>, <LUN>
       Boot LUN 1 : <Target's WWN>, <LUN>
       Boot LUN 2 : <Target's WWN>, <LUN>
       Boot LUN 3 : <Target's WWN>, <LUN>
       Boot LUN 4 : <Target's WWN>, <LUN>
       Boot LUN 5 : <Target's WWN>, <LUN>
       Boot LUN 6 : <Target's WWN>, <LUN>
       Boot LUN 7 : <Target's WWN>, <LUN>
```

See Also "boot"

boot

Allows the host's boot LUN information to be stored in the fabric zone database using a zone name containing the PWWN of an adapter port and zone members consisting of the storage target PWWN and LUN WWN. The adapter boot code can query the zone member list for the zone name that matches the adapter PWWN to determine the boot target and LUN.

NOTE
A system reboot is required for the newly-updated image to be effective.

Fabric OS 6.2 is required on adjacent switches to support fabric-based boot LUN discovery.

Refer to the *Brocade Adapters Installation and Reference Manual* for information about creating zones on the switch where the adapter is connected.

NOTE
On Solaris systems, the Download Boot Image menu is disabled if the host does not have a Fibre Channel HBA card or if the driver version is 1.1.0.7 or lower.

Synopsis

bcu boot --**blunZone** -c <cfg> -p <port_wwn> -r <rport_wwn> -l <lun_id | lun#>

bcu boot --**update** [adapter_id] <image_file> [-a]

Description

Boot commands allows the host's boot LUN information to be stored in the fabric zone database using a zone name and to update the boot code in flash.

Operands

--**blunZone**	Generates the zonecreate command to be run on the switch.
-c cfg	Specifies the boot LUN (BLUN) of the boot command.
-p port_wwn	Specifies the world wide name of the port.
-r rport_wwn	Specifies the world wide name of the remote port (rport).
-l lun_id	Specifies the ID of the logical unit. The LUN ID is specified as a hexadecimal byte; for example, FF.
-l lun#	Specifies the number of the logical unit. The LUN number is specified as a hexadecimal, eight-byte string; for example, 09AABBCCDDEEFF00.
--**update**	Updates the boot code in flash.
adapter_id	Specifies the ID of the adapter on which boot code is updated. The adapter id could be any one of the following: adapter serial number, adapter name, or adapter hardware path.
image_file	Specifies the name of the boot code image file.
-a	Indicates the boot code is updated to all the Brocade adapters found on the host. The adapter_id is not specified if -a is specified.

Example

```
bcu boot --blunZone -c BLUN -p 10:00:00:05:1e:41:9a:cb -r 50:00:00:05:1e:41:9a:ca
-l 09AABBCCDDEEFF00
```

To create the zone, copy the following line and run this command from the switch command line.

```
zonecreate “BFA_100000051E419ACB_BLUN”,”00:00:00:00:50:00:00:05;
00:00:00:01:1e:41:9a:ca; 00:00:00:02:09:aa:bb:cc, 00:00:00:03:dd:ee:ff:00”
```

See Also “bios”

debug

The debug commands gather support information on Fibre Channel components.

Synopsis bcu debug --**portlog** <*port_id*>

bcu debug --**portlogclear** <*port_id*>

bcu debug --**portlogctl** <*port_id*> <*enable* | *disable*>

Description Captures all the support information needed to diagnose suspected system issues.

Operands

--**portlog**	Displays the log of FC frames and other main control messages that were sent out and received. If the port log is disabled, the following message displays as the first line: Refer to the **portlogctl** command for more information: WARNING: port log is disabled.
port_id	Specifies the ID of the port for which you want to display the FC frame logs and other control messages.
--**portlogclear**	Clears the port's frame log.
port_id	Specifies the ID of the port for which you want to clear the port's frame log.
--**portlogctl**	Enables or disables the portlog.
port_id	Specifies the ID of the port for which you want to enable or disable the portlog.
enable	Enables the **portlogclear** command.
disable	Disables the **portlogclear** command.

Example

```
bcu debug --portlog 10/0
Total records present = 14
------------------------------------------------------------------------
time     event port code args
------------------------------------------------------------------------
08:35:28.430  fwm    10/0   00     00001234, 00050001
08:35:28.431  mbox   10/0   01     00001234, 00050001
08:35:28.433  ioctl  10/0   90     101d9910,0
08:35:28.433  Tx     10/0   164    02ffffd, 00ffffd, 0005ffff, 10000000
08:35:28.433  Rx     10/0   0      c0ffffd, 00ffffd, 00050006
08:35:28.433  Rx     10/0   164    03ffffd, 00ffffd, 00050006, 02000000
08:35:28.433  Tx     10/0   0      c0ffffd, 00fffd, 00050006
08:35:28.433  ioctl  10/0   91     103646d8, 0
08:35:28.466  ioctl  10/0   a7     3c, 1
08:35:28.483  Tx     10/0   96     02ffffd, 00ffffd, 0006ffff, 11100060
08:35:28.483  Rx     10/0   0      c0ffffd, 00ffffd, 00060007
08:35:28.483  Rx     10/0   96     03ffffd, 00ffffd, 00060007, 02100060
08:35:28.483  Tx     10/0   0      c0ffffd, 00ffffd, 00060007
08:35:28.483  ioctl  10/0   a1     0,0
------------------------------------------------------------------------

# bcu debug --portlog 1/1
Total records present = 26
------------------------------------------------------------------------
```

```
Time     Module   Event    Len  Log info
--------------------------------------------------------------------------------
13fe083a Driver   drvstrt  0    Driver Attach
14471130 HAL      pstchg   0    Port Linkup
1447135f FCXP     Tx       140  01290000,00000000,00080000,03000000
14471361 FCXP     Tx       32   01290000,00000000,00080000,62000000
14471498 FCXP     Rx       116  01980000,6c000000,051e7609,02000000
1447149c FCXP     Tx       301  20290000,00000000,00080000,01000000
1447150d FCXP     Rx       4    01980000,6d000000,051e7609,02000000
1447190e FCXP     Rx       16   20980000,6e000000,051e7609,01000000
14471910 FCXP     Tx       76   20290000,00000000,00080000,01000000
14471a29 FCXP     Rx       16   20980000,6f000000,051e7609,01000000
14471a2b FCXP     Tx       48   20290000,00000000,00080000,01000000
14471b28 FCXP     Rx       16   20980000,70000000,051e7609,01000000
14471b2a FCXP     Tx       44   20290000,00000000,00080000,01000000
14471b2d FCXP     Tx       140  01290000,00000000,00080000,03000000
14471c11 FCXP     Rx       116  01980000,71000000,051e7609,02000000
14471c18 FCXP     Tx       176  20290000,00000000,00080000,01000000
14471c19 FCXP     Tx       48   20290000,00000000,00080000,01000000
14471d1a FCXP     Rx       16   20980000,72000000,051e7609,01000000
14471e0e FCXP     Rx       16   20980000,73000000,051e7609,01000000
14472027 FCXP     Rx       788  20980000,74000000,051e7609,01000000
14472029 FCXP     Tx       48   20290000,00000000,00080000,01000000
14472144 FCXP     Rx       24   20980000,75000000,051e7609,01000000
14613597 FCXP     Tx       176  20290000,00000000,00080000,01000000
14613745 FCXP     Rx       16   20980000,76000000,051e7609,01000000
147fb9b6 FCXP     Tx       176  20290000,00000000,00080000,01000000
147fbb68 FCXP     Rx       16   20980000,77000000,051e7609,01000000
--------------------------------------------------------------------------------

bcu debug –portlogclear 1/0
portlog cleared

bcu debug –portlogctl 1/0 enable
portlog enabled

bcu debug –portlogctl 1/0 disable
portlog disabled

bcu debug –portlogctl 1/0 disable
portlog disabled
```

See Also None

diag

Lists the non-destructive group of diagnostic commands. The port can be identified using the adapter index, the port index, the port name, or the port world wide name.

NOTE
The sfpshow and beacon diag commands are not supported on the Brocade 804 mezzanine card.

Synopsis

bcu diag --**sfpshow** <*port_id*>

bcu diag --**tempshow** [*ad_id*]

bcu diag --**beacon** <*port_id*> {*on* | *off*} [<*secs*>]

bcu diag --**pciloopback** <*port_id*> <-p <*pattern*> [-c <frame_count>]

bcu diag --**loopback** <*port_id*> [-t <loopback_type>] [-s <*speed*>] [-c <frame_*count*>]

[-p <*pattern*>]

bcu diag --**memtest** <port_*id*>

bcu diag --**queuetest** <*port_id*> [-q <queue_num>]

Description

Displays the group of diagnostic commands that are non-destructive and indicates when the adapter is running at a normal operation state.

NOTE
You must disable the port prior to executing the loopback test. You must disable the adapter prior to executing the memtest.

Operands

--**sfpshow**	Monitors the attributes of the SFP. This is an online diagnostic test. Note: A notification occurs for any parameter that is not within the configured power, temperature, voltage, and current specification or policy.
port_id	Specifies the ID of the port on which you want to monitor the SFP attributes.
--**tempshow**	Reads the adapter's temperature sensor registers of the adapter. This is an online diagnostic test.
ad_id	Specifies the ID of the adapter for which you want to display temperature sensor registers.
--**beacon**	Controls the port and link end-to-end beaconing. This is an online diagnostic test.
port_id	Specifies the ID of the port for which you want to beacon.
on | *off*	Turns end-to-end beaconing on or off.
secs	Displays the beacon time duration in seconds. Beaconing is automatically turned off after the specified duration. If the duration is set to 0, beaconing continues until it is explicitly turned off.

--**pciloopback**	Checks the communications path between the host and the IO Controller (IOC).
port_id	Specifies the ID of the port for which you want to send a health check message.
-p pattern	Displays the data pattern.
-c frame_count	Specifies the frame count.
--**loopback**	Tests the data path from the IOC to the desired network loopback point (internal, serdes, external) and back. This is an offline diagnostic test.
port_id	Specifies the ID of the port on which you want to run a loopback test.
-t *loopback_type*	Specifies the loopback test type. Possible values include the following test types: • int - Internal loopback, the default • serdes - SerDes loopback • ext - External loopback). If the loopback type is not specified, all loopback tests run.
-s *speed*	Specifies the link speed as 8, 4, 2, or 1 Gbps. This is an optional parameter. If not specified, then 8, 4, and 2 Gbps speeds are tested on the 8 Gbps adapter and 4, 2, and 1 Gbps speeds are tested on the 4 Gbps adapter.
-c *frame count*	Specifies the frame count.
-p *pattern*	Specifies the pattern (must be one hex word).
--**memtest**	Performs a generic memory test using different algorithms.
port_id	Specifies the ID of the port on which you want to run a memory test.
--**queuetest**	Sends a health check message from the host to the firmware through message queues memory mapped over the PCI.
port_id	Specifies the ID of the port on which you want to run a queuetest.
-q queue_num	Specifies the CPE/RME queue number from 0 to 3. If the queue number is not specified, all queues are tested.

Example To display detailed information about a specific port:

```
# bcu diag --tempshow
temperature: 44.348787 C

# bcu diag --beacon 1/1 on
Port beacon turned on

# bcu diag --beacon 1/1 on
Link end-to-end beacon turned on
```

See Also "fcdiag"

drvconf

Sets the basic parameters for the driver to function properly.

Note: The **drvconf** commands are supported on Windows platforms only.

Synopsis bcu **–drvconf** [-key <*key_name*>] [--val <*value*>]

Description Changes the values for basic Windows registry entry parameters.

NOTE
You can directly change these values by editing the Windows registry entries for these values, or you can use the drvconf commands for the same purpose.

Operands

--**key** key_name	The name of the bfa key.
–val *value*	Sets the value of the bfa key. See below for possible values and default settings.

Possible key name and value ranges are as follows:

- key = bfa_ioc_queue_depth, value range [0-2048] default = 2048
- key = bfa_lun_queue_depth, value range [0- 32] default = 32
- key = ioc_auto_recover, value range [0-1] default = 1
- key = rport_del_timeout, value range [0-90] default = 90
- key = msix_disable, value range [0-1] default = 1
- key = pbind_enable, value range [0-1] default = 0

See Also None

fabric

Prints and resets Fabric statistics.

Synopsis bcu fabric --**stats** <*port_id*>

bcu fabric --**statsclr** <*port_id*>

Description Displays or clears Fabric statistics.

Operands

--**stats**	Prints the fabric statistics.
port_id	Specifies the ID of the fabric port for which you will print the statistics.
--**statsclr**	Resets the fabric statistics.
port_id	Specifies the ID of the fabric port for which you will reset the statistics.

Example

```
bcu fabric --stats 1/0
Fabric Stats:
FLOGI sent: 114
FLOGI rsp errors: 0
FLOGI accept errors: 0
FLOGI accepts: 58
FLOGI rejects: 0
FLOGI unknown rsp: 0
FLOGI alloc wait: 0
FLOGI received: 0
FLOGI rejected: 0
fabric offlines: 57
fabric onlines: 58
```

See Also None

fcdiag

Runs diagnostic tests on Fibre Channel components.

NOTE
The fcdiag --linkbeacon command is not supported on the Brocade 804 HBA.

Synopsis

bcu fcdiag --**fcping** <*port_id*> <*rpwwn*> [-l *lpwwn*]

bcu fcdiag --**fctraceroute** <*port_id*> <*rpwwn*> [-l *lpwwn*]

bcu fcdiag --**fcecho** <*port_id*> <*rpwwn*> [-l *lpwwn*]

bcu fcdiag --**linkbeacon** <*port_id*> {*on*|*off*}

bcu fcdiag --**scsitest** <*port_id*> <*rpwwn*> [-l *lpwwn*]

Description

Fibre Channel diagnostic tests evaluate the integrity of Fibre Channel components.

Operands

--**fcping**	Determines the basic connectivity between two Fibre Channel network points and monitors and measures network latency.
port_id	Specifies the ID of the port to which you want to issue a ping command.
rpwwn	Specifies the remote port world wide name to which you want to issue a ping command.
-l lpwwn	Specifies the logical port world wide name. This is an optional argument. The base port is specified as 0; otherwise, the port is a virtual port.
--**fctraceroute**	Reports on a SAN path, including node hops and latency data.
port_id	Specifies the ID of the port on which you want to run the fctraceroute command.
rpwwn	Specifies the remote port world wide name.
-l lpwwn	Specifies the logical port world wide name. This is an optional argument. The base port is specified as 0; otherwise, the port is a virtual port.
--**fcecho**	Sends an FC Echo Extended Link Services (ELS) request to a remote port.
port_id	Specifies the ID of the port from which you want to run the fcecho command.
rpwwn	Specifies the remote port world wide name on which you want to run the fcecho diagnostic test.
-l lpwwn	Specifies the logical port world wide name. This is an optional argument. The base port is specified as 0; otherwise, the port is a virtual port.
--**linkbeacon**	Blinks (toggles) the link beacon.
port_id	Specifies the ID of the port for which you want to run the linkbeacon command.
on | *off*	Specifies if the linkbeacon test is on or off.

--scsitest	Tests the SCSI components.
port_id	Specifies the ID of the port for which you want to run the scsitest command.
rpwwn	Specifies the remote port world wide name.
-l lpwwn	Specifies the logical port world wide name. This is an optional argument. The base port is specified as 0; otherwise, the port is a virtual port.

Example

```
bcu fcdiag --fctraceroute 2/0 50:05:07:63:04:13:46:eb
Error: Reject from attached fabric

bcu fcdiag --fctraceroute 2/0 50:05:07:63:04:13:46:eb
FC Traceroute completed successfully. Path Info:
```

Switch WWN	Switch Domain ID	Ingress Port #	Egress Port #
10:00:08:00:88:03:31:8b	127	5	11
10:00:08:00:88:03:31:8b	127	11	5

```
bcu fcdiag --fctraceroute 2/0 50:05:07:63:04:13:46:e1
FC Traceroute Failed. Reason : Destination Port not in Fabric

bcu fcdiag --fcecho 2/0 50:05:07:63:04:13:46:eb
FC ECHO completed successfully
```

See Also "diag"

fcpim

Enables or disables fast failover of initiator mode I/O. The default setting is off.

Synopsis

bcu fcpim --**stats** <*port_id*> <rpwwn> [-l <lpwwn>]

bcu fcpim --**statclr** <*port_id*> <rpwwn> [-l <lpwwn>]

bcu fcpim --**pathtov** <port_id> <*tov*>

bcu fcpim --**query** <*port_id*> rpwwn [-l <lpwwn>]

bcu fcpim --**modstats** <*port_id*>

bcu fcipim --**modstatsclr** <port_id>

Description

Enables or disables fast failover of the Fibre Channel Port (FCP) initiator mode I/O and displays or clears statistics.

Operands

--**stats**		Displays statistics related to the Fibre Channel port initiator mode.
	port_id	Specifies the ID of the port for which you want to display statistical information.
	rpwwn	Specifies the world wide name of the remote port for which you want to display statistics.
	-l lpwwn	Specifies the world wide name of the logical port for which you want to display statistics.
--**statclr**		Clears statistics related to the Fibre Channel port initiator mode.
	port_id	Specifies the ID of the port for which you want to clear statistical information.
	rpwwn	Specifies the world wide name of the remote port for which you want to clear statistics.
	-l lpwwn	Specifies the world wide name of the logical port for which you want to clear statistics.
--**pathtov**		Controls the fast failover initiator mode.
	port_id	Specifies the ID of the port for which you want to query.
	-tov	Specifies the optional path time out value in seconds (1 to 60). A value of 0 triggers the default timeout value. The default TOV is 30 seconds.
--**query**		Queries the fcpim attributes.
	port_id	Specifies the ID of the port for which you want to query.
	rpwwn	Specifies the world wide name of the remote port for which you want to query.
	-l lpwwn	Specifies the world wide name of the logical port for which you want to query.
--**modstats**		Displays statistics related to the Fibre Channel port initiator mode.
	port_id	Specifies the ID of the module for which you want to display statistical information.

–**modstatsclr**	Clears statistics related to the Fibre Channel port initiator mode.
port_id	Specifies the ID of the module for which you want to clear statistical information.

Example

```
bcu fcpim –stats 1/0 50:00:1f:e1:50:0d:da:a9
rport onlines:                  4
rport offlines:                 3
PRLI sent:                      4
PRLI Accepts:                   4
PRLI error responses:           0
PRLI responses parse err:       0
fcxp alloc waits:               0
Second level err recovery:      0
Num times in initiator mode:    0

HAL fcpim statistics
    online events:                  4
    offline events:                 3
    create events:                  1
    delete events:                  0
    create completions:             4
    delete completions:             2
    SLER events:                    0
    IOC down events:                1
    IO cleanup completions:         3
    task management commands:       0
    TM firmware responses:          0
    TM successes:                   0
    TM failures:                    0
    TM related IO cleanups:         0
    TM firmware queue resumed:      0
    TM affected by IOC down events: 0
    TM affected by ITN offline:     0
    TM offline cleanup completions: 0
    IO requests:                    456026
    IO completions:                 456026
```

See Also “ioc”
“vport”

ioc

Enables or disables the I/O Controller (IOC), which refers to the combination of port and the firmware controlling it.

The port can be identified using the adapter index, the port index, the port world wide name or the port name.

Synopsis

bcu ioc --**stats** <*port_id*>

bcu ioc --**statsclr** <*port_id*>

bcu ioc --**enable** <*port_id*>

bcu ioc --**disable** <*port_id*>

bcu ioc --**query** <*ioc_id*>

bcu ioc --**intr** <*port_id*> <-coalesce | -c> {on|off} [<Latency><Delay>]

Description

The IOC commands allow you to set the interrupt attributes for the port.

CAUTION

Disabling the IOC is a destructive operation.

Operands

--**stats**		Displays the IOC level statistics on the specified port.
	port_id	Specifies the ID of the port for which you want to display information.
--**statsclr**		Clears the IOC level statistics on the specified port.
	port_id	Specifies the ID of the port for which you want to clear statistical information.
--**enable**		Enables the IO Controller (IOC). If the IOC is already enabled, the command is ignored.
	port_id	Specifies the port of the IO Controller (IOC) you want to enable.
--**disable**		Caution: Disabling the IOC is a destructive operation. Disables the port of the IO Controller (IOC). If the IOC is already disabled, the command is ignored.
	port_id	Specifies the ID of the port you want to disable.
--**query**		Queries the attributes of the Storage IOC with the IOC ID.
	ioc_id	Specifies the port of the IO Controller (IOC) you want to enable.
--**intr**		Sets the interrupt attributes for the port.
	port_id	Specifies the ID of the port on which you want to set interrupt attributes.
	coalesce | c	Sets the coalesce flag.
	on|*off*	Sets the interrupt attributes for the port to on or off.
	-Latency	Sets the latency monitor timeout value. Latency can be between 0 to 225 microseconds. A latency value of 0 disables latency monitor timeout interrupt. The default latency value is 5 for an HBA.

-Delay Sets the delay timeout interrupt value. A delay can be between 0 to 1125 microseconds. A delay value of 0 disables the delay timeout interrupt. The default delay value is 25 for an HBA.

Example

```
#bcu ioc –query 1/0
chip rev:               Rev-B
manufacturer:           Brocade
serial#:                ARZ0351D00B
model_descr:            BR-1020
pwwn:                   10:00:00:05:1e:55:1d:3c
nwwn:                   20:00:00:05:1e:55:1d:3c
f/w ver:                pvt_bld03 05/05/2009 15.12.12
bios ver:
port count:             2
status is:              operational
ssid:                   0x0014
vendor id:              0x1657
device id:              0x0014
pci function:           0
IOC type:
interrupt coalescing:   on
interrupt delay:        25 us
interrupt latency:      0 us

# bcu ioc –stats 1/0
Num suspends: 7

bcu ioc –statsclr 1/0
ioc stats cleared.

bcu ioc –enable 1/0
ioc is enabled

bcu ioc –enable ad1_p0
ioc is already enabled

bcu ioc –disable 1/0
ioc is disabled

bcu ioc –disable ad1_p0
ioc is already disabled
bcu –intr 1/0 –coalesce off
interrupt coalescing has been turned off

bcu ioc –intr 1/0 –coalesce on
The intr settings have been configured with value(s):

Coalesce: on

bcu ioc –intr 1/0 –coalesce on 12 19
The intr settings have been configured with value(s):

Coalesce: on
Delay: 19 (micro-seconds)
Latency: 12 (micro-seconds)
```

See Also “adapter”
“lport”

log

Sets the log level for each module. If no log level is specified, the current level is used.

Synopsis bcu log –**level** <*port_id*> [<*Critical*|*Error*|*Warning*|*Info*>] [-m <fw|hal|fcs|drv|aen|all>]

Description The number of messages logged by the host depends on the predetermined logging level. Although the adapter might generate many messages, only certain types of messages are logged based on the specified logging level.

Operands

–**level** Specifies the number of messages logged by the host, which depends on the predetermined logging level.

port_id Specifies the ID of the port for which you want to set the log level.

Critical|*Error*|*Warning*|*Info*

Specifies the severity level. Supported log levels include Critical, Error, Warning, or Info. If no level is set, the default setting is used, which is Warning.

-m fw|*hal*|*fcs*|*drv*|*aen*|*all*

Example

```
#bcu log –level 2/0
FW log level is Warning
HAL log level is Warning
FCS log level is Warning
DRV log level is Warning
AEN log level is Warning

#bcu log –level 2/0 info
Log level set to Info

#bcu log –level 2/0
FW log level is Info
HAL log level is Info
FCS log level is Info
DRV log level is Info
AEN log level is Info
```

See Also None

lport

Lists the logical port (lport) commands.

Synopsis bcu lport --**list** <*port_id*>

bcu lport --**query** <*port_id*> [*-l lpwwn*]

bcu lport --**stats** <*port_id*> [*-l lpwwn*]

bcu lport --**statsclr** <*port_id*> [*-l lpwwn*]

Description Lists all the logical ports (lports) under a given port ID. A logical port is a port that is logged into a fabric. Possible logical port type values are the following:

- Base port
- Virtual port
- Logical port PWWN - logical port's port world wide name
- Logical port NWWN - logical port's port node world wide name
- FC addr - FC address of the logical port

Possible roles supported by the logical port are FCP initiator mode (IM), FCP target mode (FCPTM), and IP over FC support (IP).

Operands

--**list**	Lists all the lports for a specified port.
port_id	Specifies the ID of the port for which you want to display information.
--**query**	Lists the attributes of the logical port.
port_id	Specifies the ID of the port for which you want to display information.
-l lpwwn	Specifies the logical port's world wide name for which you want to display information. If the lpwwn is not specified, the base port is used.
--**stats**	Displays the logical port's statistics.
port_id	Specifies the ID of the port for which you want to display statistical information.
-l lpwwn	Specifies the logical port's world wide name for which you want to display statistical information. If the lpwwn is not specified, the base port is used.
--**statsclr**	Clears the logical port's statistics.
port_id	Specifies the ID of the port for which you want to clear statistical information.
-l lpwwn	Specifies the logical port's port world wide name for which you want to clear statistical information. If the lpwwn is not specified, the base port is used.

Example

```
bcu lport --list 1/0
Port ID: 1/0
Port Name:
Port PWWN: 10:00:00:05:1e:ae:e3:a4
Port NWWN: 20:00:00:05:1e:ae:e3:a4
HW Path: 0000.06:00.0
Num LPORTs: 5
```

```
# bcu lport –query hba5_port0
State:        Online
FC address:   0c0100
Port wwn:     aa:bb:cc:dd:ee:ff:aa:bb
Node wwn:     cc:dd:cc:aa:ff:cc:aa:ff
Symbolic name:
FC4 Role:     fcpim ipfc

# bcu lport –query hba5_port0 - 1 01:bb:cc:dd:ee:ff:00:01
State:        Online
FC address:   0c0101
Port wwn:     01:bb:cc:dd:ee:ff:00:01
Node wwn:     01:bb:cc:dd:ee:ff:00:00


# bcu lport –statsclr hba5_port0
lport stats cleared
```

The following are examples of a Brocade 1020 expansion card versus a Brocade 825 adapter:

```
1020 bcu lport --query

[root@HB081222-RH4u7x86 ~]# bcu lport --query 1/0
Port FC Addr:   860e01
Port Type:      Base Port (State: Linkup)
Port PWWN:      10:00:00:05:1e:8e:b6:02
Port NWWN:      20:00:00:05:1e:8e:b6:02
Symbolic name:  BR-1020 | 2.1.0.0 | HB081222-RH4u7x86 | Red Hat Enterprise Linux
AS release 4 (Nahant Update 7) |
Role:           FCP Initiator
Fabric Name:    10:00:00:05:1e:90:13:98
Switch IP Addr: 10.32.82.134
FPMA MAC Addr:  0e:fc:00:86:0e:01

825 bcu lport --query

[root@HB081222-RH4u7x86 ~]# bcu lport --query 2/0
Port FC Addr:   8a0600
Port Type:      Base Port (State: Linkup)
Port PWWN:      10:00:00:05:1e:0f:1a:b1
Port NWWN:      20:00:00:05:1e:0f:1a:b1
Symbolic name:  Brocade-425 | 2.1.0.0 | HB081222-RH4u7x86 | Red Hat Enterprise
Linux AS release 4 (Nahant Update 7) |
Role:           FCP Initiator
Fabric Name:    10:00:00:05:1e:05:09:29
Switch IP Addr: 10.32.82.138
```

See Also None

pbind

Enables target port world wide name (WWN) binding to a persistent target ID for an operating system (OS) stack.

Synopsis bcu pbind --**list** <*port_id*> [<*pwwn*>]

bcu pbind --**clear** <*port_id*>

Description Queries the list of mappings or clears existing persistent binding settings.

NOTE
The **pbind** command is only supported on the Windows platform.

Operands

--**list**		Queries the list of mappings from the persistent binding module.
	port_id	Specifies the ID of the port for which you want to display information.
	pwwn	Specifies the world wide name of the port.
--**clear**		Clears existing persistent binding settings.
	port_id	Specifies the ID of the port on which you want to clear existing persistent binding settings.

See Also None

port

Lists the port commands (the physical ports on the adaoter). The port can be identified by the adapter index, the port index, the port name, or the port world wide name.

NOTE
1 Gbps speed is not valid for an 8 Gbps HBA; 4 Gbps speed is not valid for a 4 Gbps HBA.

Synopsis

bcu port --**list**

bcu port --**name** <*port_id*> [*port_name*]

bcu port --**enable** <*port_id*>

bcu port --**disable** <*port_id*>

bcu port --**stats** <*port_id*>

bcu port --**statsclr** <*port_id*>

bcu port --**query** <*port_id*>

bcu port --**topology** <*port_id*> [{*auto*|*p2p*}]

bcu port --**speed** <*port_id*> <1|2|4|8|auto>

bcu port --**dfsize** <*port_id*> [<*dfsize*>]

Description

Lists all the physical ports for a given port identifier. Possible port identifiers could be any one of the following:

- Adapter ID
- Port ID
- Port WWN
- Port name (user assigned)
- Port hardware path

Operands

--**list**	Lists all the physical ports along with their basic attributes.
--**name**	Queries or sets the port name. You can clear the port name using an empty string (“ “).
port_id	Specifies the ID of the port for which you want to display information.
port_name	Specifies a new name for the port. The name can include up to 15 characters, must begin with an alphabetic letter, can consist of letters, digits, hyphens, and underscore characters, but no spaces. Naming a port is optional; if you do not specify a port name, the current port name displays.
--**enable**	Enables the physical port if it is disabled.
port_id	Specifies the ID of the port you want to enable.

--**disable**	Disables the physical port, if currently enabled. This is a destructive operation and affects normal operation of the port. The port is taken offline, all remote FCP sessions are logged out, and all outstanding I/Os are terminated. You are prompted before disabling occurs.
port_id	Specifies the ID of the port you want to disable.
--**stats**	Displays the physical port-level statistics.
port_id	Specifies the ID of the port for which you want to display statistical information.
--**statsclr**	Clears port-level statistics.
port_id	Specifies the ID of the port for which you want to clear statistical information.
--**query**	Queries and displays port-related details for a port.
port_id	Specifies the ID of the port for which you want to display information.
--**speed**	Queries or sets the port speed. The port speed can be changed dynamically (when the port is enabled). If the port is disabled, the new port speed setting takes effect when the port is re-enabled.
port_id	Specifies the ID of the port for which you want to set the port speed.
1|2|4|8|auto	Specifies the port speed. Possible values are auto (to auto-negotiate the speed) and 1, 2, 4, 8 speeds. **Note:** The 1 Gbps speed is not valid for an 8 Gbps HBA (825, 815) and the 8 Gbps speed is not valid for a 4 Gbps HBA (425, 415). All speeds are valid for a mezzanine card (804).
--**dfsize**	Queries or sets the port's maximum receive data field size. If you do not specify a value, the current receive buffer size displays. Note: The new receive data field size takes effect when the port is re-enabled.
port_id	Specifies the ID of the port for which you want to set the data field size.
df_size	Indicates the maximum supported receive data field size, in decimal value. If set to auto, the driver default value displays. Possible values are 512, 1024, 2048, and 2112. If set to 'auto,' the default value is used, which is 2112.
--**topology**	Queries or sets the port topology. The port topology can be changed dynamically (when the port is enabled). If the port is disabled, the new topology setting takes effect when the port is re-enabled.
port_id	Specifies the ID of the port for which you want to display or set the topology.
auto|p2p	Specifies the topology type. Supported topology modes are as follows: • auto - auto-discovers the topology • p2p - point-to-point • loop - loop mode **Note:** The topology setting will take effect after the port --disable and port --enable commands are executed.

Example

```
# bcu port –list
-------------------------------------------------------------------------
Port#  Type  PWWN/MAC               FC Addr/  Media  State       Spd
                                    Eth dev
-------------------------------------------------------------------------
 1/0 fc   10:00:00:05:1e:ae:e3:a4 dd0500 mz Linkup 4G
 1/1 fc   10:00:00:05:1e:ae:e3:a5 dd0500 mz Linkup 8G
 1/1 fc   10:00:00:05:1e:ae:e3:a6 -- mz Disabled --
 1/1 fc   10:00:00:05:1e:ae:e3:a7 -- mz Disabled --
-------------------------------------------------------------------------

# bcu  port –name 1/0 emc_fab3_ad5_p0
Port 1/0’s name set to emc_fab3_ad5_p0

# bcu  port –name 1/0
Port 1/0’s name is emc_fab3_ad5_p0

# bcu port –enable 2/1
port enabled

# bcu port –enable 2/1
port is already enabled

# bcu port –disable 2/1
port disabled

# bcu port –disable 2/1
port is already disabled

# bcu port –stats 4/0
tx_frames: 4096
tx_words: 202448224
rx_frames: 1024
rx_words: 10224844
lip_count: 2096
nos_count: 64
error_frames: 2
dropped_frames: 12
link_failures: 6
loss_of_syncs: 2
loss_of_signals: 8
primseq_errs: 2
invalid orrdered set: 0
nonframe coding err: 0
invalid_tx_words: 4
invalid_crcs_frames: 32
undersized frames: 0
oversized frames: 0
bad EOF frames: 0

# bcu port –statsclr dell_s1_ad0_p1
port stats cleared
```

```
# bcu port –query 1/0
port id:                1/0
port type:              FC
port instance:          0
port name:
Media: mz
pwwn: 10:00:00:05:1e:ae:e3:a4
nwwn:  20:00:00:05:1e:ae:e3:a4
Factory pwwn: 10:00:00:05:1e:ae:e3:a4
Factory nwwn: 20:00:00:05:1e:ae:e3:a4
state:                  Disabled
Speed:
        current:        4G
        configured:     Auto
Topology:
        current:        P2P
        configured:     P2P
SNIA port type:         N
supported classes:      Class-3
symbolic name:          Brocade-804 | 2.1.0.0 | BL490-2 | SUSE Linux
Enterprise Server 10 (i586) | PATCHLEVEL = 2
maximum frame size:     2112
receive bb credits:     48
transmit bb credits:    8
QOS:                    Disabled
TRL:                    Disabled
TRL default speed:      1G
Path TOV:               30 seconds
Beacon status:          Off
pbind status:           Enabled
Portlog:                Enabled


# bcu port –topology 1/1
Current topology: auto

# bcu port –topology 1/1 p2p
Topology set to p2p

# bcu port –topology 1/1 auto
Topology set to auto

# bcu port –speed 1/1 auto
Port speed set

# bcu port –dfsize 1/0 2112
Setting will be enforced after port --disable and port--enable

# bcu port –dfsize 1/0 auto
Setting will be enforced after port --disable and port--enable
```

See Also “adapter”
“ioc”

qos

Quality of Service (QoS) works in conjunction with the QoS feature on Brocade switch F_ports. The Fabric operating system (FOS) provides a mechanism to assign traffic priority (high, medium, or low) for a given source and destination traffic flow. By default, all flows are marked as medium.

Synopsis

bcu qos --**enable** <*port_id*>

bcu qos --**disable** <*port_id*>

bcu qos --**query** <*port_id*>

bcu qos --**stats** <*port_id*>

bcu qos --**statsclr** <*port_id*>

Description

Enables or disables Quality of Service (QoS).

Operands

--**enable**	Enables Quality of Service (QoS).
port_id	Specifies the ID of the port on which QoS is enabled.
--**disable**	Disables Quality of Service (QoS).
port_id	Specifies the ID of the port on which QoS is disabled.
--**query**	Queries the QoS details.
port_id	Specifies the ID of the port for which you want to display information.
--**stats**	Displays the QoS statistics.
port_id	Specifies the ID of the port for which you want to display statistical information.
--**statsclr**	Clears the QoS statistics.
port_id	Specifies the ID of the port for which you want to clear statistical information.

Example

```
bcu qos --query 1/0
```

See Also

None

ratelim

Enables or disables target rate limiting support on the HBA side.

Synopsis bcu ratelim --**enable** <*port_id*>

bcu ratelim --**disable** <*port_id*>

bcu ratelim --**query** <port_id>

bcu ratelim --**defspeed** <port_id> [<1|2|4>]

Description The target rate limiting feature is used to minimize congestion at the HBA port due to a slow drain device operating in the fabric at a slower speed. A remote port's operating speed is determined from the fabric. Traffic destined to the remote port is limited to its current operating speed.

The default rate limit is 1 Gbps. Target rate limiting (TRL) is supported only when the HBA port is connected to the fabric. Therefore, TRL is not supported when the port is directly connected with another device.

Possible port identifiers could be any one of the following:

- Adapter ID
- Port ID
- Port WWN
- Port name (user assigned)
- Port hardware path

NOTE
You must first enter the bcu port –disable <port_id> command, followed by the **port** --**enable** command, before the **ratelim** --**enable** or **ratelim** --**disable** commands take effect.

Operands

--**enable**	Enables target rate limiting, if currently disabled.
port_id	Specifies the ID of the port you want to enable.
--**disable**	Disables target rate limiting on the HBA, if currently enabled.
port_id	Specifies the ID of the port you want to disable.
--**query**	Queries the target rate limiting details.
port_id	Specifies the ID of the port for which you want to display information.
--**defspeed**	Sets the default target rate limiting speed. The default TRL speed must be supported and less than the maximum speed at which the card can operate.
port_id	Specifies the ID of the port on which you want to set the speed.
1|2|4	Sets the default target rate limiting speed on the HBA. Options are 1 Gbps, 2 Gbps, and 4 Gbps

See Also None

rport

Lists the commands that apply to a remote port in a fabric. A remote port is a port that is physically separated from the adapter.

Synopsis

bcu rport --**list** <*port_id*> [-l <*lpwwn*>]

bcu rport --**osname** <port_id> [-l <*lpwwn*>]

bcu rport --**query** <*port_id*> <*rpwwn*> [-l <*lpwwn*>]

bcu rport --**stats** <*port_id*> <*rpwwn*> [-l <*lpwwn*>]

bcu rport --**statsclr** <*port_id*> <*rpwwn*> [-l <*lpwwn*>]

Description

Lists all the remote ports (rports) under a given port ID.

Operands

--**list**	Lists all remote ports accessible for a given logical port.
port_id	Specifies the ID of the port for which you want to display rport information.
lpwwn	Specifies the logical port world wide name. This is an optional argument.
	Note: If the -l lpwwn argument is not specified, the base port is used.
--**osname**	Lists all the osnames of the remote ports that are visible through the local port.
port_id	Specifies the ID of the port for which you want to display osnames.
lpwwn	Specifies the logical port world wide name. This is an optional argument.
--**query**	Displays detailed attributes of a remote port.
port_id	Specifies the ID of the port for which you want to query attributes of a remote port.
rpwwn	Specifies the remote port world wide name for which you want to query attributes.
lpwwn	Specifies the logical port world wide name for which you want to query attributes of a remote port. This is an optional argument.
	Note: If the -l lpwwn argument is not specified, the base port is used.
--**stats**	Displays remote port statistics.
port_id	Specifies the ID of the port for which you want to display information.
rpwwn	Displays the remote port's port world wide name.
lpwwn	Displays the logical port world wide name. This is an optional argument.
	Note: If the -l lpwwn argument is not specified, the base port is used.
--**statsclr**	Clears the remote port statistics.
port_id	Specifies the ID of the port for which you want to clear remote port statistics.
rpwwn	Specifies the remote port's port world wide name for which you want to clear remote port statistics
lpwwn	Displays the logical port world wide name. This is an optional argument.

Example

```
bcu rport –list 2/0

-------------------------------------------------------------------------
FC Addr  Remote Port PWWN          QOS-P/F   SPD     State     F  df_sz
-------------------------------------------------------------------------
01fd01   50:00:1f:e1:50:10:09:48     U/0     ---     online     T  2048
01f701   50:06:01:60:41:e0:68:c0     U/0     ---     online     T  2048
01f202   50:06:0e:80:03:75:5e:05     U/0     ---     online     T  2048
01f002   20:02:00:0e:11:10:fc:25     U/0     ---     online     T  2048
01ff01   50:05:07:63:0e:04:12:ef     U/0     ---     online     T  2048
01fe01   50:06:01:60:3c:e0:0c:a3     U/0     ---     online     T  2048
01fc01   50:01:43:80:01:3b:fb:38     U/0     ---     online     T  2048
01f601   20:16:00:a0:b8:42:20:ac     U/0     ---     online     T  2048
-------------------------------------------------------------------------

bcu rport –query 1/0 21:00:00:04:cf:75:6a:04
RPORT FC Address:               01f701
RPORT port wwn:                 50:06:01:68:41:e0:68:c0
RPORT node wwn:                 50:06:01:60:c1:e0:68:c0
Status:                         online
Class of Service:               Class-3
Function:                       Target
Data Field size:                2048
Cont.Incr.seq_cnt(CISC):        Not Supported
Current Speed:                  ---
symbolic name:                  DGC     LUNZ            0324
Vendor:                         DGC
Product ID:                     DISK
Product Rev:                    0324
QOS priority:                   Unknown
QOS flow id:                    0
TRL enforced:                   No

bcu rport –stats 1/0 aa:bb:cc:dd:ee:ff:00:01
offlines:       1
onlines:        2
RSCN :          0
PLOGI sent:     2
PLOGI accepts : 2
PLOGI timeouts: 0
PLOGI failed:   0
PLOGI rejects : 0
PLOGI received: 0
PRLI  received: 0
ADISC sent:     0
ADISC received: 0
ADISC rejects : 0
ADISC accepts : 0
ADISC failed:   0
ADISC rejected: 0
LOGO sent:      0
LOGO accepts:   0
LOGO failed:    0
LOGO rejected:  0
LOGO received:  0
RPSC received:  0
RPSC rejects:   0
RPSC sent:      8
RPSC accepts:   0
RPSC failed:    8
```

```
RPSC rejected:  0

HAL rport statistics:
    uninit: create events:       1
    uninit: exception events:    0
    created: online events:      1
    created: delete events:      0
    created: IOC down:           0
    created: exception events:   0
    fw create: f/w responses:    2
    fw create: delete events:    0
    fw create: offline events:   0
    fw create: IOC down:         0
    fw create: exception events: 0
    online: offline events:      1
    online: delete events:       0
    online: IOC down events:     0
    online: exception events:    0
    fw delete: fw responses:     1
    fw delete: delete events:    0
    fw delete: IOC down events:  0
    fw delete: exception events: 0
    offline: delete events:      0
    offline: online events:      1
    offline: IOC down events:    0
    offline: exception events:   0
    delete: fw responses:        0
    delete: IOC down events:     0
    delete: exception events:    0
    delete pend: fw responses:   0
    delete pend: IOC downs:      0
    delete pend: exceptions:     0
    off-pending: fw responses:   0
    off-pending: deletes:        0
    off-pending: IOC downs:      0
    off-pending: exceptions:     0
    IOC down: offline events:    0
    IOC down: delete events:     0
    IOC down: online events:     0
    IOC down: exceptions:        0

bcu rport –statsclr 1/0 aa:bb:cc:dd:ee:ff:00:01
Successfully reset the rport level stats
```

See Also None

vport

Lists the commands that apply to a virtual port.

Synopsis

bcu vport --**create** <*port_id*> <*vpwwn*> [-*n* <*vnwwn*>] [-*s* <*sname*>]

bcu vport --**delete** <*port_id*> <*vpwwn*>

bcu vport --**query** <*port_id*> <*vpwwn*>

bcu vport --**stats** <*port_id*> <*vpwwn*>

bcu vport --**statsclr** <*port_id*> <*vpwwn*>

Description

The **vport** commands enable you to create and delete vports and display statistics about them.

NOTE
The **vport** commands are not supported on Solaris platforms.

Operands

--**create**	Adds a new V_Port in the base fabric. If the virtual fabric ID is not specified, the V_Port is created in the base fabric. FCP initiator mode is supported.
port_id	Specifies the ID of the port for which you want to add a new V_Port.
vpwwn	Adds the virtual port by its world wide name. The V_Port WWN is a required argument.
n *vnwwn*	Adds the virtual port by the node's world wide name for the V_Port. This is an optional argument. If not specified, the base port node's world wide name is used.
s *sname*	Adds the symbolic name for the virtual port. This is an optional argument.
--**delete**	Deletes the specified V_Port. This deletes all associated objects, such as any associated login sessions and active I/O requests.
port_id	Specifies the ID of the port for which you want to delete a V_Port.
vpwwn	Deletes the virtual port by its world wide name. The V_Port WWN is a required argument.
--**query**	Queries information about the V_Port. This provides the V_Port's status and information associated with FC-4s. If no port WWN is specified, the information provided is for the base V_Port.
port_id	Specifies the ID of the port for which you want to query V_Port information.
vpwwn	Queries the virtual port by its world wide name. The V_Port WWN is a required argument.
--**stats**	Displays the statistics that are associated with the V_Port. If you do not specify the port's world wide name, the statistics listed are for the base V_Port.
port_id	Specifies the ID of the port for which you want to display statistical information.
vpwwn	Displays the statistics for the virtual port by its world wide name. The V_Port WWN is a required argument.

–statsclr	Clears the statistics that are associated with the V_Port. If you do not specify the port's world wide name, the statistics listed are for the base V_Port.
port_id	Specifies the ID of the port for which you want to clear statistical information.
vpwwn	Clears the statistics for the virtual port by its world wide name. The V_Port WWN is a required argument.

Example

```
bcu vport –query 1/0 10:00:00:05:1e:ae:e3:03
Port wwn: 10:00:00:05:1e:ae:e3:03
Node wwn: 20:00:00:05:1e:ae:e3:a4
FC Addr: dd0504
State: online
Role: FCP initiator

bcu vport –stats hba5_port0
fdisc sent: 15
fdisc accepts: 7
fdisc retries: 8
fdisc timeouts: 2
fdisc rsp err: 18
fdisc acc bad: 9
fdisc rejects: 3
fdisc unknown: 0
fdisc alloc waits: 6
logo sent: 12
logo accepts: 8
logo rejects: 4
logo rsp err: 4
logo unknown rsp: 6
logo alloc waits: 6
no npiv: 7
fab offline: 5
fab online: 8
fab cleanup: 9

bcu vport –statsclr hba5_port0
vport stats cleared
```

See Also None

Appendix

C

HCM Troubleshooting

In this appendix

This section discusses known problems with HCM usability features and the workaround.

HCM tab navigation

Problem There are various places within the Host Connectivity Manager (HCM) where you cannot navigate without using the mouse on the KDE GUI on the Linux operating system. If you use the tab key to enter any of the fields listed below, you cannot exit the field without using the mouse.

The problem includes any of the following right pane properties:

Host > Properties fields

Host > Adapter fields

Adapter > Properties fields

Adapter > Ports fields

Port > Properties fields

Port > LPORT fields

Port > SFP fields

Port > POM fields

Base Port > Properties

Base Port > Remote Properties

Target > Properties

Target > LUNs

LUN > Properties

Master Log Details

Application Log Details

Workaround The Ctrl + Tab combination is the default in KDE GUI on Linux platforms. Therefore, the Ctrl + Tab combination is intercepted by the KDE shell. To navigate HCM using the keyboard, you must manually disable the Ctrl+ Tab shortcut.

HCM does not restrict duplicate WWNs if BCU is used to create V_Ports

Problem The HCM GUI should post an error message for duplicate V_Ports (detected in the Vports.db file) and prompt the user to remove the duplicate when it detects duplicate world wide names (WWNs), but it does not. The HCM does not restrict duplicate WWNs when the BCU is used to create V_Ports.

Workaround Do not use the BCU for virtual port management, because it does not handle duplicate V_Port world wide names. Instead, use only the HCM GUI to manage V_Ports.

RHEL4 U7 x86/x64 OS crashes after invalid operand from hcmagent

Problem With HCM open, the RHEL4 U7 x86/x64 operating system hangs within five to ten minutes of sitting idle. This happens only on RHEL4 U7 x86 kernel version (2.6.9-78). The error message in the /var/log/messages file indicates an illegal operand in the HCM agent.

Workaround Upgrade the kernel to the latest patch release: from 2.6.9-78 to 2.6.9-78.0.5.

Appendix

Glossary and Acronyms D

Available BB_Credit

A value used by a transmitter to determine permission to transmit frames and, if so, how many. The transmitter may transmit a frame when the available BB_Credit is greater than zero.

Available_receive_buffers

The current number of buffers in a receiving port that are available for receiving frames at link rate.

Bandwidth The maximum information-carrying capacity of a system.

Baud The encoded bit rate per second.

BCU Brocade Command Line Utility (BCU).

Beaconing A continuous signaling of error conditions on a LAN. Beaconing can occur either on the port or on one or both sides of the link (known as end-to-end beaconing).

Byte A group of eight data bits.

Class of service A frame delivery scheme exhibiting a specified set of delivery characteristics and attributes.

Credit Permission given by a receiving port to a sending port to send a specified number of frames.

DCFM Data Center Fabric Manager

Domain_ID An eight-bit value that identifies a domain.

FCP The Fibre Channel Protocol for mapping SCSI-3 operations to Fibre Channel.

FLOGI FC Fabric Login request.

FL_Port A switch port that is capable of arbitrated loop operations and is connected to one or more NL_Ports in an arbitrated loop topology.

FOS Fabric Operating System.

FPMA Fabric Provided MAC Address.

F_Port Fabric Port. A port on a switch to which an N_Port connects.

HBA The host bus adapter is a hardware facility in a node that provides an interface attachment.

HCM Host Connectivity Manager.

IOC I/O Controller.

ITL Initiator-Target-LUN. An Initiator Port (HBA controller) talks to one Target Port addressing one LUN.

LLDP	Link Layer Discovery Protocol.
Lossless Ethernet MAC	A full duplex Ethernet MAC supporting at least 2.5KB jumbo frames and implementing extensions to avoid Ethernet frame loss resulting from congestion.
LUN	Logical unit number. An address for an individual disk drive or virtual partition (volume) within a storage device.
LUN mapping	A process that makes a LUN available to some hosts and unavailable to other hosts.
MAC	Media Access Control.
MIB	Management Information Base.
MTU	Maximum Transfer Unit.
N_Port	A node port (a Fibre Channel host or storage port in a fabric or point-to-point connection) that is assumed to be incapable of arbitrated loop operations.
NPIV	N_Port ID Virtualization (NPIV) enables a single Fibre Channel protocol port to appear as multiple, distinct ports, providing separate port identification within the fabric for each operating system image behind the port (as if each operating system image had its own unique physical port).
Persistent binding	A Fibre Channel (FC) host bus adapter (HBA) feature that enables you to permanently assign a system SCSI target ID to a specific FC device, even though the device's ID on the FC loop may be different each time the FC loop initializes.
PFC	Priority Flow Control.
Port	A generic reference to an N_Port, NL_Port, F_Port, FL_Port, E_Port, or other type of Fibre Channel port.
Port name	A 64-bit unique identifier assigned to each Fibre Channel port. The port name is communicated during the login and port discovery processes.
R_Port	Remote port in a fabric. A remote port is a port that is physically separated from the adapter.
SNMP	Simple network management protocol, defined for providing network management and monitoring functions.
SAN	A storage area network configuration allowing multiple systems and storage devices to be interconnected using storage command protocols.
Switch_Name	A 64-bit unique Fibre Channel name assigned to a switch.
TLV	Type Length Value, where: • *Type* is a numeric code that indicates the kind of field this part of the message represents. • *Length* is the size of the value field, typically measured in bytes. • *Value* is a variable-sized set of bytes that contain data for this part of the message.

Topology	An interconnection scheme that allows multiple Fibre Channel ports to communicate. For example, point-to-point and arbitrated loop are Fibre Channel topologies.
VF	Virtual Fabric.
VLAN	Virtual Local Area Network.
WWNN	World Wide Node Name. The unique name for any particular node in the fabric; for example, an HBA.
WWPN	World Wide Port Name. The unique name for any particular port in the fabric. A WWNN can have multiple associated WWPNs.

D Glossary and Acronyms

Index

F

H

I

L

M

N

P

Q

R

S

T

V

W