53-1001253-01
09 June 09

Brocade Adapters

Troubleshooting Guide

Supporting CNA Models BR-1010, BR-1020

Supporting HBA Models BR-815, BR-825, BR-415, BR-425

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 Troubleshooting Guide	*53-1001253-01*	New document	June 2009

Contents

About this Document

In this chapter

How this document is organized

This manual provides troubleshooting information on Brocade host bus adapters (HBAs) and converged network adapters (CNAs). It 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, "Introduction to troubleshooting" provides an introduction and approach to troubleshooting adapter problems, as well as tips for gathering problem information. A checklist is also provided to verify that required procedures have been followed during installation.
- Chapter 2, "Isolating Problems" provides information on common adapter problems and procedures to diagnose and recover from these problems.
- Chapter 3, "Tools for Collecting Data" provides a summary of diagnostic and monitoring tools available through the HCM, Brocade Command Line Utility (BCU), Fabric OS commands, and host system to help you isolate and resolve adapter-related problems.
- Chapter 4, "Performance optimization" contains guidelines for optimizing adapter performance on your host system.
- Appendix A, "Event Message Reference" contains details on all event messages generated by adapter drivers.

NOTE
This publication is a companion guide to be used with the *Brocade Adapters Administrator's Guide*. That publication provides detailed information on adapter monitoring and diagnostic tools in Host Connectivity Manager (HCM) and the BCU.

Supported CNA hardware and software

This section describes adapter hardware and software support.

CNA support

The following FCoE CNAs are supported in this release:

- Brocade BR-1010. Single-port CNA with a per-port maximum of 10Gbps.
- Brocade BR-1020. Dual-port CNA with a per-port maximum of 10 Gbps.

NOTE
Install only Brocade-branded SFPs in these CNAs.

Fabric OS and switch support

Brocade CNAs must connect to Fibre Channel SANs and Ethernet data networks through a compatible FCoE switch. For a current list of compatible switches, refer to the latest CNA compatibility matrix. Log into Brocade Connect or the Partner Network through www.brocade.com. After login, select **Compatibility Matrices** from **Quick Links.**

Host operating system support

The following operating systems support Brocade Host Connectivity Manager (HCM), Brocade Command Line Utility (BCU), and HBA drivers.

HCM Support

- Windows Server 2003, version R2 with SP2
- Windows Server 2008
- Windows Server Core
- Linux RHEL4, RHEL5, SLES10, and SLES11
- Solaris 10 (x86 and SPARC)
- VMware ESX Server 3.5

  NOTE
  Drivers, BCU, and HCM Agent are supported only on the VMware “console” Operating System. HCM is supported only on the guest operating system on VMware.

- Windows Vista
- Windows XP

NOTE
Specific operating system service pack levels and other patch requirements are detailed in the current CNA release notes.

FCoE support

- Windows Server 2003, version R2 with SP2
- Windows Server 2008
- Windows Server Core
- Linux RHEL4, RHEL5, SLES10, and SLES11
- Solaris 10 (x86 and SPARC)
- VMware ESX Server 3.5

NOTE
Drivers, BCU, and HCM Agent are supported only on the VMware "console" Operating System. HCM is supported only on the guest operating system on VMware.

Specific operating system service pack levels and other patch requirements are detailed in the current CNA release notes.

Ethernet support

- Windows Server 2003, version R2 with SP2
- Windows Server 2008
- Windows Server Core
- Linux RHEL4, RHEL5, SLES10, and SLES11
- VMware ESX Server 3.5

NOTE
Refer to the latest CNA compatibility matrix for a list of supported host systems and operating systems. Log into Brocade Connect or the Partner Network through www.brocade.com. After login, select **Compatibility Matrices** from **Quick Links.**

Supported HBA hardware and software

This section describes HBA hardware and software support.

HBA support

The following Fibre Channel host bus adapters (HBAs) are supported in this release.

- Brocade 815. Single-port HBA with a per-port maximum of 8 Gbps using an 8 Gbps SFP+.
- Brocade 825. Dual-port HBA with a per-port maximum of 8 Gbps using an 8 Gbps SFP+.
- Brocade 415. Single-port HBA with a per-port maximum of 4 Gbps using a 4 Gbps SFP.
- Brocade 425 Dual-port HBA with a per-port maximum of 4 Gbps using a 4 Gbps SFP.

Notes:

- This publication only supports the HBA models listed above and does not provide information about the Brocade 410 and 420 Fibre Channel HBAs, also known as the Brocade 400 Fibre Channel HBAs.

- Although you can install an 8 Gbps SFP+ into a Brocade 415 or 425 HBA, only 4 Gbps maximum port speed is possible.
- Install only Brocade-branded SFPs in these HBAs.

Fabric OS and switch support

For a current list of servers, switches, and applications compatible with Brocade HBAs, refer to the latest HBA compatibility matrix. Log into Brocade Connect or the Partner Network through www.brocade.com. After login, select **Compatibility Matrices** from **Quick Links.**

Host operating system support

The following operating systems support Brocade Host Connectivity Manager (HCM), Brocade Command Line Utility (BCU), and HBA drivers:

- Windows Server 2003, version R2 with SP2
- Windows Server 2008
- Linux RHEL4, RHEL5, SLES10, and SLES11
- Solaris 10 (x86 and SPARC)
- VMware ESX Server 3.5

NOTE
Drivers, BCU, and HCM Agent are supported only on the VMware "console" Operating System. HCM is supported only on the guest operating system on VMware.

- Windows Vista (HCM only)
- Windows XP (HCM only)

NOTE
Specific operating system service pack levels and other patch requirements are detailed in the current HBA release notes.

What's new in this document

This is a new document. For further information about new features not covered in this document and documentation updates for this release, refer to the adapter release notes.

Document conventions

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

Text formatting

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

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

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

Command syntax conventions

Command syntax in this manual follows these conventions:

command	Commands are printed in bold.
--**option, option**	Command options are printed in bold.
-**argument,** arg	Arguments.
[ ]	Optional element.
variable	Variables are printed in italics. In the help pages, values are underlined or enclosed in angled brackets < >.
...	Repeat the previous element, for example “member[;member...]”
value	Fixed values following arguments are printed in plain font. For example, **--show** WWN
|	Boolean. Elements are exclusive. Example: **--show -mode** egress | ingress

Command examples

This book describes how to perform configuration tasks using the Fabric OS command line interface and the BCU interface, but does not describe the commands in detail. For complete descriptions of all commands, including syntax, operand description, and sample output, see the *Fabric OS Command Reference* and *Brocade Adapters Administrator's Guide*.

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 technical glossaries on Brocade Connect. See "Brocade resources" on page xv for instructions on accessing Brocade Connect.

For definitions specific to this document, see the *Brocade FCoE Installation and Reference Manual*.

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, Windows Server 2003, Windows Server 2008, Vista, XP, PE for Windows, Hyper V for Windows, Windows Automated Installation Kit (WAIK)
Sun Microsystems, Inc.	Solaris
Red Hat Inc.	Red Hat Enterprise Linux (RHEL)
Novell, Inc	SUSE Linux Enterprise Server (SLES)
VMware Inc.	ESX Server
SPARC International, Inc	SPARC

Additional information

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

Brocade resources

For adapter resources, such as product information, software, firmware, and documentation, visit the following websites:

- HBA web site at www.brocade.com/hba.
- CNA web site at www.brocade.com/cna

To get up-to-the-minute information, join Brocade Connect. Go to *http://www.brocadeconnect.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

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

Providing details for support

Contact your Brocade FCoE CNA support supplier for hardware, firmware, and software support, including product repairs and part ordering. Provide the following information:

1. General information:
   - Brocade adapter model number
   - Host operating system version
   - Software name and software version, if applicable
   - syslog message logs
   - bfa_supportsave output.

     To expedite your support call, use the bfa_supportsave feature to collect debug information from the driver, internal libraries, and firmware. You can save valuable information to your local file system and send it to support personnel for further investigation. For details on using this feature, refer to "Support Save overview" on page 65.
   - 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.
2. Adapter serial number:

   The adapter serial number and corresponding bar code are provided on the serial number label illustrated below. This label is affixed to the adapter card.

   

   You can also display the serial number through the following HCM dialog boxes and BCU commands:

   - Adapter **Properties** tab in HCM.

     Select an adapter in the device tree, then click the **Properties** tab in the right pane.

- **BCU adapter –list** command.

  This command lists all adapters in the system and information such as model and serial numbers.

3. Port World-Wide Port Name (PWWN).

   Determine this through the following resources:

   - Label affixed on adapter card provides the WWPN for each port.
   - Brocade BIOS Configuration Utility.

     Select the appropriate adapter port from the initial configuration utility screen, then select **Adapter Settings** to display the WWNN and PWWN for the port. For details, refer to "Configuring BIOS using the Brocade configuration utility" on page 75.

   - Port **Properties** tab in HCM.

     Select a port for a specific adapter in the device tree, then click the **Properties** tab in the right pane.

   - The following BCU commands:

Command	Function
port --query <port_id>	Displays port information, including the PWWN for the FCoE port. The <port_id> parameter is the port number.
port --list	Lists all the physical ports on the CNA along with their basic attributes, such as the PWWN.

4. Media access control (MAC) addresses (CNAs only)

   The CNA card MAC address can be found in HCM by selecting the CNA in the device tree and clicking the **Properties** tab in the right pane. This displays the CNA **Properties** panel. Look for the **MAC Address** field.

   Each port has two "burned-in" MAC addresses.

   - CEE MAC address.

     This is the MAC address of the FCoE port and the source MAC for LLDP communications between the CNA and FCoE switch. To find this MAC address, perform one of the following tasks:

     - Select a CEE port in the HCM device tree, then click the **Properties** tab in the right pane to display the port **Properties** panel. Look for the **Local port MAC** field.
     - Select an FCoE port n the HCM device tree, then click the **Properties** tab in the right pane to display the port **Properties** panel. Look for the **FCoE MAC** field.

   - Ethernet MAC address.

     This MAC address is used for normal Ethernet operations. To find this MAC address using HCM, select an Ethernet port in the HCM device tree, then click the **Properties** tab in the right pane to display the port **Properties** panel. Look for the **Current MAC address** field.

   Each enode logging into the fabric through a local CNA port is assigned a MAC address during FCoE Initialization Protocol (FIP) operations. This MAC is assigned for the current FCoE communication only. To find this MAC address, perform one of the following tasks:

   - Select an FCoE port in the HCM device tree, then click the **Properties** tab in the right pane to display the port **Properties** panel. Look for the **FCoE MAC** field.

- Enter the **port –query <port_id>** BCU command: Look for the FCoE MAC.

The FCoE Forwarder (FCP) MAC address is the address of the attached FCoE switch. Select an FCoE port in the HCM device tree, then click the **Properties** tab in the right pane to display the port **Properties** panel. Look for the **FCF MAC** field.

You can also determine port MAC addresses using the following BCU commands.

Command	Function
port ---query <port_id>	Displays port information, including the MAC addresses. The <port_id> parameter is the port number.
port ---list	Lists all the physical ports on the CNA along with their Ethernet and FCoE MAC addresses.

NOTE
For details on using HCM and BCU commands, refer to the Brocade Adapters Administrator's Guide.

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 Introduction to troubleshooting

In this chapter

How to use this manual for troubleshooting

An adapter, such as an HBA or CNA, is one component of a larger network consisting of switches, storage devices, host systems and the cabling and connections to these components. Although there may be a problem in the adapter or an adapter component, the problem could also originate in another network component or connections between these components. Before removing and replacing adapters, launching adapter diagnostics, or even gathering statistics on adapter operation, it is important that you perform the following tasks:

1. Fully describe the problem and gather complete information about the symptoms that suggest a problem exists. Refer to "Gathering problem information" on page 2.
2. Isolate or resolve the problem by first using information in Chapter 2, "Isolating Problems".

   Adapter problems are organized under the following categories:

   - "General HBA and CNA problems"
   - "HBA problems"
   - "Ethernet network interface problems (CNA only)"
   - "FCoE and Fibre Channel problems"
   - "CEE network problems (CNA only)"

   Search through the list of problems in Table 2 on page 5. Problems are organized in the table by problem title, category, and whether the problem is operating-system-specific. Click on a problem to go to the chapter section containing details of possible causes and actions for resolution.

   Each problem section in Chapter 2 provides a complete description of the problem, possible causes, and actions for resolution. Fixes and actions may reference BCU commands, HCM features, and host operating system commands described in Chapter 3, "Tools for Collecting Data" which you can use to further isolate or resolve the problem.

   Other helpful sections in Chapter 2 include the following:

   - "Adapter driver installation verification" on page 34.
   - "Verifying Fibre Channel and CEE links" on page 32.
   - "Additional references for isolating problems" on page 37

3. Use the BCU commands, HCM features, and host operating system commands described in Chapter 3, "Tools for Collecting Data" to gather data for resolving problems. Although many of these tools are specifically referenced for problems described in Chapter 2, many more are included that can provide helpful data for troubleshooting, such as event logs, operating statistics, and diagnostics.
4. Consider these factors when isolating and resolving the problem:
   - Can the issue be resolved using the latest supported combination of host system BIOS, operating system, operating system updates, or adapter drivers?
   - Does the issue persist when the adapter is installed in a different platform or is connected using a different switch port, SFP, and cable?
   - Can this problem be reproduced on one or more adapters, port, or host system? Can you identify specific steps that consistently reproduce this problem on one or more hosts?
   - Is the problem documented in release notes for the adapter, operating system, or host system BIOS?
   - Is the problem documented in release notes for the switch and target storage system?
   - Is unexpected behavior intermittent or always present?

   If the problem is in a Fibre Channel or FCoE switch, cabling, storage device, or in connectivity between these components, refer to documentation, help systems, or service providers of that equipment.
5. If you cannot resolve the problem, gather and provide problem information to your adapter support provider for resolution.

NOTE
If troubleshooting information in this manual does not resolve problems, check the installed version of the adapter (chip revision) and driver (fw version) using the BCU **adapter –query** command. To use this command, refer to "Collecting adapter data using BCU commands" on page 45. Also refer to release notes posted on the Brocade adapter website for known problems relating to the adapter and driver versions. The HBA website is www.brocade.com/hba. The CNA website is www.brocade.com/cna.

Gathering problem information

Perform the following tasks to obtain as much information as possible before contacting technical support. Be sure to take careful notes for use as a record and reference.

- Describe the symptoms that you are observing. Be specific. Here are some examples:
  - User experiences, such as slow performance or file access.
  - LEDs not functioning on an adapter port that is connected to the fabric.
  - All LEDs on adapter port flashing amber.
  - Expected storage devices not visible from the HCM or host system's storage management application.
  - Adapter not recognized by host system BIOS.
  - Adapter not recognized as PCI device by host system operating system.
- What happened prior to the observed symptoms?
- Describe all observed behavior that is unexpected and compare against expected behavior.

- Gather information for support:
  - Use appropriate tools on storage targets to gather information such as disk, tape, and controller model and firmware levels.
  - Run the **bfa_supportsave** BCU command on the host system and save output to a file on your system.

    This command captures all driver, internal libraries, firmware, and other information needed to diagnose suspected system issues.You can save captured information to the local file system and send it to support personnel for further investigation.
  - Run the Fabric OS **supportSave** command on any Brocade switch and save output. This command collects RASLOG, TRACE, supportShow, core file, FFDC data and other support information.

  For details on using the Support Save feature, refer to "Support Save" on page 42.
- Draw a topology map of the SAN from the adapters to the storage targets. Include the components described in Table 1.

TABLE 1 Topology map details

Component	How to identify
adapter	Model, World-Wide Name (WWN), and driver release level.
Fibre Channel switches	Model, WWN, and Fabric OS version.
Fiber optic links between adapter, switches, and storage ports	Port WWNs connected to all links.
Host hardware	Model and hardware revision.

The **bfa_supportSave** and FOS **supportsave** commands can provide current information for the topology map. Also, consider using the Brocade SAN Health products to provide information on your SAN environment, including an inventory of devices, switches, firmware versions, and SAN fabrics, historical performance data, zoning and switch configurations, and other data. Click the **Support** tab on www.brocade.com for more information on these products.

- Run appropriate diagnostic tools for storage targets.
- Determine what has changed in the SAN. For example, if the SAN functioned without problems before installing the adapter, then the problem is most likely in the adapter installation or configuration, adapter hardware, or adapter driver package. Other examples to investigate could be changes in the switch or storage system firmware, an offline switch, or a disconnected or faulty cable between the adapter, switch, or storage controller fiber optic ports.
- Record the time and frequency of symptoms and the period of time symptoms have been observed.
- Determine if unexpected behavior is intermittent or always present.
- List steps that have been taken to troubleshoot the problem, including changes attempted to isolate the problem.

1 Gathering problem information

Chapter

2

Isolating Problems

In this chapter

How to use this chapter

Operation problems are arranged in this chapter in these categories:

- "General HBA and CNA problems"
- "HBA problems"
- "Ethernet network interface problems (CNA only)"
- "FCoE and Fibre Channel problems"
- "CEE network problems (CNA only)"

Use Table 2 to quickly navigate to sections in this chapter on specific problems. Each problem section in this chapter contains a description of the problem, possible causes, and actions for resolution.

TABLE 2 Isolate adapter problems

Problem	Category	OS Specific
"Adapter not reported under server's PCI subsystem"	"General HBA and CNA problems"	All
"No adapters reported though BCU adapter --list command"	"General HBA and CNA problems"	All
"Port link is not active"	"General HBA and CNA problems"	All
"Errors when installing brocade_driver_linux_<versions>.tar.gz package"	"General HBA and CNA problems"	Linux
"Installer program does not autorun (Windows only)"	"General HBA and CNA problems"	Windows
"Host system freezes or crashes"	"General HBA and CNA problems"	All
"Operating system errors (blue screen)"	"General HBA and CNA problems"	All

TABLE 2 Isolate adapter problems

Problem	Category	OS Specific
"Failed to connect to agent on host... error when using HCM"	"General HBA and CNA problems"	All
"Driver event messages appearing in host system log files"	"General HBA and CNA problems"	All
"Files needed for bfad.sys message appears"	"General HBA and CNA problems"	Windows
"Cannot roll back driver on all adapter instances using Device Manager"	"General HBA and CNA problems"	Windows
"BCU version mismatch warning"	"General HBA and CNA problems"	All
"I/O data traffic issues"	"General HBA and CNA problems"	All
"Quality of Service (QoS) performance issues"	"HBA problems"	All
"Unable to create more than 126 Virtual (NPIV) ports for HBA"	"HBA problems"	All
"Host not booting from remote LUN"	"HBA problems" "UEFI boot problems"	All
"Boot devices not available in host's Boot Manager menu"	"HBA problems" "UEFI boot problems"	All
"Target not visible from host"	"HBA problems" "BIOS boot problems"	Windows
"LUN not visible from host"	"HBA problems" "BIOS boot problems"	Windows
"<CTL-B> option does not display when booting host"	"HBA problems" "BIOS boot problems"	Windows
"No target devices found or link down! message displays in Brocade BIOS Configuration menu"	"HBA problems" "BIOS boot problems"	Windows
"Unable to boot from the stored boot device settings in the adapter"	"HBA problems" "BIOS boot problems"	Windows
"Remote LUNs are not visible to the host"	"HBA problems" "BIOS boot problems"	Windows
"Boot from SAN may stop on some Hewlett Packard hosts"	"HBA problems" "BIOS boot problems"	Windows
"Adapter <port id>: BIOS not installed displays during boot process"	"HBA problems" "BIOS boot problems"	Windows
"Ethernet link ports or LOM not coming up on reboot in Linux"	"Ethernet network interface problems (CNA only)"	Linux
"Loss of adapter hardware address in Linux"	"Ethernet network interface problems (CNA only)"	Linux
"Loss of adapter IP address in Linux"	"Ethernet network interface problems (CNA only)"	Linux
"Ethernet link ports or LOM not coming up on reboot in Linux"	"Ethernet network interface problems (CNA only)"	Linux
"Ethernet loopback test problems"	"Ethernet network interface problems (CNA only)"	All

TABLE 2 Isolate adapter problems

Problem	Category	OS Specific
"Network stack runs out of heap"	"Ethernet network interface problems (CNA only)"	VMware
"NIC numbering unexpected on VMware systems"	"Ethernet network interface problems (CNA only)"	VMware
"Poor network performance"	"Ethernet network interface problems (CNA only)"	Linux Windows
"VLAN creation and operation problems"	"Ethernet network interface problems (CNA only)"	Windows
"Loss of sync and loss of signal errors in port statistics"	"FCoE and Fibre Channel problems"	All
"Ping to remote server is failing"	"Ethernet network interface problems (CNA only)"	All
"Fabric authentication failures"	"FCoE and Fibre Channel problems"	All
"I/Os are not failing over immediately on path failure in MPIO setup"	"FCoE and Fibre Channel problems"	Windows Linux VMware
"Disk I/O requests causes low throughput and high latency on Linux"	"FCoE and Fibre Channel problems"	Linux
"Disk I/O requests causes low throughput and high latency on VMware"	"FCoE and Fibre Channel problems"	VMware
"Adapter is not showing in the fabric"	"FCoE and Fibre Channel problems"	All
"Virtual devices not listed in name server"	"FCoE and Fibre Channel problems"	All
"Adapter not registering with the name server or cannot access storage"	"FCoE and Fibre Channel problems"	All
"FCoE link is down"	"FCoE and Fibre Channel problems"	All
"I/O problem on connected FCoE device"	"FCoE and Fibre Channel problems"	All
"CEE is not enabled"	"CEE network problems (CNA only)"	All

General HBA and CNA problems

This section provides resolution for common problems that could with installed CNAs or HBAs, such as the adapter not being reported under the server's PCI subsystem or BCU adapter --list command, or the port link to the switch is not active.

Adapter not reported under server's PCI subsystem

The adapter is installed but not visible as a device in the host system's PCI subsystem.

Verify whether the adapter is visible as a PCI device by executing your host's operating system command to list PCI devices in the system. For details on this command, refer to the "List PCI Devices" row in Table 5 on page 40. If the adapter is not in the device list, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

1. **Possible Cause:** Card not seated properly.

   Action: Reseat the adapter.

2. **Possible Cause:** Server slot issues.

   Action: Install an adapter of known working condition to determine whether there is a slot malfunction.

   Action: Try installing the adapter into a different slot, if available.

3. **Possible Cause:** Adapter not compatible with host operating system or connected storage systems.

   Action: Verify compatibility by reviewing the *Brocade Server Connectivity Compatibility Matrix*. To find this document, log into Brocade Connect on www.brocade.com, then select the Compatibility Information quick link under Documentation Library.

No adapters reported though BCU adapter --list command

If the adapter does not display when the BCU **adapter –list** command is initiated, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

1. **Possible Cause:** Adapter is not reported under server's PCI subsystem.

   Action: Verify if the adapter is visible as a PCI device by executing your host's operating system command to list PCI devices in the system. For details on this command, refer to the "List PCI Devices" row in Table 5 on page 40.

   Action: If the adapter does not appear in the list of PCI devices, refer to "Boot devices not available in host's Boot Manager menu" on page 18 for possible causes and recommended actions.

2. **Possible Cause:** Adapter driver is not loaded.

   Action: Verify if the adapter is visible as a PCI device by executing your host's operating system command to list PCI devices in the system. For details on these commands, refer to the "List PCI Devices" row in Table 5 on page 40.

Port link is not active

The link between the adapter and switch port does not appear to be active because of adapter LED operation, lack of data over the link, or BCU **port –query** or **port –list** command shows that the link state is down. Refer to "Displaying the port list" on page 73 for more information.

Refer to the following descriptions of possible causes and recommended actions or fixes for the problem.

1. **Possible Cause:** SFP or cable problems.

   Action: Ensure that the SFPs and cables are connected properly on both adapter and switch sides. Check for any cable damage.

2. **Possible Cause:** Switch port is disabled or switch is disabled.

   Action: Execute either the Fabric OS **switchShow** or **portShow** commands on the attached switch to ensure that the switch or individual port is not disabled or offline. Use appropriate switch commands to enable the port.

3. **Possible Cause:** Adapter port is disabled. Verify port state using the HCM **Port Properties** dialog box or BCU **port –list** command. Use BCU **port –enable** command to enable the port.

4. **Possible Cause:** Adapter's port speed or topology mismatch with the switch port (HBA only).

   Action: Check the port topology setting on the switch using the Fabric OS **portCfgShow** command to ensure that Locked L_Port is OFF. Use the **portCfgLport** command to change the setting to OFF if required.

   Action: Check the switch port speed using the Fabric OS **portCfgShow** command to verify that speed is either AUTO or matches the speed of the attached adapter port (for example, the speed setting for both ports is 4 Gbps).

   Action: Check port speed on the adapter with the BCU **port –list** or **port –query** commands to display the current and configured speed. Refer to "Displaying port speed" on page 73 and "Performing a port query" on page 73 for details on using these commands.

5. **Possible Cause:** Non-Brocade branded SFP installed. If non-Brocade branded SFPs are inserted on the adapter or switch, the port link will not come up.

   Action: On the switch, execute the Fabric OS **switchShow** command to verify that "Mod_Inv" (invalid module) does not display for the port state.

   Action: On the adapter, execute the **port –list** or **port –query** BCU commands to verify the adapter. Refer to "Displaying the port list" on page 73 and "Performing a port query" on page 73. If an unsupported SFP is detected, the **Sfp** field displays 'us' (unsupported SFP) for port --list and the **Media** field displays "Unsupported SFP" for port --query.

   For additional actions and fixes for the port link not coming up, refer to "Verifying Fibre Channel and CEE links" on page 32.

6. **Possible Cause:** Firmware failure. In most cases this causes a heartbeat failure, and if auto-recovery is enabled, the driver recovers. No corrective action is needed.

   Action: If link does not recover and BCU **port –list** command shows fcoe and eth state is **link down**, download the latest driver package from the Brocade adapter website (www.brocade.com/hba or www.brocade.com/cna). Remove and reinstall the driver package using instructions in the "Installation" chapter of the *Brocade Adapters Installation and Reference Manual*.

Errors when installing brocade_driver_linux_<versions>.tar.gz package

If errors occur when installing the noarch brocade_driver_linux_<versions>.tar.gz driver package, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: Appropriate distribution kernel development packages are not installed on your host system for the currently running kernel.

Action: If you are installing the noarch driver package, the driver module compiles on the system during installation. If driver build errors result when you install the package, verify that the appropriate distribution kernel development packages are installed on your host system for the currently running kernel. These should include the gcc compiler and the kernel sources. If these are not installed, you may need to reinstall the operating system before continuing installation. Be sure to “install everything” including the developer library options.

Installer program does not autorun (Windows only)

If the installer program does not automatically run from the CD that you create with the ISO file containing all supported software installation packages, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

NOTE
This ISO file can be downloaded from the CNA and HBA websites (www.brocade.com/cna or www.brocade.com/hba).

Possible Cause: Autorun is not enabled on your system.

Action: Refer to “Installer program does not autorun (Windows only)” on page 10 for more information to isolate this problem.

Host system freezes or crashes

If the BIOS and the operating system recognize the adapter, but the host system freezes or crashes during startup and does not boot, refer to the following descriptions of possible causes and recommended actions to help resolve the problem

Possible Causes:

- Faulty fiber optic cabling and connections.
- Faulty or unseated SFPs or unsupported SFPs.
- Conflicts with port operating speed or topology of attached devices.
- Adapter not compatible with host system.

Action: Disconnect all devices from the adapter, then reboot the host system.

- If the system does not freeze when rebooted and operates correctly, use the following information to resolve the problem:
  a. Check for faulty cable and cable connections.
  b. Try rebooting the system without any connectivity to the switch. This will help isolate any hang caused by switch and device interactions.

c. Reseat SFPs in the adapter. Determine whether the installed SFPs are faulty by observing LED operation by the adapter ports. If all LEDs are flashing amber, the SFP is invalid and may not be a required Brocade model. You can also verify SFP operation by replacing them with SFPs in known operating condition. If the problem is resolved after replacement, original SFP is faulty.

d. Check for conflicts with attached devices. Verify that data speed (1-8 Gbps) and connection topology (for example, point-to-point) for devices attached to the adapter are compatible with settings on the adapter port. Although *auto* may be set, configuring settings manually on the adapter port and devices may allow connection. Also, note that the adapter only supports point-to-point connection topology. Refer to the *Brocade Adapters Administrator's Guide* for procedures to configure adapter ports.

NOTE
Observe the LEDs by adapter ports. Illuminated LEDs indicate connection, link activity, and connection speed negotiated with the attached device. For the meaning of LED operation, refer to the *Brocade Adapters Installation and Reference Manual*.

- If the system freezes perform the following tasks:

a. Verify whether the host system firmware supports PCIe specifications listed in the *Brocade Adapters Installation and Reference Manual*. If not, download a firmware update to support the adapter.

b. Verify compatibility by reviewing the Brocade Server Connectivity Compatibility Matrix. To find this document, log into Brocade Connect on www.brocade.com, then select the Compatibility Information quick link under Documentation Library.

c. On Windows systems, determine when the system freezes during the boot process. If it freezes as the driver loads, uninstall and reinstall the driver. If it freezes during hardware recognition, uninstall both the driver and adapter, then reinstall both.

d. Remove the adapter and reboot the system. If the system boots, reinstall the adapter.

e. Reseat the adapter.

f. Uninstall and reinstall the driver.

g. Try installing the adapter into another host system. If the problem does not occur, the adapter may not be compatible with the original host system. If the problem occurs in the new system, replace the adapter.

Action: Refer to "Verifying Fibre Channel and CEE links" on page 32 for more information to isolate this problem.

Operating system errors (blue screen)

If critical errors display for the host system and the system blue screen appears, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: Adapter driver not loaded.

Action: Refer to "Adapter driver installation verification" on page 34 for methods to verify driver installation.

Failed to connect to agent on host... error when using HCM

An “Adapter failed to connect to agent on host...” message indicates that the client application cannot connect to the HCM Agent listening on the configured port - normally TCP port 34568. Refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Causes:

- The agent is not running.
- The agent is not accepting connections on the expected port.
- The agent is not listening on the expected port.
- Communication between the client and agent is blocked by a firewall preventing access to the port (usually only a consideration for remote HCM management).

Action: For Linux, Solaris, and VMware systems, perform the following steps to help isolate the problem:

1. Verify that the agent is running by executing the appropriate **status** command for your operating system as described in the *Brocade Adapters Installation and Reference Manual*. Refer to the section on modifying HCM agent operation.
2. If you receive a message that the hcmagent is stopped, restarting the agent should resolve the problem. To restart, use the appropriate **start** command for your operating system which is also described in the *Brocade Adapters Installation and Reference Manual*.

   Note that one command described in the manual restarts the agent, but the agent will not restart if the system reboots or the agent stops unexpectedly. Another command restarts the agent, but the agent will restart if the system reboots.
3. Confirm the HCM agent is responding to requests using the expected user password. Execute the following command to connect to the HCM agent and force it to collect the adapter driver supportsave data.

   NOTE
   This command is a single line. The localhost can be replaced with a different IP address.

   ```
   wget --no-check-certificate
   https://admin:password@localhost:34568/JSONRPCServiceApp/
   SupportSaveController.do
   ```

   If successful, the file SupportSaveController.do (actually a zip format file) will contain the data from the HCM agent.
4. If you are managing a VMware host system through HCM from a remote system, the host’s firewall may be blocking TCP/IP port 34568, which allows agent communication with HCM.

   Use the following command to open port 34568:

   ```
   /usr/sbin/esxcfg-firewall-o 34568,tcp,out,https
   ```

   Use Windows Firewall and Advanced Service (WFAS) to open port 34568.

   NOTE
   You can change the default communication port (34568) for the agent using procedures in the “Installation” chapter of the *Brocade Adapters Installation and Reference Manual*. Refer to the section on modifying HCM agent operation.

5. If HCM is still unable to connect to the HCM agent after using the preceding steps, collect the following data and send to your Support representative for analysis:
   - Data collected from the previous step in SupportSaveController.do.
   - Data from the HCM application SupportSave feature. Select **Tools** > **SupportSave** to generate a supportsave file. The data file name and location displays when the SupportSave feature runs.
   - Adapter agent files on the adapter host (where the HCM agent is installed). Collect these files using the following command:

     ```
     tar cvfz hbaagentfiles.tgz /opt/hbaagent
     ```

     Output collects to hbaagentfiles.tgz.
   - Data collected on the adapter host from the bfa_supportsave feature using the following command:

     ```
     bfa_supportsave
     ```

     Output collects to a file and location specified when the SupportSave feature runs.

Action: For Windows systems, perform the following steps on to help isolate the problem:

1. Verify that the agent is running by executing the appropriate **status** command for your operating system described in the *Brocade Adapters Installation and Reference Manual*. Refer to the section on modifying HCM agent operation.
2. If you receive a message that the hcmagent is stopped, restarting the agent should resolve the problem. To restart, use the appropriate **start** command for your operating system which is also described in the *Brocade Adapters Installation and Reference Manual*.

   Note that one command described in the manual restarts the agent, but the agent will not restart if the system reboots or the agent stops unexpectedly. Another command restarts the agent, but the agent will restart if the system reboots.
3. If the HCM agent starts, verify which TCP port the agent is listening on by executing the following command at the Windows command prompt:

   ```
   netstat -nao | findstr 34568
   ```

   Output similar to the following should display.

   ```
   TCP    0.0.0.0:34568          0.0.0.0:0              LISTENING       1960
   ```

   The value 1960 in the last column is the process identifier for the Windows process listening on the TCP port. Note that this identifier may be different on your system.
4. Enter the following command to confirm that the process identifier bound to TCP port 34568 is for the hcmagent.exe process:

   ```
   tasklist /svc | findstr 1960
   ```

   The following should display if the identifier from step 3 is bound to TCP port 34568:

   ```
   hcmagent.exe                 1960 hcmagent
   ```

5. If you are managing a Windows 2008 host system through HCM from a remote system, the host's firewall may be blocking TCP/IP port 34568.

   Use Windows Firewall and Advanced Service (WFAS) to open port 34568.

NOTE
You can change the default communication port (34568) for the agent using procedures in the *Brocade Adapters Installation and Reference Manual*. Refer to the section on modifying HCM agent operation.

6. If the hcmagent is running and listening on port 34568 and there are no firewall issues (as explained in step 5), but you get the same “Failed to connect to agent on host..." error when using HCM, collect the following data. Send this data to your support representative for analysis:

   - Copies of output from the commands in step 3 and step 4.
   - Files from the output directory created after you execute the support save feature.

     To collect these files, execute the following command:

     ```
     bfa_supportsave
     ```

     Support data is collected to a file in your system’s tmp directory by default. For more information on using the Support Save feature, refer to “Support Save” on page 42.
   - Build information for the HCM application. Select **Help > About** in HCM to display the version, build identification, and build date.
   - Support data from the HCM application SupportSave feature.

     Select **Tools > SupportSave** to generate a supportsave file.

     If HCM cannot connect to the agent, a message displays an error (Agent Support Save could not be collected) and explains that only a basic collection is possible. Messages also display that provide the location of the zip file created.

     By default, a zip file is created in the following location.

     C:\Program Files\BROCADE\FCHBA\client\data\localhost\supportsave

     The zip file will have a name similar to the following:

     SupportSave_Basic_2008723_0_50_57.zip

Driver event messages appearing in host system log files

If event messages for the adapter driver are appearing in the host system log files, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: Various causes and severity levels.

Action: Follow the recommended action in the message.

Action: Resolve critical-level messages and multiple major or minor-level messages relating to the same issue as soon as possible.

Action: For details on event messages, refer to “Logs” on page 48.

Files needed for bfad.sys message appears

If a “Files needed for bfad.sys” message appears on Windows systems when removing a driver, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: This occurs if you perform the following sequence of steps:

1. Install the driver using the driver installer program (brocade_installer.bat) or Brocade Adapters Software Installer (GUI or command-based application).
2. Uninstall the Brocade adapter using Windows Device Manager.
3. Re-install the driver using the driver installer program (brocade_installer.bat) or Brocade Adapters Software Installer (GUI or command-based application).
4. Uninstall the driver using the driver installer program (brocade_installer.bat) program.

Action: To avoid this problem, do not uninstall the driver using the Device Manager if you have used the Brocade installer driver installer programs to install driver instances. Always use the Brocade installer programs. If only one driver is present in the system, then the Brocade programs also remove the Fibre Channel devices from the Device Manager.

Cannot roll back driver on all adapter instances using Device Manager

If you cannot roll back the driver for all adapter instances using Windows Device Manager, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: Installing the driver using the Brocade driver installer program (brocade_installer.bat) or Brocade Adapters Software Installer (GUI or command-based application), then rolling back driver adapter instances using the Device Manager.

Actions: Perform the following actions:

- Install the driver for each adapter instances using the Device Manager, then roll back the driver using Device Manager.
- Use the driver installer program (brocade_installer.bat) or Brocade Software Installer (GUI or command-based application) to install or upgrade the driver, then use the Brocade Software Uninstaller to roll back drivers on all adapter instances in one step.

BCU version mismatch warning

BCU output includes warning about version mismatch.

Symptom: Output from BCU commands has following warning message.

```
WARNING: BCU and Driver versions don’t match !!!
```

Possible Cause: Installation may be incomplete. Either the BCU or one or more driver instances were not upgraded to the latest version.

Action: Remove the driver package, then reinstall. Refer to the “Installation” chapter in the Brocade Installation and Reference Manual.

I/O data traffic issues

I/O data traffic issues are occurring, such as an application is not receiving data, FTP problems on an Ethernet network, ping failures, or data is not reaching a target on a Fibre Channel network.

1. **Possible Cause:** Ethernet traffic problem (CNAs only).

   Action: Run the Ethernet loopback serdes test on the suspected Ethernet port using the BCU **ethdiag –loopback <port_id> -t serdes** command. This tests internal adapter hardware components. If the test passes, suspect the following external problems:

   - Faulty fiber
   - Faulty software
   - Destination host problem

   Action: Run the BCU Ethernet external loopback test using the BCU command **ethdiag –loopback <port_id> -t ext**. Be sure that a loopback connector is installed in the port. If the serdes or internal loopback test passes, but the external test fails, suspect the following problems:

   - Loopback connector not inserted in transceiver
   - Faulty SFP or loopback connector.

2. **Possible Cause:** Fibre Channel or FCoE I/O problems.

   Action: Run the loopback serdes test on the suspected Fibre Channel port (HBA only) or FCoE port (CNA only) using the BCU **diag –loopback <port_id> -t serdes** command. If the test passes, suspect the following external problems:

   - Faulty fiber
   - Faulty software
   - Target problem

   Action: Run the BCU external loopback test using the BCU command **diag –loopback <port_id> -t ext**. Be sure that a loopback connector installed in the port. If the serdes or internal loopback test passes, but the external test fails, suspect the following problems:

   - Loopback connector not inserted in transceiver
   - Faulty SFP or loopback connector.

HBA problems

This section provides information for resolving problems more specific to HBA function.

Quality of Service (QoS) performance issues

If enabling QoS is causing poor performance, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

NOTE
QoS is not supported on CNAs.

1. **Possible Cause:** QoS is not enabled on both switch and adapter port.

   Action: Verify if QoS is enabled for an adapter port using the **qos -query <port_id>** BCU command. Verify if it is enabled on the switch using the **islShow** command.

   Action: Verify zones on the switch using the Fabric OS **cfgActvShow** command.

2. **Possible Cause:** QoS zones not created properly on switch for high, medium, and low priority targets.

   Action: Verify that QoS is configured on switch using instructions in the *Fabric OS Administrator's Guide*.

Unable to create more than 126 Virtual (NPIV) ports for HBA

If you cannot configure more than 126 N-Port ID Virtualization (NPIV) ports (maximum is 255 for Fiber Channel) refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: The maximum NPIV limit for the connected switch has been reached.

Action: Execute the Fabric OS **configure** command on the attached switch and change the maximum logins per port parameter under the **F_Port login parameters** menu to increase the maximum NPIV IDs allowed per port.

UEFI boot problems

This section describes problems that may occur when using the Brocade adapter and unified extensible firmware interface (UEFI) for booting a host system from a remote storage device (boot over SAN). Possible causes and recommended actions to help resolve the problems are provided.

NOTE
Currently, the Brocade CNAs do not support the boot over SAN feature.

Host not booting from remote LUN

If the host system where the adapter is installed does not boot from the remote boot LUN, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: Boot from LUN not configured correctly.

Action: If booting the host from a remote boot device, verify whether "boot over SAN" configuration is complete and correct. For example, verify the following:

- A zone is created on the attached switch that contains only the PWWN of the storage system port for the boot LUN and the PWWN of the adapter port.
- BIOS or EFI is enabled to support boot over SAN from a specific adapter port.
- BIOS or EFI is configured to boot from a specific LUN.
- The host's operating system, adapter driver, and other necessary files are installed on the boot LUN.

Boot devices not available in host's Boot Manager menu

Fibre Channel attached boot devices do not appear in the EFI Boot Manager Menu or a boot device appears, but it is not functioning. Following are descriptions of possible causes and recommended actions or fixes for the problem.

1. **Possible Cause:** Adapter is not seated properly.

   Action: Select the EFI Shell from the EFI Boot Menu and use the **devices** command to determine if EFI has detected the Brocade adapter.

   A Brocade adapter will have "Brocade Fibre Channel" in the device name. A CNA will also have "Brocade Ethernet Controller" in a device name.

   If the adapter is not listed, perform the following steps:

   - Reseat the adapter.
   - Replace the adapter with an adapter in known working condition to determine whether there is a slot malfunction.

2. **Possible Cause:** Host system slot Issues.

   Action: Perform the following steps:

   a. Reseat the adapter.

   b. Replace the adapter with an adapter in known working condition to determine whether there is a slot malfunction.

   c. Reinstall the adapter in a different slot.

3. **Possible Cause:** Adapter is not compatible with host operating system or connected storage systems.

   Action: Verify compatibility by reviewing the *Brocade Server Connectivity Compatibility Matrix*. To find this document, log into Brocade Connect on www.brocade.com, then select the Compatibility Information quick link under Documentation Library.

4. **Possible Cause:** No Fibre Channel attached drives are available from the Fibre Channel switch.

   Action: Check for attached disk devices.

   a. Use the **devices** EFI shell command to display the detected devices.

      A Brocade HBA may display as:

      ```
      29 B X -  1  2  8 Brocade Fibre Channel HBA
      ```

      "29" is the device handle, and will be different in most systems. More than one Brocade adapter may display.

   b. Use the EFI shell **oh** command to display additional information about each Brocade adapter. This will include any attached Fibre Channel disk devices. For example, you would enter the following for the HBA with device handle 29:

      ```
      Shell> dh -d 29
      ```

      The following displays:

      ```
      29: PciIo ScsiPassThruExt BusSpecificDriverOverride DevPath
      (..P0A08,300)/Pci(0|0)/Pci(0|0))
      ...
           Managed by :
      ```

```
        Drv[25] : Brocade Fibre Channel Adapter Bus Driver
        Drv[26] : SCSI Bus Driver
...
     Child Controllers  :
        Child[70] : SCSI Disk Device
        Child[71] : SCSI Disk Device
        Child[72] : SCSI Disk Device
```

The SCSI Disk Devices under “Child Controllers” are the LUNs that the Fibre Channel Adapter can access.

If an expected Fibre Channel attached disk does not appear in the “dh -d” list for a Brocade adapter, check the cabling, the adapter’s link status LEDs, and the Fibre Channel switch configuration.

NOTE
The Brocade adapter port may have been disabled with the EFI shell **drvcfg** command. Use the **drvcfg -s** shell command to check the enabled status and configuration of the port, including the requested speed. After entering **drafted -s** select the appropriate adapter from the **Adapter List** screen and press **Enter** to view and modify port properties.

BIOS boot problems

This section describes problems that may occur when using the Brocade adapter and Basic Input/Output System (BIOS) for booting a host system from a remote storage device (boot over SAN). Possible causes and recommended actions that may fix the problems are provided.

NOTE
Currently, the Brocade CNAs do not support the boot over SAN feature.

Target not visible from host

If the storage target configured for containing the boot LUN is not visible from the host, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

1. **Possible Cause:** No fabric connectivity between adapter and target or target is not online.

   Action: Execute the Fabric OS **nsAllShow** command on the attached switch to verify that the target and the host are online in the fabric and registered in the name server.

2. **Possible Cause:** The target and the adapter are not on the same zone.

   Action: Execute the Fabric OS **cfgActvShow** command on the attached switch and verify that the host and target are in the same zone (either using domain area members, port area members, or port or node WWNs)

3. **Possible Cause:** The adapter driver is not loaded.

   Action: The adapter driver may not be loaded. Refer to “Verifying Fibre Channel and CEE links” on page 32 for methods to verify driver installation

4. **Possible Cause:** There is a problem with the remote port.

   Action: Verify that the remote target port (rport) is reporting itself online by comparing rport online and rport offline statistics. Refer to "Remote port statistics" on page 59 for details on displaying these statistics. The rport online counter should be one greater than the rport offline counter. If not, clear the counters and try connecting to the remote port again. Verify the rport online and rport offline statistics again.

LUN not visible from host

If the LUN from which the host system will boot is not visible from the host system, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

1. **Possible Cause:** Missing or improper storage array LUN masking setting.

   Action: Check LUN mapping and masking using storage array configuration tools.

2. **Possible Cause:** Adapter driver not loaded.

   Action: The adapter driver may not be loaded. Refer to "Adapter driver installation verification" on page 34 for methods to verify driver installation.

<CTL-B> option does not display when booting host

When booting the host, the CTL-B option does not display so that you can access the **BIOS Configuration** menu.

1. **Possible Cause:** The adapter might not be loaded with the latest adapter boot image (bfa_boot_fw).

   Action: Download bfa_boot_fw from the HBA website (www.brocade.com/hba) and load to option ROM on adapter using the **BCU boot –upload** command.

2. **Possible Cause:** Due to memory constraints system BIOS might not be able to execute the Brocade adapter option ROM.

   Action: Disable option ROM on several add-in cards installed in system.

No target devices found or link down! message displays in Brocade BIOS Configuration menu

"No target devices found or link down" message displays on Brocade BIOS configuration menu during boot device discovery.

1. **Possible Cause:** There is no fabric connectivity between the Brocade adapter and target, or the target is not online.

   Action: Execute the Fabric OS **nsAllShow** command on the attached switch to verify that the target and the host are online in the fabric and registered in the name server.

2. **Possible Cause:** The target and the adapter port are not on the same zone.

   Action: Execute the Fabric OS **cfgActvShow** command on the attached switch and verify that the host and target are in the same zone by using either domain area members, port area members, or port or node WWNs.

3. **Possible Cause:** The link between the adapter port and target is not active yet.

   Action: Check that the speeds for the adapter port and the connected switch port match. The best approach is to set both speeds to “auto” or “autonegotiate.”

Unable to boot from the stored boot device settings in the adapter

The host is unable to boot from the boot device settings stored in the adapter. A “No boot LUNs configured” message will display next to the adapter value when booting.

1. **Possible Cause:** In the Brocade BIOS Configuration Utility, the **Boot LUN** field In the **Adapter Settings** screen is set to **Auto Discover** or **First LUN**.

   Action: Change the **Boot LUN** setting on the **Adapters Settings** screen to **Flash Values.** Refer to “Configuring boot over SAN” **on page 74** for details.

2. In HCM, the boot option is set to **Auto Discovered from Fabric** or **First Visible LUN** in the **Boot over SAN** dialog box.

   Action: Change the boot options to **User Configured LUNs** in the **Boot Over SAN** dialog box. Refer to “Configuring boot over SAN” on page 74 for details.

Remote LUNs are not visible to the host

Remote LUNs configured for boot over SAN feature are not available from the host.

Possible Cause: The driver update disk (DUD) used to install the driver and necessary file structure on remote LUNs for boot over SAN operation is not correct for the host operating system being installed on the LUN.

Action: Download and install the correct the driver update disk for the OS that is being installed. Download the DUD from the Brocade HBA website (www.brocade.com/hba).

Possible Cause: Missing or improper storage array LUN mask setting.

Action: Check LUN mapping and masking using the storage array configuration applications.

Boot from SAN may stop on some Hewlett Packard hosts

The boot process may stop on some Hewlett Packard systems, such as the HP DL180, and the following message displays:

```
02a2: BMC System Error Log (SEL) Full`
/Press F1 to Continue, Press F2 to Setup/
```

Possible Cause: The System Event Log may become full of erroneous IPMI (intelligent platform management interface) events reported by the system BIOS.

Action: Perform the following steps:

1. Boot the server and press **F10** when prompted to run BIOS Setup.
2. Select the **Advanced** menu.
3. Scroll down to **IPMI** and press **ENTER**.
4. Scroll down to the **System Event Log** selection and press **ENTER**.
5. At the **Clear System Event Log** selection, press **ENTER** to toggle between **Enable** and **Disable**.
6. Select **Enable**.

7. Press **F10** to save the changes and exit the BIOS Setup.

NOTE
Action: Refer to Hewlett Packard (HP) Customer Advisory Document c01199684 on the HP technical support website for detailed information.

Adapter <port id>: BIOS not installed displays during boot process

An "Adapter <port id>: BIOS not installed" message displays when booting from an adapter.

Possible Cause: Either the boot image is not present in the adapter option ROM or initialization of the adapter failed for some reason.

Action: Bring up the host system either using the Brocade live CD or boot from local disk. Download the latest boot image (bfa_boot_fw) from the HBA website at www.brocade.com/hba. Enter the BCU **boot upload [adapter_id] <imange file> -a** command to flash the option ROM on all installed adapters with the same boot image.

Ethernet network interface problems (CNA only)

Use the following information to isolate problems that are more specific to CNA function.

NOTE
Switch command examples used in this section are for the Brocade 8000 Switch.

Ethernet link ports or LOM not coming up on reboot in Linux

The host system's LAN on motherboard (LOM) is not coming up or CNA ports are not visible after rebooting Linux host.

1. **Possible Cause:** A ifcfg-ethX script is not configured to bring up each LOM and CNA during the system boot process.

   Action: Make sure that a script is configured for each CNA and LOM once drivers are installed. Scripts are located in the following directories:

   - SLES - /etc/sysconfig/network
   - RHEL - /etc/sysconfig/network-scripts

2. **Possible Cause:** NetworkManager is enabled. There are known issues with NetworkManager managing multiple NICs in some Linux distributions.

   Action: Disable NetworkManager.

   To check if NetworkManager is running enter either of the following commands:

   - chkconfig --list | grep NetworkManager
   - nm-tool

   To disable NetworkManager for RHEL 5 systems, enter the following commands:

   ```
   chkconfig NetworkManager off
   chkconfig NetworkManagerDispatcher off
   ```

To disable NetworkManager for SLES systems, perform the following steps.

a. Open YaST.

b. Select the **Network Devices Network Card**.

c. On the first screen set the **Network Setup Method** option to **Traditional Method with ifup**.

Loss of adapter hardware address in Linux

The ifconfig command displays HW Addr as 00:00:00:00:00:00.

Possible Cause: The CNA failed to initialize for some reason.

Action: Disable the Ethernet I/O controller by entering the BCU **ethioc –disable** command, then enable the I/O controller by entering the BCU **ethioc –enable** command.

Loss of adapter IP address in Linux

The IP address for the adapter disappears when the adapter goes down or system reboots.

Symptom: The IP address set in Linux with the ifconfig command disappears when the adapter goes down or host system reboots.

1. **Possible Cause:** The IP address was set with the ifconfig command and the adapter is enabled in DHCP (Dynamic Hardware Configuration Protocol) mode.

   Action: Configure IP address using system GUI-based networking tools.

2. **Possible Cause:** The IP address is not configured in the ifcfg-ethX script.

   Action: Manually configure IP address in ifcfg-ethX script.

Ethernet loopback test problems

Errors occur during BCU Ethernet loopback tests.

1. **Symptom:** Loopback test returns “Check link/cable or SFP” error when executed with -t cable option.

   Possible Cause: Loopback cable not inserted in tested port.

   Action: Verify that loopback cable is securely inserted in the port that you are testing.

2. **Symptom:** Loopback test returns a “port not disabled” error.

   Possible Cause: Port is enabled.

   Action: Disable the port using the BCU **port –disable** command before running loopback test.

3. **Symptom:** Loopback test returns a “port not disabled” error.displays even after disabling the port.

   Possible Cause: Network load balancing service is enabled. This will cause the adapter to disable and enable, and the previously configured state (port disable) is lost.

   Action: Disable network load balancing and retest.

4. **Symptom:** The loopback test returns “Device busy - Retry operation” or “diag busy.”

   Possible Cause: Other users or sessions are running another instance of loopback tests.

Action: Check for other instances of this diagnostic using **ps -ef** for Linux and VMware, and Task Manager for Windows systems.

Action: Wait a few minutes before retrying the command (Check if the other instance is done using ps -ef command or Task Manager).

5. **Symptom:** The loopback test returns “Missing frame check and replace SFP/cable.”

   Possible Cause: The loopback cable was pulled during the test.

   NOTE
   This should only occur when the test is run in ext mode and not in serdes mode.

   Action: Restart the test with the cable connected.

Network stack runs out of heap

The network stack on VMware systems is running out of heap space.

Possible Cause: Enabling NetQueue and using jumbo frames has caused the network stack to run out of heap with default values set for netPktHeapMaxSize and netPktHeapMinSize. Leaving default values can result in unpredictable behavior.

Action: Perform the following steps.

1. Log in to the VI Client.
2. Click the **Configuration** tab for the ESX Server host.
3. Click **Advanced Settings**.
4. Click **VMkernel**.
5. Find the corresponding value field for VMkernel.Boot.netPktHeapMaxSize, and enter 128 .
6. Find the corresponding value field for VMkernel.Boot.netPktHeapMinSize, and enter 32 .
7. Click **OK** to save the changes.
8. Reboot the system.

NIC numbering unexpected on VMware systems

After installing CNA drivers on VMware systems, NIC numbering is not what is normally expected. For example, instead of vmnic32 or vmnic33, number is vmnic2 and vmnic3.

Possible Cause: CNA hardware was installed before drivers.

Action: When installing a CNAs on a VMware systems, it is advisable to install the driver before the CNA cards so that the NICs will be properly enumerate in the system. To resolve the problem, you must perform the following steps:

1. Uninstall the drivers.
2. Remove the CNA card.
3. Reboot your system without the CNA.
4. Install the drivers.
5. Install the card.

6. Reboot the host system.

Ping to remote server is failing

Pings generated between servers are failing.

1. **Possible Cause:** Ethernet interface on either server is in the following states:

   - Administratively down. Running the Linux or VMware **ifconfig** command shows that the UP flag is not set.
   - Administratively up, but link is down. Running the Linux or VMware **ifconfig** command shows that the RUNNING flag is not set.

   Action: To determine link state, run the **ifconfig** command for Linux or VMware systems. For Windows systems, run **ipconfig /all** or use **Settings > Network Connections**.

   Action: For the interface to send and receive packets, both the UP and RUNNING flag must be set.

   Action: If pinging a server on a different network. make sure that the route to that host network or that the default gateway is correctly configured.

2. **Possible Cause:** Other link problems.

   Action: Refer to "Port link is not active" on page 9.

3. **Possible Cause:** IP address and network mask of CNA port are set incorrectly.

   Action: Verify and set IP address and network mask if necessary:

   - Linux - Run the **ifconfig** command to determine if port has proper IP address and network mask and to verify that the link is up.
   - Windows - Use **Device Manager** and network connection tools.

4. **Possible Cause:** Packets are not being received or stack is dropping packets at remote server due to incorrect IP address set on adapter or incorrect MTU size.

   Action: Verify if packets arrived at the remote server using the following commands:

   - Linux - Run the **tcpdump** command.
   - Windows - Run the Wireshark application.

   Action: Verify MTU size on your system and increase size if necessary. Note that MTU size set on adapter must not be more than MTU size set on attached FCoE switch. To set MTU size on the adapter, refer to the "Adapter Configuration" chapter in the *Brocade Adapters Installation and Reference Manual*.

   Action: Verify and set IP address and network mask if necessary:

   - Linux - Run the **ifconfig** command to determine if port has proper IP address and network mask and to verify that the link is up.
   - Windows - Use **Device Manager** and network connection tools.

VLAN creation and operation problems

VLAN creation fails with BCU command or HCM or pass-through VLAN stops working after creating with Device Manager. These problems result when VLANs are created using HCM or BCU commands and also using Device Manager. Follow these guidelines to avoid problems:

- If you need to create a single VLAN and VLANs have not been created using BCU commands or HCM, you can use Device Manager.
- If you want to configure multiple VLANs, disable the port VLAN created in Device Manager (set to 0 value), then configure VLANs using HCM or BCU. Refer to the *Brocade Adapters Administrator's Guide* for instructions.

1. **Symptom:** When using BCU commands or HCM, to create VLANs, the initial VLAN fails with an error message.

   Possible Cause: Port VLAN was created through Device Manager.

   Action: Set port VLANID to 0 in Device Manager and create VLANs using BCU commands or HCM.

2. **Symptom:** Pass-through VLAN stops working.

   Possible Cause: Port VLAN was configured through Device Manager.

   Action: Set port VLANID to 0 in Device Manager.

3. **Symptom:** Right-clicking on a VLAN device in Device Manager, then selecting **Update** does not work.

   Possible Cause: The upgrade option for Brocade 10 Gig Ethernet service is not available.

   Action: Uninstall and install the service.

4. **Symptom:** No VLAN operation works except "bcu vlan –list."

   Possible Cause: Port VLAN is configured in Device Manager.

   Action: Set port VLANID to 0 in Device Manager.

Enabling and disabling port VLAN in Device Manager

Access the port VLAN configuration in Device Manager using the following steps

1. Open Device Manager.
2. Expand **Network Adapters**

   An instance of the adapter model should display for each installed adapter port.

3. Right-click an adapter instance and select **Properties**.
4. Select the **Advanced** tab.
5. Select **VlanID.**
6. Set VLANID to 0 to disable or enable by setting an ID number.

Poor network performance

Poor network performance apparent for Windows and Linux systems.

1. **Symptom:** Checksum offloads are disabled.

   Action: For Windows, verify if checksum offload parameters are enabled using the **Advanced** tab on the **Network Adapters** > **Properties** dialog box in Device Manager.

   Action: For Linux, run the **ethtool -K <interface ID>** command. If offload parameters are on, information similar to the following displays in the output.

   ```
   rx-checksumming: on
   tx-checksumming: on
   tcp segmentation offload: on
   ```

   Action: Checksum offloads should be enabled by default. If not, refer to the "Adapter Configuration" appendix in the *Brocade Adapters Installation and Configuration Manual*.

2. **Symptom:** Dynamic interrupt moderation is disabled.

   Action: For Windows, verify if interrupt moderation is enabled using the **Advanced** tab on the **Network Adapters** > **Properties** dialog box in Device Manager.

   Action: For Linux, run the **ethtool -C <interface ID>** command. If interrupt moderation is enabled, information similar to the following displays in the output.

   ```
   Coalesce parameters for eth2:
   Adaptive RX: on  TX: off
   ```

   Action: Interrupt moderation should be enabled by default. If not, refer to the "Adapter Configuration" appendix in the *Brocade Adapters Installation and Configuration Manual*.

3. **Symptom:** Not all eight lanes of PCIe bus are functioning.

   Action: For Linux, run the following command:

   ```
   lspci –vv –d 1657:0014
   ```

   If eight lanes are detected, information similar to the following should appear in the command output:

   ```
   Link: Supported Speed unknown, Width x8, ASPM L0s L1, Port 0
   Link: Speed 2.5Gb/s, Width x8
   ```

   Action: If eight lanes are not detected, try rebooting the system. If this does not fix the problem, contact customer support for your adapter.

FCoE and Fibre Channel problems

This section provides resolution of problems related to Fiber Channel and FCoE.

Loss of sync and loss of signal errors in port statistics

If the port is having loss of synchronization and signal errors, refer to the following descriptions of possible causes and recommended actions to help resolve the problem. Learn more about displaying port statistics in "Port statistics" on page 59.

Possible Cause: Possible physical link problem.

Action: Check authentication settings on the switch and adapter. For the switch, execute the authutil **–show Fabric** Fabric OS command. For the adapter, execute the BCU **auth –show** command (refer to "Authentication settings" on page 73).

Action: Use the **BCU auth –show <port>** command on the adapter and Fabric OS **authutil –show** command on the switch.

Action: Check the shared secret configuration on the attached switch and on the adapter. For the switch, execute the **secAuthSecret** Fabric OS command. For the adapter, execute the **auth –-secret** BCU command. Refer to "Authentication settings" on page 73 for details on using the auth-secret command.

Fabric authentication failures

If failures in the authentication process between the adapter in host system and the connected switch occur, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: Authenticating configuration is incorrect.

Action: Check authentication settings on the switch and adapter. For the switch, execute the **authutil –show** Fabric OS command. For the adapter, execute the BCU **auth –show** command (refer to "Authentication settings" on page 73).

Action: Check the shared secret configuration on the attached switch and adapter. For the switch, execute the **secAuthSecret Fabric** OS command. For the adapter, execute the **auth –-secret** BCU command. Refer to "Authentication settings" on page 73 for details on using the auth-secret command.

I/Os are not failing over immediately on path failure in MPIO setup

When multipath I/O (MPIO) is enabled and input/output operations are not failing over immediately when a path failure occurs, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: Improper driver mpiomode setting.

Action: Execute the **port –query <port_id>** BCU command and ensure fcpim MPIO mode is enabled (which implies zero Path TOV values) or that fcpim MPIO mode is disabled with the expected "Path TOV" settings (default is 30 seconds).

Disk I/O requests causes low throughput and high latency on Linux

If a high number of I/O requests is causing low throughput and high latency on Linux systems, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: The maximum input/output operations per second are too low on Linux hosts.

Action: Refer to "Linux tuning" on page 77 for suggestions to optimize adapter performance in Linux systems.

Disk I/O requests causes low throughput and high latency on VMware

If a high number of I/O requests is causing low throughput and high latency on VMware systems, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: The maximum input/output operations per second are too low on VMware hosts.

Action: Refer to "VMware tuning" on page 79 for suggestions to optimize adapter performance in VMware systems.

Adapter is not showing in the fabric

If the adapter does not appear as a Fibre Channel device in the fabric, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Cause: There is a problem in the fabric or a protocol issue between the adapter and a fabric.

Action: Check the fabric statistics. Refer to "Fabric statistics" on page 56 for methods to display fabric statistics for the adapter.

- If counts for FLOGI sent and FLOLGI accept fabric statistics do not match, suspect fabric problem or protocol issue between adapter and fabric.
- If fabric offline counts increase and fabric maintenance is not occurring, this may indicate a serious fabric problem. Refer to your switch troubleshooting guide to isolate and resolve the problem.

Virtual devices not listed in name server

If virtual devices are not listed in the fabric's name server, refer to the following descriptions of possible causes and recommended actions to help resolve the problem.

Possible Causes:

- Problem in the fabric or a protocol issue between the adapter and fabric.
- NPIV is not supported or is disabled on the switch.

Action: Check virtual port statistics, such as FDISK sent, FDISK accept, and No NPIV support statistics. Refer to "Virtual port statistics (HBA only)" on page 61 for methods to display virtual port statistics.

Adapter not registering with the name server or cannot access storage

If the adapter is not registering with the name server or cannot access storage, refer to the following descriptions of possible causes and recommended actions to help solve the problem.

1. **Possible Cause:** Adapter cannot log in to the name server.

   Action: Display logical port statistics (refer to "Logical port statistics" on page 58 for details on displaying these statistics). Check for increasing name server port login (NS PLOGI) error rejects and unknown name server port login response (NS login unknown rsp). These errors mean that the adapter most likely cannot log in to the name server.

2. **Possible Cause:** Adapter has a problem registering with the name server.

   Action: Display logical port statistics (refer to "Logical port statistics" on page 58 for details on displaying these statistics). Check for increasing errors of the following types. These indicate that the adapter has a problem registering with the name server:

   - Name server register symbolic port name identifier (NS RSPN_ID) errors.
   - Name server register symbolic port name identifier response (NS RFT_ID rsp) errors.
   - Name server register symbolic port name identifier response rejects (NS RFT_ID rejects).

3. **Possible Cause:** Adapter has a problem querying the name server for available storage.

   Action: Display logical port statistics (refer to "Logical port statistics" on page 58 for details on displaying these statistics). Check for increasing name server get all port ID response (NS GID_FT rsp), rejects (NS_GID FT rejects), or unknown responses (NS_GID FT unknown rsp). This indicates that the adapter has a problem querying the name server for available storage.

FCoE link is down

The FCoE link is down between the CNA and switch.

1. **Possible Cause:** The FCoE link is not administratively enabled.

   Action: Determine if the link is enabled by entering the BCU **port –list** command. If the port is administratively disabled, the **"port state"** field will show **Disabled**.

   Action: Enable the port by entering the BCU **port –enable <port_id>** command.

2. **Possible Cause:** The CEE is not enabled on the CNA

   Action: Verify that the CEE status using the BCU **port –list** command is displayed as "CEE Linkup". If "Linkdown" or "Linkup" displays, refer to "CEE is not enabled" on page 32.

3. **Possible Cause:** The VLAN to which the FCoE switch front-end port belongs is not FCF-capable.

   Action: Verify if VLAN on front-end port is FCF-capable using the appropriate Fabric OS command on the attached switch. Refer to the *Fabric-OS Command Reference Manual* for more information.

   Action: Set the VLAN as FCF-capable using the appropriate Fabric OS commands on the attached FCoE switch. Refer to the *Fabric-OS Command Reference Manual* for more information.

4. **Possible Cause:** The FC-MAP on the FCoE switch is not set for a VLAN with FCF capability.

   Action: Verify if the FC-MAP on the switch is set for a VLAN with FCF capability using appropriate Fabric OS command on the attached switch. Refer to the *Fabric OS Command Reference Manual* for more information.

   Action: Set the FC-MAP for a VLAN with FCF capability using the appropriate Fabric OS command on the attached switch. Refer to the *Fabric OS Command Reference Manual* for more information.

5. **Possible Cause:** The FCoE Login group is not created on the FCoE switch, not allowing all VF-Ports to be part of the login group.

   Action: Verify if FCoE Login group is created on switch using the appropriate Fabric OS command. Refer to the *Fabric OS Command Reference Manual* for information.

   Action: Create an FCoE login group on the switch using the appropriate Fabric OS command.

6. **Possible Cause:** PFC (priority flow control), CEE Map, and FCoE Map is not configured correctly on the FCoE switch.

   Action: Refer to "CEE is not enabled" on page 32.

I/O problem on connected FCoE device

There is an I/O problem on a connected FCoE device.

1. **Possible Cause:** Link between CNA and switch is down.

   Action: Refer to "FCoE link is down" on page 30.

   Action: Refer to "CEE is not enabled" on page 32.

2. **Possible Cause:** PFC (priority flow control), CEE Map, and FCoE Map is not configured correctly on the FCoE switch.

   Action: Verify configuration using the appropriate Fabric OS command on the attached switch. Refer to the *Fabric OS Command Reference Manual* for information.

   Action: Configure PFC using the appropriate Fabric OS command on the attached switch while in switch configuration mode.

3. **Possible Cause:** Zoning is configured incorrectly on FCoE switch.

   Action: Verify zoning configuration on the attached switch using the appropriate Fabric OS command. Refer to the *Fabric OS Command Reference Manual* for more information.

CEE network problems (CNA only)

This section provides information to resolve problems of CNA operation on the converged enhanced Ethernet (CEE) network.

CEE is not enabled

The CEE state does not show “CEE Linkup” when you run the **bcu port –query** command.

1. **Possible Cause:** The link between the CNA port and switch is down.

   Action: Run the **cee –query** command for the port to gain a better understanding of LLDP attributes, CEE maps, and priority tables configured for the port. Also check the error reason code for the CEE link failure. The error reason code will tell you why the CEE is not enabled or active. If the error reason is “Physical Link down,” refer to “Port link is not active” on page 9 and “Verifying Fibre Channel and CEE links” on page 32

2. **Possible Cause:** Adapter did not receive CEE configuration or received invalid CEE configuration from the FCoE switch.

   Action: Run the BCU **cee –query** command for the port to gain a better understanding of LLDP attributes and CEE configuration (such as CEE maps and priority tables) configured for the port. Also check for the error reason code for the CEE link failure. The reason code will tell you why the CEE is not enabled or active. Change or fix the CEE configuration at the switch appropriately based on the displayed error reason code.

   Action: Check FCoE switch configuration using the appropriate Fabric OS command on the attached switch. Refer to the *Fabric OS Command Reference Manual* for information. Change configuration as necessary using appropriate Fabric OS command on the attached switch. Refer to the *Fabric OS Command Reference Manual* for information.

3. **Possible Cause:** The front-end Ethernet port on the FCoE switch is not configured as “switchport” or is not set to converged mode.

   Action: Use the appropriate Fabric OS command on the attached switch to display information about the VLAN interface. Refer to the *Fabric OS Command Reference Manual* for information.

   Action: Configure the FCoE port as a “switchport” using the appropriate Fabric OS command on the attached switch. Refer to the *Fabric OS Command Reference Manual* for information.

   Action: Configure the FCoE port to converged mode using the appropriate Fabric OS command on the attached switch.

Verifying Fibre Channel and CEE links

Check for link problems by observing LED operation for adapter ports. LED operation other than expected or LEDs may indicate link problems. For example, all LEDs flashing amber for a port indicates that an invalid non-Brocade SFP may be installed. For details on adapter LED operation, refer to the “LED Operation” section for your adapter (CNA or HBA) in the *Brocade Adapters Installation and Reference Manual*. If LEDs do not illuminate to indicate an active link, use appropriate Fabric OS and adapter diagnostic commands and HCM options in Table 3 on page 33. For additional diagnostics commands, refer to Chapter 3, “Tools for Collecting Data” for HCM and BCU commands and the *Fabric OS Administrators Guide* for Fabric OS commands.

NOTE
Also verify LED operation on a switch port that is connected to an adapter port. Refer to the switch Hardware Reference Manual to analyze LED meaning.

Common link problems can be caused by the following:

- Damaged cables. (Note that damaged cables can also cause errors and invalid data on links.)
- Cables that are not rated or compatible with adapter port speeds. Refer to cable specifications in the *Brocade Adapters Installation and Reference Manual*.
- Faulty switch or adapter SFPs. Verify if an SFP is the problem by connecting a different link to the adapter port or, if convenient, replace the cable with a cable of known quality. If the errors or invalid data on the link still indicate a cable problem, the SFP may be faulty. Try replacing the SFP.
- SFP issues on the adapter or switch. For example, the SFP may not be compatible with the adapter, but is compatible with the switch, or vice versa. SCSI retries and timeouts determine communication between the adapter and storage. Dropped packets cause timeouts, and packets can drop because of SFP issues. Run the BCU **port -stats** command to display port statistics, and look for errors and dropped frames.

Table 3 lists HCM options and BCU commands, as well as Fabric OS commands that you can use to determine link status.

TABLE 3 Tools to determine link status

Application	Tool	References
HCM	• Port Statistics • Loopback and PCI loopback test • Fibre Channel ping, echo, and trace route tests • Link Beaconing (HBAs only) • Port Properties • SFP information	*Chapter 3, "Tools for Collecting Data"*
BCU	• **fcdiag** and **diag** commands. • Port commands, such as **port –stats**. **port –list**, and **port –query.**	*Chapter 3, "Tools for Collecting Data"*
Switch Fabric OS	• switchShow • portShow • portStatsShow • portErrShow • fcpProbeShow • fPortTest	• *Chapter 3, "Tools for Collecting Data"* • *Fabric OS Administrator's Guide* • *Fabric OS Troubleshooting* and *Diagnostics Guide*

Adapter driver installation verification

Problems with adapter operation may be due to improper hardware or software installation, incompatibility between the adapter and your host system, unsupported SFPs installed on the adapter, improper cable connected to the fabric, or the adapter not operating within specifications. Determine if problems may exist because of these factors by reviewing your installation with information in the *Brocade Adapters Installation and Reference Manual* listed in Table 4.

TABLE 4 *Installation and Reference Manual* references

Information	Chapter
Hardware and software compatibility information.	Product Overview
Software installation packages supported by host operating system and platforms.	Product Overview
Hardware and software installation instructions.	Installation
Product specifications.	Specifications

Adapter driver packages from Brocade contain the current driver, firmware, and HCM agent for specific operating systems. Make sure that the correct package is installed for your operating system. Refer to the installation chapter in the *Brocade Adapters Installation and Reference Manual*.

An out-of-date driver may cause the following problems:

- Storage devices and targets not being discovered by the device manager or appearing incorrectly in the host's device manager.
- Improper or erratic behavior of HCM (installed driver package may not support HCM version).
- Host operating system not recognizing adapter installation.
- Operating system errors (blue screen).

NOTE
If a driver is not installed, try re-installing the driver or re-installing the adapter hardware and then the driver.

You can use HCM and tools available through your host's operating system to obtain information such as driver name, driver version, and adapter port WWNs.

Confirming driver package installation with HCM

Use the following steps to display the adapter PWWN, driver name and version, firmware name and version, and the BIOS version currently in operation.

1. Launch HCM.
2. Select the adapter in the device tree.
3. Select the **Properties** tab in the right pane to display the **Properties** dialog box.

   The dialog box displays adapter properties.

Confirming driver package installation in Windows systems

Use the Device Manager to determine driver installation. Verify if the driver is installed and Windows is recognizing the adapter using the following steps.

1. Open the **Device Manager**.
   - For HBAs and CNAs, when you expand the list of **SCSI and RAID controllers**, an instance of **Brocade 10G FCoE HBA** should display for adapter port installed. For example, if two two-port adapters (total of four ports) are installed, four instances of the adapter model display.
   - For CNAs only, when you expand **Network adapters**, an instance of **Brocade 10G Ethernet Adapter** should also display for each port of the adapter installed. For example, if two two-port adapters (total of four ports) are installed, four instances of the adapter model display.

   If instances of your adapter model do not display, but generic instances flagged with yellow question marks *do* display under **Other Devices**, the driver is not installed. For example, **Fibre Channel Controller** may display as a generic instance for an HBA.
2. Right-click the Brocade adapter model where you are installing the driver.
3. Select **Properties** to display the **Properties** dialog box.
4. Click the **Driver** tab to display the driver date and version. Click **Driver Details** for more information.

NOTE
If driver is not installed, try re-installing the driver or re-installing the adapter hardware and then the driver.

Confirming driver package installation in Linux systems

Verify if the adapter driver installed successfully using the following commands:

- **# rpm -qa|grep -i bfa**

  This command prints the names of the Brocade adapter storage driver package (bfa) if installed.
- **# rpm -qa|grep -i bna**

  This command prints the names of the Brocade adapter network driver package (bfa) if installed.
- **# lspci**

  This utility displays information about all PCI buses in the system and all devices connected to them. **Fibre Channel: Brocade Communications Systems, Inc.** displays for an HBA. **Fibre Channel: Brocade Communications Systems, Inc.** and **Ethernet Controller** display for a CNA if driver packages have correctly loaded.
- **# lsmod**

  This command displays information about all loaded modules. If **bfa** appears in the list, the storage driver is loaded to the system. If **bna** appears in the list, the network driver is loaded to the system.

- **# dmesg**

  This command prints kernel boot messages. Entries for **bfa** (storage driver) and **bna** (network driver) should display to indicate driver activity if the hardware and driver are installed successfully.

- These commands display the location of the driver modules if loaded to the system:
  - The following command displays the storage driver module location. The module will have a **bfa** prefix.

    ```
    # modprobe -l bfa
    ```

  - The following command displays the network driver module location. The module will have a **bfa** prefix.

    ```
    # modprobe -l bna
    ```

Confirming driver package installation in Solaris systems

Verify if the adapter driver installed successfully using the following commands.

- **pkgchk -nv bfa**

  This checks for and lists the installed adapter storage driver package files.

- **pkginfo -l bfa**

  This displays details about installed Brocade storage (bfa) adapter drivers. Look for information as in the following examples. Note that the VERSION may be different, depending on the driver version you installed. The ARCH and DESC information may also be different, depending on your host system platform. If the adapter driver package is installed, bfa_pkg should display with a “completely installed” status.

  Storage driver (bfa)

```
PKGINST: bfa
      NAME:  Brocade Fibre Channel Adapter Driver
  CATEGORY:  system
      ARCH:  sparc&i386
   VERSION:  alpha_bld31_20080502_1205
   BASEDIR:  /
    VENDOR:  Brocade
      DESC:  32 bit & 64 bit Device driver for Brocade Fibre Channel
adapters
    PSTAMP:  20080115150824
  INSTDATE:  May 02 2008 18:22
   HOTLINE:  Please contact your local service provider
    STATUS:  completely installed
```

Confirming driver package installation in VMware systems

Verify if the adapter driver installed successfully using the following commands:

- **vmkload_mod -l**

  This lists installed driver names, R/O and R/W addresses, and whether the ID is loaded. For storage drivers, verify that an entry for **bfa** exists and that the ID loaded. For network drivers, verify that an entry for bna exists and that the ID loaded.

- **cat /proc/vmware/version**

  This displays the latest versions of installed drivers. For storage drivers look for a **bfa** entry and related build number. For network drivers, look for a **bna** entry and related build number.

- **rpm -qa|grep -i bfa**

  This command prints the names of the Brocade adapter storage driver package (bfa) if installed.

- **rpm -qa|grep -i bna**

  This command prints the names of the Brocade adapter network driver package (bna) if installed.

- **lspci**

  This utility displays information about all PCI buses in the system and all devices connected to them.**Brocade Communications Fibre Channel** displays for an HBA. **Brocade Communications Fibre Channel** and **Ethernet Controller** display for a CNA if driver packages have correctly loaded.

Additional references for isolating problems

Refer to the following publications and to chapters in this manual for gathering information to further isolate and resolve adapter problems.

- Chapter 3, “Tools for Collecting Data” in this manual

  Contains procedures to perform adapter diagnostics, display adapter statistics and event logs, and collect data for troubleshooting using BCU commands, HCM options, Fabric OS commands, and your host system commands.

- *Fabric OS Administrator’s Guide*

  Provides detailed information on features available on Brocade storage area network (SAN) products, and how to configure and administer these products

- *Fabric OS Command Reference Manual.*

  Provides detailed descriptions of command line interface commands to help system administrators and technicians operate, maintain, and troubleshoot Brocade SAN products.

- *Fabric OS Troubleshooting and Diagnostic Guide.*

  Provides help with isolating problems in other Brocade SAN components.

- Your host’s operating system documentation and help system.

  Provides details on commands for gathering information and isolating problems.

Chapter

3

Tools for Collecting Data

In this chapter

For detailed information

This chapter provides basic instruction on tools useful for gathering information to isolate adapter problems. For more detailed information on using these tools, refer to the following publications:

- *Brocade Adapters Administrator's Guide.*

  The following chapters in this guide cover adapter HCM and BCU monitoring and diagnostics tools:

  - Monitoring
  - Diagnostics
  - Brocade Command Utility (BCU)
- *Fabric OS Troubleshooting and Diagnostics Guide*

  This guide provides detailed information on collecting troubleshooting information and isolating general SAN problems between the switch, host systems, and storage systems.
- *Fabric OS Command Reference Manual*

  Fabric OS diagnostic and monitoring commands.
- Your host system's operating system user and administrator's guides.

  Host system diagnostics, logs, and system monitoring tools.

Data to provide support

When problems occur requiring support assistance, provide a detailed description of the problem, as well as output collected from the following HCM and BCU tools:

- Support Save
- Diagnostics
- Port logs
- Port statistics and properties
- Adapter properties
- Host operating system error logs

Data collection using host system commands

The following table describes commands common to each supported operating system that you can use to gather information for troubleshooting problems. For details on these commands, refer to your system's online help and documentation.

NOTE
Output from all of these commands is captured using the Support Save feature.

TABLE 5 Host system data collection commands

Task	Linux	Windows	VMware	Solaris
Listing PCI devices	lspci -vv	In Windows registry location HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Enum\PCI devcon find pci*	lspci -vv, esxcfg-info -w	prtdiag -v, prtconf -pv
Listing installed HW details	lsdev	msinfo32.exe Click the plus sign(+) next to Components to view hardware details.	esxcfg-info -a	prtdiag -v, prtconf -pv
Displaying process information	ps -efl, top	Windows Task Manager, tasklist.exe	ps -efl, top	ps -efl, top
Displaying memory usage	top, vmstat -m	Windows Task Manager, tasklist.exe	top, vmstat -m	vmstat -s
Monitoring performance	iostat, vmstat, sar	Windows Task Manager, perfmon.exe	vmstat, VM Performance: esxtop [first type 'v', 'e' then enter vm# in the list down], Disk Performance: esxtop [type 'v' then 'd'].	iostat -nx 1 5, vmstat, mpstat, sar
Listing driver modules	lsmod	driverquery	vmkload_mod -l	modinfo
Checking for Brocade Fibre Channel adapter (BFA) driver module	lsmod | grep bfa	driverquery /v | findstr bfad	vmkload_mod -l | grep bfa	modinfo | grep bfa

TABLE 5 Host system data collection commands

Task	Linux	Windows	VMware	Solaris
Checking for Brocade network (BNA) driver module	lsmod | grep bna	driverquery /v | findstr bnad	vmkload_mod -l | grep bfa	NA
Displaying driver information	• Use lsmod command for general driver information. • Use ethtool options to query network driver information and settings.	On Device Manager Right-click storage controller or network adapter instances, select **Properties**, then select **Driver** tab.	• For general driver information use vmkload_mod -i. • For network driver information, use esxcfg-nics.	Use modinfo options for bna or bfa driver.
Locating system log messages **NOTE:** For more information, refer to "Host system logs" on page 48.	dmesg, /var/log/message*	System Category in Windows Event Viewer (eventvwr.exe)	/var/log/vmkernel* /var/log/vmkwarning*/proc /vmware/log /var/log/message*	dmesg, /var/adm/message*
Showing operating system distribution info	(SuSE) cat /etc/SuSE-release,(RedHat) cat /etc/redhat-release	systeminfo.exe	cat /etc/vmware-release	uname -a, cat /etc/release
Locating BFA configuration file	/etc/bfa.conf	Windows Registry (HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services\bfad\Parameters\Device), adapter Flash	/etc/bfa.conf	/kernel/drv/bfa.conf
Locating BFA device file	/dev/bfa*	Windows Registry (HKEY_LOCAL_MACHINE \HARDWARE\DEVICEMAP\Scsi\Scsi Port x)	/opt/brocade/adapter/bfa/ bfa.conf	• (Release 1.0) - /devices/pci*/pci*/ fibre-channel@0:devctl, • (Release 1.1 and later) - /devices/pci*/pci*/ bfa@0:devctl
Locating BNA device file	/dev/bna*	Windows Registry (HKEY_LOCAL_MACHINE \HARDWARE\DEVICEMAP\Scsi\Scsi Port x)	/dev/bna*	• (Release 1.0) - /devices/pci*/pci*/ fibre-channel@0:devctl, • (Release 1.1 and later) - /devices/pci*/pci*/ bfa@0:devctl
Verifying network interface parameters, such as link status, IP address, and subnet mask.	ifconfig	ipconfig Settings > Network Connections	ifconfig	N/A

TABLE 5 Host system data collection commands

Task	Linux	Windows	VMware	Solaris
Ethernet statistics	ethtool -S <interface_name>	netstat	ethtool -S <interface_name>	N/A
Ethernet link status	ethtool interface_name>	netstat	esxcfg-nics -l	N/A

Data collection using BCU commands and HCM

You can collect a variety of information on installed Brocade adapters, such as firmware version installed, operational status, port speed, WWN, PCI data, configuration data, flash status, and other details for troubleshooting using BCU commands, HCM menu options, and host operating system commands.

Support Save

The Support Save feature is an important tool for collecting debug information from the driver, internal libraries, and firmware. You can save this information to the local file system and send to support personnel for further investigation. Use one of the following options to launch this feature:

- In HCM, launch **Support Save** through the **Tools** menu.
- Through BCU, enter the **bfa_supportsave** command.
- Through your internet browser (Internet Explorer 6 or later or Firefox 2.0 or later), you can collect bfa_supportsave output if you do not have root access, do not have access to file transfer methods such as FTP and SCP, or do not have access to the Host Configuration Manager (HCM).
- A bfa_supportsave collection can also occur automatically for a port crash event.

The Support Save feature saves the following information:

- Adapter model and serial number
- Adapter firmware version
- Host model and hardware revision
- All support information
- Adapter configuration data
- All operating system and adapter information needed to diagnose field issues
- Information about all adapters in the system
- Firmware and driver traces
- Syslog message logs
- Windows System Event log .evt file
- HCM GUI-related engineering logs
- Events
- Adapter configuration data

- Environment information
- Data.xml file
- Vital CPU, memory, network resources
- HCM Agent (logs, configuration)
- Driver logs
- Install logs
- Core files
- Details on the CNA's Ethernet interface, including IP address and mask
- Status and states of all adapter ports, including the Ethernet, FCoE, and CEE ports on CNAs
- CEE status and statistics for CNAs
- Network driver information, Ethernet statistics, offload parameters, and flow control coalesce parameters for CNAs
- Ethernet offload, flow control, and coalescing parameters for CNAs

NOTE
Master and Application logs are saved when Support Save is initiated through HCM, but not through BCU.

Initiating Support Save through HCM

Initiate Support Save by selecting **Tool > Support Save**.

Messages display during the Support Save operation that provide the location of the directory where data is saved. If you are initiating Support Save from a remote management station and receive a warning message that support files and Agent logs could not be collected, the HCM Agent is unavailable on the remote host. Select **Tool** > **Backup** to backup data and configuration files manually.

Support data is collected to a file in your system's tmp directory by default.

For more information and additional options for using this feature, refer to the *Brocade Adapters Administrator's Guide*.

Initiating Support Save through BCU commands

Use the bfa_supportsave command to Initiate Support Save through the BCU:

- bfa_supportsave - creates and saves the supportsave at /tmp.
- bfa_supportsave <dir>- creates and saves the supportsave under a directory name that you provide.
- bfa_supportsave <dir> <ss_file_name> - creates and saves the supportsave under a directory and file name that you provide. If the directory already exists, it will be overwritten.

Messages display as the system gathers information. When complete, an output file and directory display. The directory name specifies the date when the file was saved.

For more information and additional options for using this feature, refer to the *Brocade Adapters Administrator's Guide*.

Initiating Support Save through the internet browser

Initiate bfa_supportsave through an internet browser.

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

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

   where localhost is the IP address of the server from which you want to collect the bfa_supportsave information.

2. Log in using the factory default user name (admin) and password (password). Use the current user name and password if they have changed from the default,

   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.

Initiating Support Save through 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 on these logs, refer to "HCM logs" on page 49.

Support Save differences

Following are differences in data collection for the HCM, BCU, and browser applications of bfa_supportsave:

- BCU

  Collects only driver-related logs and configuration files.

- Browser

  Collects driver-related and HCM Agent logs and configuration files.

- HCM

  Collects, HCM, driver-related, and HCM Agent logs and configuration files.

Collecting adapter data collection using HCM

Select an adapter from the HCM device tree and click the **Properties** tab in the right pane to display basic information about the adapter.

- The Host Bus Adapter (HBA) adapter **Properties** panel displays information about the adapter, such as its WWN, disabled or enabled status, temperature, maximum speed supported, installed driver name, driver version, firmware version, and BIOS version. This panel also displays PCI information for the adapter, such as vendor ID, device ID, subsystem ID, current number of lanes, and PCI generation.

- The Converged Network Adapter (CNA) adapter **Properties** panel displays information about the adapter, such as the MAC address, enabled or disabled status, maximum speed supported, hardware path, serial number, temperature, installed driver name, driver version, firmware version, and BIOS version. This panel also displays PCI information for the adapter, such as vendor ID, device ID, subsystem ID, current number of lanes, and PCI generation.

Use the adapter **Properties** panel in HCM to display information about the adapter.

1. Launch HCM.
2. Select an adapter in the device tree
3. Click the **Properties** tab in the right pane.

Collecting adapter data using BCU commands

Use the BCU adapter command to list and query available adapters seen by the driver.

The **bcu adapter –list** command lists all adapters on the system with a brief summary of information such as model number, serial number, and adapter number. Enter the following command:

```
adapter --list
```

where:

list — Lists all adapters in the system. For each adapter in the system, a brief summary line is displayed.

The **adapter –query** command displays adapter information, such as the current version of the adapter (chip revision) and driver (fw version), maximum port speed, model information, serial number, number of ports, PCI information, pwwn, nwwn, hardware path, and flash information (such as firmware version).

```
adapter –-query <ad_id>
```

where:

ad_id — ID of the adapter for which you want to query.

Data collection using Fabric OS commands

Use the following Fabric OS commands on attached Brocade switches to gather information and help isolate connectivity and other problems between the adapter, switch, and storage ports. For details on using these commands, refer to the *Fabric OS Command Reference Manual*.

- **authUtil**

  Use this command to display and set local switch authentication parameters.

- **cfgShow**

  Use this command to display zone configuration information for the switch. You can use command output to verify target ports (by port WWN) and LUNs that are intended to be accessible from the adapter.

- **fcpProbeShow**

  Use this command to display the Fibre Channel Protocol daemon (FCPd) device probing information for the devices attached to a specified F_Port or FL_Port. This information includes the number of successful logins and SCSI INQUIRY commands sent over this port and a list of the attached devices.

- **nsShow**

  Use this command to display local NS information about all devices connected to a specific switch. This includes information such as the device PID, device type, and the port and node WWN.

- **zoneshow**

  Use this command without parameters to display all zone configuration information (both defined and enabled).

- **portErrShow**

  Use this command to display an error summary for all switch ports.

- **portLogShow**

  Use this command to display the port log for ports on a switch.

- **portLogShowPort**

  Use this command to display the port log for a specified switch port.

- **portPerfShow**

  Use this command to display throughput information for all ports on the switch.

- **portStatsShow**

  Use this command to display hardware statistics counters for a specific switch port.

- **portShow**

  Use this command to display information and status of a specified switch port, including the speed, ID, operating state, type, and WWN.

- **SecAuthSecret**

  Use this command to manage the DH-CHAP shared secret key database used for authentication. This command displays, sets, and removes shared secret key information from the databases

- **sfpShow**

  Use this command to display detailed information about specific SFPs installed in a switch.

- **show vlan brief**

  Displays information about a VLAN interface on the switch.

- **show cee maps**

  Displays information about the configured CEE maps in the switch.

- **switchShow**

  Use this command to display switch and port information. Output may vary depending on the switch model. Use this information to determine the fabric port WWN and PID connected to an adapter port. Also display topology, speed, and state of each port on the switch.

Adapter event messages

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 may contain the following information:

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

NOTE
For details of all driver event messages refer to Appendix A, "Event Message Reference".

Message details are also contained in HTML files, which load your system when you install the adapter driver. You can view these HTML files using any internet browser application. Table 6 provides the default location where these message files install for each supported operating system.

TABLE 6 Message catalog location

Operating System	Catalog Location
Linux	/opt/bfa
VMware	/opt/bfa
Solaris	/opt/bfa
Windows	aen.zip loaded to your driver installation directory. Unzip this file to obtain all message catalog files.

Table 7 lists the message file names and content for the message files.

TABLE 7 Event message files

Event Catalog File	Content
bfa_aen_adapter.html	Adapter events, such as adapter added or removed
bfa_aen_audit.html	Audit events, such as authentication enabled or disabled for base port
bfa_ethport.html	Base port Ethernet events, such as the Ethernet link up and link down.
bfa_aen_ioc.html	IO controller (IOC) events.
bfa_aen_itnim.html	Initiator-target nexus events.
bfa_aen_lport.html	Logical port events.
bfa_aen_port.html	Physical base port events.

TABLE 7 Event message files

Event Catalog File	Content
bfa_aen_rport.html	Remote port (R_Port) events.
hba_error_codes.doc	List of error codes and meanings for the following events: • Adapter - events relating to the adapter • Physical port • L_Port - logical port • R_Port - remote initiator or target port • ITNIM - initiator target nexus • Audits • IOC - I/O controller • Ethernet port

NOTE
Complete content for adapter driver event messages is included in Appendix A, "Event Message Reference".

Logs

Event and error messages that occur during adapter, driver, and HCM operation are important tools for isolating and resolving problems. These messages provide descriptions of an event or problem, severity, time and date of the event, and in some cases, cause and recommended actions. Messages are captured in logs available through HCM, BCU commands, and through host system commands. Monitoring events and errors in these logs allows early fault detection and isolation on a specific adapter.

Host system logs

Brocade adapter event messages are captured in host system log files. All messages related to the Brocade adapter are identified in these logs by BFA (Brocade fabric adapter), BNA (Brocade network adapter), and BFAL (Brocade fabric adapter library].Table 8 describes the logs for each supported operating system where adapter event messages display, and how to view these logs.

TABLE 8 System Event Logs

Operating System	Log Name	Location	Viewing Message Log
Solaris	Syslog	/var/adm/messages	dmesg command
Windows	Event Log	Not applicable	System category in Event Viewer (eventvwr.exe)
Linux	Messages Log	/var/log/message	dmesg command
VmWare[1]	Messages Log	/var/log/message* , /var/log/vmkernel*, /var/log/vmkwarning*,/proc/vmware/log	dmesg command

1. For ESX Server Console operating system. For Guest system, refer to information in Windows or Linux.

Syslog support

You can configure the HCM agent to forward events to a maximum of three system log destinations using the **Syslog** option on the HCM **Configure** menu. These events will display in the operating system logs for systems such as Solaris and Linux. For procedures to configure syslog destinations, refer to the *Brocade Adapters Administrator's Guide*.

HCM logs

You can view data about adapter operation through HCM logs that display in HCM. These logs display on the bottom of the HCM main window. Click the **Master Log** or **Application Log** to toggle between logs.

- The **Master Log** displays informational and error messages during adapter operation. This log contains the severity level, event description, date and time of event, and the function that reported the event (such as a specific adapter port or remote target port).
- The **Application Log** displays informational and error messages related to user action in HCM, discovery, or HCM application issues.

Master Log

The **Master Log** displays event information in seven fields:

- Sr No.

  Sequence number assigned to the event when it occurred, in ascending order.

- Severity

  Event severity level (informational, minor, major, or critical).

  - 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, IO controller heartbeat failure is a critical error.
  - Major messages represent conditions that do not impact overall system functionality significantly.
  - Minor messages highlight a current operating condition that should be checked or it might lead to a failure.
  - Information-level messages report the current non-error status of the system components, for example, the online and offline status of a port.

- WWN

  World Wide Name of adapter where the event occurred.

- Category

  The category or type of event. Categories define the component where events occur:

  - ADAPTER - Events pertaining to the adapter.
  - CEE - Events pertaining to Converged Enhanced Ethernet.
  - ETHPORT - Events pertaining to the Ethernet port.
  - 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.
- Subcategory of main category.
- Event description, Date, and Time

  Brief description of event and date and the time when the event occurred.

NOTE
Complete content of adapter event messages is provided in Appendix A, "Event Message Reference".

You can block events from display in the **Master Log** by severity, category, and WWN of adapter using the **Master Log Filter** dialog box. To display this dialog box, click the **Filter** button in the **Master Log** section of the main HCM screen. Select areas that you want to filter and click **OK**.

Application Log

The **Application Log** 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.

Logging levels adjustment

Adjust the logging level for related adapter logs using the following BCU commands and HCM options. By adjusting the logging level, you can control the number and type of messages that are captured the log.

NOTE
For greater detail on adjusting logging levels, refer to the *Brocade Adapters Administrator's Guide*.

Adjusting the adapter event logging level

Specify the number of event messages logged by the host system log for the storage driver using this BCU command.

Port logging level

Adjust logging level for port logs using BCU commands and HCM.

Adjusting the port logging level through HCM

Adjust port logging level through HCM using the following steps:

1. Select **Configure** > **Basic Port Configuration** from HCM.

   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, and Log Info.

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

Adjusting the port logging level through BCU

Adjust port logging level using this BCU command.

```
bcu log –-level <port_id> [<level>]
```

where:

port_id The ID of the port for which you want to set the log level.

level Critical | Error | Warning | Info

Specifies the severity level. Error is the default setting.

Adjusting the Ethernet logging level through HCM

Adjust logging level for each port for Ethernet driver messages through HCM using the following steps. This is available for CNAs only.

1. Select an Ethernet port from the HCM device tree.
2. Select **Configure** > **Basic Port Configuration**.

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

3. Select a value from the **Eth Logging Level** list.

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

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

Adjusting the Ethernet logging level through BCU

Adjust port logging level for each Ethernet driver using this BCU command.

```
ethlog --level <port_id> [<Critical | Error | Warning | Info>]
```

where:

<port_id> ID of port for which you want to change the logging level.

Adjusting the HCM logging level

Adjust logging levels for the following logs using HCM:

- 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.

To adjust the logging level, use the following steps.

1. Select **Configure** >**HCM Logging Levels**.
2. Select a level on the **Agent Communication Log** and **HCM Debug Log** lists.

   Values are Trace, Debug, Info, Warning, Error, and Fatal.

Statistics

You can access a variety of statistics using BCU commands and HCM. Use these statistics to monitor adapter performance and traffic between the adapter and LUNs and isolate areas that impact performance and device login.

You can display statistics for the following:

- Adapter ports
- CEE
- Ethernet
- Ethernet IO controller
- Fibre Channel over Ethernet (FCoE)
- IO controller (IOC)
- Virtual ports (vport)
- Link Layer Discovery Protocol (LLDP)
- Logical ports (lport)
- Remote ports (rport)
- Fibre Channel Protocol (FCP) initiator mode
- Fabric
- Targets
- Security authentication
- VLAN

This section provides an overview of these statistics and how to access them. For more detail, refer to the *Brocade Adapter's Administrator's Guide*.

CEE statistics (CNA only)

Use BCU commands and HCM to display converged enhanced Ethernet (CEE) statistics, such as the following:

- Logical link layer discovery protocol (LLDP) frames transmitted, received, timed out, discarded, with error, type-length-values (TLVs) discarded, and TLVs unrecognized.
- Data center bridging capability exchange (DCBX) TLVs unrecognized, negotiation fails, remote configurations changed, TLVs received and invalid, status up and down, and received invalid configurations.

Displaying statistics through BCU

Use the following BCU command to display CEE statistics.

```
bcu cee --stats <port_id>
```

where:

<port_ID> The ID of the Ethernet port.

Displaying statistics through HCM

Display the **CEE Statistics** dialog box using the following steps:

1. From the device tree, select a physical port of a CNA.
2. Select **Monitor > Statistics > CEE Statistics**.

CEE query (CNA only)

Query the CEE information on a selected port and display such information as LLDP attributes and the priority group table.

```
bcu cee --query <port_id>
```

where:

<port_ID>The ID of the Ethernet port.

Ethernet statistics (CNA only)

Use BCU commands and HCM to display total numbers of the following statistics:

- Transmitted unicast octets
- Transmitted unicast frames
- Transmitted unicast VLANs
- Transmitted multicast octets
- Transmitted multicast frames
- Transmitted multicast VLANs

- Transmitted broadcast octets
- Transmitted broadcast frames
- Transmitted broadcast VLANs
- Transmitted errors
- Transmitted VLAN filters
- Transmitted filter MAC source addresses
- Received unicast octets
- Received unicast frames
- Received unicast VLANs
- Received multicast octets
- Received multicast frames
- Received multicast VLANs
- Received broadcast octets
- Received broadcast frames
- Received broadcast VLANs
- Received frame drops
- Received packets
- Transmitted packets
- Received bytes
- Transmitted bytes
- Linux NetIf queue stops
- Linux NetIf queue wakups
- Linux TSO IPv4 packets
- Linux TSO IPv6 packets
- Linux errors
- TCP checksum offloads
- UDP checksum offloads
- Checksum help requests
- Checksum help errors
- Hardware statistics updates

Displaying statistics through BCU

Display Ethernet statistics using the following BCU command.

```
ethport --stats <port_id>
```

where:

<port_ID> The ID of the Ethernet port.

Displaying statistics through HCM

To display the **Ethernet Statistics** dialog box, use the following steps:

1. Select an Ethernet port from the device tree.
2. Select **Monitor > Statistics > Eth Statistics** from the main menu.

   OR

   Right-click the Ethernet port and select **Statistics > Eth Statistics** from the list.

The **Ethernet Statistics** dialog at the host level displays.

Ethernet IOC statistics (CNA only)

Use HCM options and BCU to display statistics relevant to the Ethernet IO controller (IOC). A variety of statistics display, such as the following:

- Mailbox interrupts
- Enable and disable events
- Heartbeat failures
- Firmware boots
- Ethernet ICO statistic timeouts
- Checksum help errors
- VLAN transmit and receive transactions

You can also select options to keep running data, set the polling frequency, start polling data, and reset statistics.

Displaying statistics through HCM

To display Ethernet IOC statistics use the following steps:

1. Select an Ethernet port from the device tree.
2. Select **Monitor** > **Statistics** > **Eth IOC Statistics** from the main menu.

   OR

   Right-click the Ethernet port and select **Statistics** > **Eth IOC Statistics** from the list.
3. The **Eth IOC Statistics** dialog at the host level displays.

Displaying statistics through BCU

Use the **bcu ethioc** command to display Ethernet IOC statistics.

```
ethioc --query <port_id>
ethioc --stats <port_id>
ethioc --statsclr <port_id>
```

--query	Displays attributes of the Ethernet IOC.
port_id	Specifies the ID of the Ethernet port for which you will display attributes.
--stats	Displays the Ethernet IOC statistics.

port_id	Specifies the ID of the Ethernet port for which you will display the statistics.
--statsclr	Clears the Ethernet IOC-level statistics.
port_id	Specifies the ID of the Ethernet port for which you will reset the statistics.

FCoE statistics (CNA only)

Use HCM to display statistical information related to a selected Fibre Channel over Ethernet (FCoE) port. Statistics include the number of transmitted and received packets and transmitted and received bytes. You can also select options to continue running data, configure polling frequency, and start polling.

To display FCoE statistics through HCM, use the following steps.

1. Select an FCoE port from the device tree.
2. Select **Monitor** > **Statistics** > **FCoE Statistics** from the device tree.

   OR

   Right-click the FCoE port and select **Statistics** > **FCoE Statistics** from the list.
3. The **FCoE Statistics** dialog box at the host level displays.

Fabric statistics

Use BCU and HCM to display statistics for fabric login (FLOGI) activity and fabric offlines and onlines detected by the port. Use these statistics to help isolate fabric login problems. Following are two examples of how to use these statistics for troubleshooting:

- If the adapter is not showing in the fabric, check the *FLOGI sent* and *FLOGI accept* statistics. If the counts do not match, the switch or fabric may not be ready to respond. This is normal as long as it does not persist. If the problem persists, this could indicate a problem in the fabric or a protocol issue between the adapter and fabric.
- If *fabric offline* counts increase and fabric maintenance is not being done, this may indicate a serious fabric problem. Slow fabric performance or hosts unable to address storage could also be seen.

Displaying fabric statistics through BCU

Use the **fabric –stats** command to display fabric statistics.

```
fabric --stats <port_id>
```

where:

port_id	ID of the adapter port for which you want to display statistics.

Displaying fabric statistics through HCM

Use the **Fabric Statistics** dialog box to monitor a variety of port data.

1. Launch the HCM.
2. Select the base adapter port from the device tree window.
3. Click **Monitor > Statistics > Fabric Statistics**.

IOC statistics

Use BCU and HCM to display port-level statistics for the I/O controller through the BCU and HCM. The I/O controller refers to the firmware entity controlling the port. The following types of IOC statistics are displayed:

- IOC driver
- IOC firmware
- Firmware IO
- Firmware port FPG
- Firmware port PHYSM
- Firmware port LKSM
- Firmware port SNSM

Displaying IOC statistics through BCU
Use the **ioc** command to display IOC statistics.

```
ioc --stats --query <ioc_id>
```

where:

stats	Displays IOC statistics.
query	Displays IOC attributes.
ioc_id	ID of the IOC controller for which you want to display statistics.

Displaying IOC statistics through HCM

Use the **IOC Statistics** dialog box to monitor a variety of port data.

1. Launch the HCM.
2. Select the base adapter port from the device tree window.
3. Click **Monitor > Statistics > IOC Statistics**.

FCP initiator mode statistics

Use HCM and BCU to display Fibre Channel Protocol Initiator Mode (FCP IM) statistics such as the number of online and offline remote ports, process login (PRLI) activity, and HAL statistics.

Displaying FCP initiator mode statistics through BCU

Use the **fcpim** command to display FCIP initiator mode statistics.

```
fcpim --stats <port_id> --query <port_id> <rpwwn [-l <lpwwn>]
```

where:

stats	Displays FCIP statistics.
query	Displays FCIP attributes.
port_id	ID of the port for which you want to display statistics.

lpwwn	Logical port world wide name. This is an optional argument. If the -l lpwwn argument is not specified, the base port is used.
rpwwn	Remote port world wide name.

Displaying FCP initiator mode statistics through HCM

Use the following steps to display **FCP IM Statistics** dialog box:

1. Launch the HCM.
2. Select the base adapter port from the device tree window.
3. Click **Monitor > Statistics > Remote port statistics > FCP IM Statistics**.

Logical port statistics

Use HCM and BCU to display logical port statistics for the following:

- Name server (NS) port logins (plogin) activity
- Register symbolic port name (RSPN_ID) identifier activity
- Register FC4 type identifier (RFT_ID) activity
- Register FC4 type identifier (RFT_ID) activity
- Get all port ID requests for a given FC4 type (NS_GID_FT) activity
- Retries
- Timeouts

Use these statistics to help determine if the adapter is not registering with the name server or cannot access storage. Following are examples of how these statistics indicate these problems:

- If name server port login (NS PLOGI) error rejects and unknown name server port login response (NS login unknown rsp) errors increase, then the adapter most likely cannot log in to the name server.
- If name server register symbolic port name identifier (NS RSPN_ID) or name server register symbolic port name identifier response (NS RFT_ID rsp) errors or rejects (NS RFT_ID rejects) are increasing, the adapter has a problem registering with the name server.
- If name server get all port ID response NS GID_FT rsp), rejects (NS_GID FT rejects), or unknown responses (NS_GID FT unknown rsp) are increasing, the adapter has a problem querying the name server for available storage.

Displaying logical port statistics through HCM

Display logical port statistics by selecting **Monitor > Statistics > Logical Port Statistics**

OR

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

Displaying logical port statistics through BCU

Use the **lport –stats** command to display logical port statistics.

```
lport –-stats <port_id> [-l lpwwn]
```

where:

port_id	ID of the port for which you want to display statistics.
lpwwn	Logical port world wide name for which you want to display statistics. This is an optional argument. If the -l lpwwn argument is not specified, the base port is used.
rpwwn	Remote port world wide name for which you want to display statistics.

Port statistics

Use BCU and HCM to display a variety of port statistics, such as transmitted and received frames and words, received loop initialization primitive (LIP) event counts, error frames received, loss of synchronization, link failure and invalid CRS counts, and end of frame (EOF) errors. Use these statistics to isolate link and frame errors. For example, loss of synch and loss of signal errors indicate a physical link problem. To resolve these problems, check cables, SFPs on the adapter or switch, and patch panel connections.

Displaying statistics through BCU

Use the **port –stats** BCU command to display statistics for a specified adapter port.

```
port --stats <port_id>
```

where:

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

Displaying statistics through HCM

Use the **Port Statistics** dialog box to monitor a variety of port data.

1. Launch the HCM.
2. Select the base adapter port from the device tree window.
3. Click **Monitor > Statistics > Port Statistics**.

Remote port statistics

Remote port statistics can help isolate end-to-end login problems. Use HCM and BCU to display statistics for the following:

- Port login (PLOGI) activity
- Authentication and discovery (ADISC) activity
- Logout (LOGO) activity
- RCSNs received
- Process logins (PRLI) received

- Hardware abstraction layer (HAL) activity

As an example of using these statistics for troubleshooting, if the host cannot see the target, you can verify that the remote port (rport) is reporting itself online by comparing the *rport offline* and *rport online* statistics. The *rport online* counter should be one greater than the *rport offline* counter. If not, clear the counters and retry connecting to the remote port. Verify the *rport online* and *rport offlin*e statistics again.

Displaying target statistics through HCM

Use the **Target Statistics** dialog box to display target statistics.

1. Launch the HCM.
2. Select the base adapter port from the device tree window.
3. Click **Monitor > Statistics > Remote Port Statistics > Target Statistics**.

Displaying remote port statistics through BCU

Use the **rport –stats** command to display remote port statistics.

```
rport –-stats <port_id> <rpwwn> [-l lpwwn]
```

where:

port_id	ID of the port for which you want to display rport statistics.
lpwwn	Displays the logical port world wide name. This is an optional argument. If the -l lpwwn argument is not specified, the base port is used.
rpwwn	Displays the remote port's port world wide name.

Quality of service statistics (HBA only)

Use HCM and BCU to display quality of service (QoS) statistics for individual ports. You can display statistics for fabric login (FLOGI) activity, exchange link parameter (ELP) activity, and received QOS registered state change notifications (RSCNs).

Displaying QoS statistics through HCM

Use the **QOS Statistics** dialog box to display QoS statistics.

1. Launch the HCM.
2. Select the base adapter port from the device tree window.
3. Click **Monitor > Remote Port Statistics > QOS Statistics**.

Displaying QoS statistics through BCU

Use the **qos –stats** command to display remote port statistics.

```
vport --stats <port_id> vpwwn
```

where:

port_id	ID of the port for which you want to display rport statistics.

Virtual port statistics (HBA only)

Use HCM and BCU to display logical port statistics for fabric discovery (FDISK) activity, logouts (LOGO) activity, NPIV support, number of fabrics online and offline, and fabric cleanups.

Use these statistics to isolate NPIV login problems. Following are examples of what to check if virtual devices are not listed in the name server:

- If *FDISK sent* and *FDISK accept* statistics do not match, the fabric or switch may not be ready for data transmission. This is normal as long as it does not persist. If it does persist, there may be a problem in the fabric or a protocol issue between the adapter and fabric. Note that in this case *FDISK retries* also increase.
- Check the *No NPIV support* statistics to verify that NPIV is supported and enabled on the switch.

Displaying virtual port statistics through HCM

Display statistics by selecting **Monitor > Statistics > Virtual Port Statistics**

OR

Right-click a virtual port on the device tree and select **Virtual Port Statistics**.

Displaying virtual port statistics through BCU

Use the **vport –stats** command to display statistics.

```
vport --stats <port_id> vpwwn
```

where:

port_id	ID of the port for which you want to display rport statistics.
vpwwn	Displays the statistics for the virtual port by its WWN. If no part WWN is specified, the information provided is for the base vport.

VLAN Statistics (CNA only)

The HCM and BCU display statistics related to a specific VLAN, such as VLAN ID, VLAN name, number of transmit and receive bytes, length of time between byte transmission and reception, and correction status. You can also use options to set the polling frequency, start polling, and reset statistics.

Displaying virtual port statistics through HCM

To display the **VLAN Statistics** dialog box, use the following steps:

1. Select an Ethernet port from the device tree.
2. Select **Monitor > Statistics > VLAN Statistics** from the main menu.

The **VLAN Statistics** dialog box displays.

Displaying virtual port statistics through BCU

Use the vlan –query command to display VLAN statistics.

```
vlan --query <port_id> <vlan_id>
```

where:

port_id	Specifies the Ethernet port associated with the VLAN.
vlan_id	Specifies the VLAN identifier. The range for the VLAN ID is 1 to 4094.

Diagnostics

Diagnostics, available through BCU commands and HCM, evaluate the integrity of adapter hardware and end-to-end connectivity in the fabric. All of these diagnostics can be used while the system is running.

NOTE
Be sure to disable the port before running any type of port diagnostics.

NOTE
It is advisable to not perform other operations on the adapter while running HCM or BCU diagnostics.

Beaconing

Initiate beaconing on a specific adapter port to flash the port LEDs and make it easier to locate the adapter in an equipment room.

Initiate *link beaconing* to flash the LEDs on a specific adapter port and the LEDs on a connected switch port to verify the connection between adapter and switch. When you initiate link beaconing, commands are sent to the other side of the link. When the remote port receives these commands, that port's LEDs flash. The remote port sends a command back to the originating port. When that port receives this command, the port's LEDs flash.

NOTE
To initiate link beaconing, this feature must be available on the connected switch.

Toggle beaconing on and off and set beaconing duration using the BCU or HCM.

Enabling beaconing through BCU

Use the **diag –beacon** command to enable beaconing for a specific adapter port.

```
diag --beacon <port_id> <on | off> [<duration>]
```

where:

port_id	ID of the port for which you want to enable beaconing.
duration	Length of time between blinks.

Use the **fcdiag –linkbeacon** command to enable link beaconing.

```
fcdiag --linkbeacon <portid> {on | off} [<duration>]
```

where:

port_id	ID of the port for which you want to run a link beacon test.
on | off	Toggle on or off. If turned on, you can specify duration.
duration	Length of time between blinks.

Enabling beaconing through HCM

Enable link and port beaconing using the following steps.

1. Launch the HCM.
2. Select the base adapter port from the device tree window.
3. Click **Configure > Beacon**.
4. Click the **Beacon Link** check box, the **Beacon Port** check box, or both.

Internal and external loopback tests

Use the BCU or the HCM to perform a loopback test for a specific port. Loopback tests require that you disable the port. The following loopback tests are available:

- Internal

  Random data is sent to the adapter port, then returned without transmitting through the port. The returned data is validated to determine port operation. Errors may indicate a failed port.

- External

  For this test, a loopback connector is required for the port. Random data is sent to the adapter port. The data transmits from the port and then returns. The returned data is validated to determine port operation. Errors may indicate a failed port.

Performing loopback tests through BCU

Use the **diag –loopback** BCU command test to verify port function through a loopback test.

```
bcu diag --loopback <port_id> [-t <loopback_type>][<duration>][-s <speed>]
[-c <frame_count>] [-p <pattern>]
```

where:

port_id	ID of the port for which you want to run the test.
loopback type	Type of loopback test. Possible values are internal, external, and serdes.
speed	HBAs only. For 8 Gbps adapter, this is 2, 4, or 8. For 4 Gbps adapter, this is 1, 2 or 4.
duration	Length of time between blinks.
frame count	Integer from 0 to 4,294,967,295. Default is 8192.
-p pattern	Hex number. Default value is A5A5A5A5.

Performing loopback tests through HCM

Use the **Port Tests** tab on the **Diagnostics** dialog box to perform a loopback test.

1. Launch the HCM.
2. Select **Configure > Diagnostics**
3. Click the **Port Tests** tab.
4. Select **Loopback Test**.

   You can modify the following test parameters

   - Subtest - The three options are Internal, Serdes, and External.
   - Link Speed (HBA only) - For 8G adapter, 2G, 4G and 8G. For 4G adapter, 1G, 2G and 4G.
   - Frame Count - Integer from 0 to 4,294,967,295. Default value is 8192.
   - Data Pattern - Hex value. Default value is A5A5A5A5
5. Click **Start**.

Ethernet port loopback test (CNA only)

Use BCU commands and HCM to test the Ethernet data path from the host to serdes or external loopback based on your selection. You must disable the port before testing and use a loopback connector for the test.

NOTE
For 64-bit platforms only, you cannot perform Ethernet loopback tests on the port unless a VLAN is first created for the port.

Performing Ethernet loopback tests through HCM

Using the **Ethernet Tests** tab on the **Diagnostics** dialog box, you can set test parameters such as external or serdes subtest, link speed, frame count, test cycle, and data pattern to test. Results display on the bottom of the tab as the test commences.

1. Launch the HCM.
2. Select **Configure > Diagnostics**.
3. Click the **Ethernet Tests** tab.
4. Select **Loopback Test**.

Performing Ethernet loopback tests through BCU

Use the ethdiag --loopback command to run an Ethernet loopback test.

```
bcu ethdiag --loopback <port_id> [-t <loopback_type] [-c <frame_count>] [-p
pattern]
```

where:

port_id	ID of the port for which you want to run the test.
-t loopback-type	Specifies the loopback type. Possible values are serdes, and ext.

-c frame count Specifies the frame count.

-p pattern Specifies the pattern (must be one hex word).

NOTE
You must disable the port before running a loopback test.

PCI loopback test

Use BCU commands or HCM to perform a PCI loopback test for a specific port. In this test, a data pattern is sent from the host to adapter firmware through the PCI bus. The returned data is validated to determine PCI operation.

NOTE
You need to disable the port before you run loopback tests.

Performing PCI loopback tests through BCU

Use the **diag –pciloopback** BCU command to perform a PCI loopback test.

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

where:

port_id	ID of the port from which you want to run the test.
pattern	Specifies the data test pattern. Must be at least one hexadecimal word.
frame count	Specifies the frame count as an integer from 0 to 4,294,967,295.

Performing PCI loopback tests through HCM

Use the **Port Tests** dialog box to perform a PCI loopback test.

1. Launch the HCM.
2. Select **Configure > Diagnostics**.
3. Click the **Port Tests** tab.
4. Select **PCI Loopback Test**.

   You can modify the following parameters

   - Frame count: Specifies the frame count as an integer from 0 to 4,294,967,295.
   - Data pattern: Specifies the data test pattern. Must be at least one hexadecimal word.
   - Test cycle: The number should be positive and the default is 1.
5. Click **Start**.

Memory test

Use the BCU or the HCM to perform a memory test for the adapter.

NOTE
Performing the memory test disables the adapter.

Performing a memory test through BCU

Use the **diag –memtest** command to test the adapter's memory blocks.

```
diag --memtest <ad_id>
```

where:

ad_id ID of the adapter.

Performing a memory test through HCM

Use the **Port Tests** dialog box to perform a memory test.

1. Launch the HCM.
2. Select **Configure > Diagnostics**.
3. Click the **Port Tests** tab.
4. Select **Memory Test**.
5. Specify the test cycle using a positive number.
6. Click **Start**.

Adapter temperature

Use the BCU **diag –tempshow** command to read the adapter's temperature sensor registers.

```
diag --tempshow <ad_id>
```

where:

ad_id ID of adapter.

Ping end points

Use the BCU and HCM to ping a Fibre Channel end point from an adapter port to determine the basic connectivity to the remote port and monitor network latency. Note that this is not supported on Solaris systems.

Issuing a ping command to end points through BCU

Use the **fcdiag --fcping** BCU command to test the connection to a Fibre Channel end point.

```
fcdiag --fcping <port_id> <rpwwn> [-l lpwwn]
```

where:

port_id	ID of the adapter port from which you want to ping the remote port.
rpwwn	Remote port WWN that you want to ping.
lpwwn	Logical port WWN. 0 indicates the base port.

Issuing a ping command to end points through HCM

Use the **Protocol** tab on the **Diagnostics** dialog box to test the connection to Fibre Channel end points. Use the following steps to ping end points.

1. Launch the HCM.
2. Select **Configure > Diagnostics.**
3. Click the **FC Protocol Tests** tab.
4. Select **FC Ping Test**.
5. Select the adapter port and target that you wish to ping.
6. Enter a test cycle if applicable.
7. Click **Start**.

Trace route

Use the BCU and HCM to trace the SAN path between the adapter and remote end point.

Tracing the route through BCU

Use the **fcdiag --traceroute** BCU command to trace the route between end points.

```
fcdiag --fctraceroute <port_id> <rpwwn> [-l lpwwn]
```

where:

port_id	ID of the port from which you want to trace the route.
rpwwn	Remote port WWN to which you want to trace the route.
lpwwn	Logical port WWN. 0 indicates the base port.

Tracing the route through HCM

Use the FC Trace Route feature to trace the route between the adapter port and a target port:

1. Launch the HCM.
2. Select **Configure > Diagnostics**.
3. Click the **FC protocol Tests** tab.

4. Select **FC Trace Route**.
5. Select the adapter port and target for which you wish to trace the route.
6. Enter a test cycle if desired.
7. Click **Start**.

Echo test

Use the BCU and HCM to initiate an echo test between the adapter port and a Fibre Channel end point. This sends an ECHO command and response sequence between the adapter port and target port to verify connection with the target.

Performing an echo test through BCU

Use the **fcdiag –fcecho** BCU command to initiate an echo test between the adapter and remote port.

```
fcdiag –-fcecho <port_id> <rpwwn> [-l lpwwn]
```

where:

port_id	ID of the port for which you want to perform the test.
rpwwn	Remote port WWN to which the echo command is being sent.
lpwwn	Logical port WWN. 0 indicates the base port.

Performing an echo test through HCM

Use the Echo Test feature to initiate an echo test between the adapter port and a Fibre Channel end point:

1. Launch the HCM.
2. Select **Configure > Diagnostics**
3. Click the **FC Protocol Tests** tab.
4. Select **Echo Test**.
5. Select the adapter port and target port for the test.
6. Enter a test cycle if applicable.
7. Click **Start**.

SCSI test

Use the **fcdiag –scsitest** BCU command to test the SCSI link between the adapter and remote port.

```
fcdiag –-scsitest <port_id> <rpwwn> [-l lpwwn]
```

where:

port_id	ID of the port for which you want to test the SCSI link.
rpwwn	Remote port WWN connected to the adapter by the SCSI link.

lpwwn Logical port WWN. 0 indicates the base port; otherwise.

Test Logs

While running a diagnostic test in HCM, a log of the test results displays at the bottom of the **Diagnostic** dialog box. Display details of the test log by double-clicking a row in the log.

Collecting LLDP data (CNA only)

Collect information on the Link Layer Discovery Protocol (LLDP) associated with a specific CNA using the HCM **LLDP Properties** panel.

The **LLDP Properties** panel displays information such as the MAC address of the local system, LLDP operational status, system management address, user-configured port description, port identification, configured name of local system, system capabilities based on system model, and time to live (TTL) values in LLDP frames.

To collect LLDP data, perform the following steps.

1. Select a CNA in the device tree.
2. Click the **LLDP** tab in the right pane.

Collecting SFP data

This section provides an overview of BCU commands and HCM features that provide information, on small form factor pluggable (SFP) transceivers.

SFP properties

BCU and HCM provide detailed information on the SFP transceiver for a selected port, such as its health status, port speed, connector type, minimum and maximum distance, as well as details on the extended link.

Display SFP properties through BCU

Use the **diag –sfpshow** BCU command to display detailed attributes for a specific SFP transceiver.

```
diag --sfpshow <port_id>
```

where:

port_id ID of the port for which you want to display SFP attributes.

Initiating SFP properties through HCM

Use the port **SFP** properties dialog box to display properties for a selected small form-factor pluggable (SFP) transceiver.

1. Launch the HCM.
2. Select a port in the device tree.

3. Click the **SFP** tab in the right pane.

Port power on management

Use the **Port POM** properties panel to monitor the SFP attributes. A notification is given for any parameters that are not within the power, temperature, voltage, and current specification.

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

Collecting port data

This section provides an overview of BCU commands and HCM features that provide information on adapter ports. such as port WWN, node WWN, port type, configured speed, operating speed, configured topology, operating topology. link and port beaconing state, and other information.

Displaying base port properties

Use the **Base Port Properties** panel to display information about a selected base adapter port, such as the following:

- Port number
- PWWN and node WWN
- Offline or online state
- Role of port (for example, FCP initiator)
- Fibre Channel address
- WWN of the attached switch

Use the following steps to display base port properties.

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

Displaying CEE port properties (CNA only)

Use the **CEE Port Properties** panel to display information for a selected converged Ethernet adapter (CEE) port.

Information such as the following displays:

- Node WWN
- PWWN
- Port type
- Fibre Channel address
- CEE online or offline state
- Local port MAC address
- Configured port speed

- Operating speed
- Receive and transmit BB credit
- Frame data field size
- MPIO enabled or disabled status
- Queue depth
- Interrupt control coalesce on or off status
- Interrupt control latency and delay values
- Boot over SAN configuration
- Beaconing state
- Target rate limiting on or off status
- FC-SP parameter statistics
- MPIO on or off state
- Health status of Fibre Channel security protocol parameters

To display CEE port properties, use the following steps:

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

Displaying Ethernet port properties (CNA only)

The **HCM Ethernet Port Properties** panel enables you to display the properties associated with a selected Ethernet port.

Information such as the following displays:

- Name of Ethernet device
- Port type
- MAC address
- IOC identification
- WWN of hardware
- Status of port, such as linkup
- Ethernet logging level

To display Ethernet port properties, use the following steps.

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

Displaying FCoE port properties (CNA only)

Use the HCM **FCoE Port Properties** to display FCoE port properties such as the following:

- Port WWN
- Node WWN
- Supported class
- FC frame size

- Maximum transmission unit (MTU)
- Target rate limiting (TRL) enabled or disabled status
- SCSI queue depth
- Beaconing status
- Fibre Channel Initialization Protocol (FCIP) online or offline state
- Priority group ID
- Bandwidth percentage for priority group
- MAC address for FCoE forwarder
- Fabric WWN
- Fibre Channel map ID
- FCoE forwarder writing or nonwriting mode

To display the HCM **FCoE Port Properties** panel, use these steps.

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

Displaying remote port properties

Use the HCM **Remote Port Properties** panel to display properties that are associated with the remote port, such as WWN, node WWN, port name, Fibre Channel address, frame data field size, online or offline state, role (such as target or initiator), remote device information, QoS priority, QoS flow, and target ID.

1. From the device tree, select a remote port.
2. Click the **Remote Port Properties** tab in the right panel.

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

Displaying logical port properties

Use the HCM **LPorts Properties** panel to display properties associated with a logical port, such as port and node WWN, Fibre Channel address, online or offline state, and name server activity. To display logical port properties, use the following steps.

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

Displaying virtual port properties

Use the HCM **Virtual Port Parameters** properties panel to display the properties associated with a virtual port, such as port and node WWN, Fibre Channel address, offline or online state, role (such as FCP initiator), and attached switch WWN. To display virtual port properties, use the following steps:

1. From the device tree, select a virtual port.
2. The **Virtual Port Parameters** properties panel displays.

Displaying the port log

Use the HCM **debug –portlog** BCU command to display a log of Fibre Channel frames and other main control messages that were sent out and received on a specific port. You can use this information to isolate adapter and Fibre Channel protocol problems.

```
debug --portlog <port_id>
```

where:

port_id The ID of the port for which you want to display the port log.

NOTE
If the port log is disabled, a warning message displays. Use the **debug -portlogctl** command to enable and disable the port log.

Displaying the port list

Use the **port –list** BCU command to list all physical ports on the adapter along with their physical attributes, such as PWWN, Fibre Channel address, port type, speed, and state.

```
port --list
```

Performing a port query

Use **port –query** BCU command to display port information, such as WWN, NWWN, state, current and configured speed, topology, received and transmitted BB_Credits, and beacon status.

```
port --query <port_id>
```

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

Displaying port speed

Use **port –speed** BCU command to display the current port speed setting.

```
port --speed <port_id>
```

where:

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

Authentication settings

Use the Brocade CLI utility (BCU) or the HCM GUI to display the adapter authentication settings and status.

Displaying authentication settings through HCM

Use the **Fibre Channel Security Protocol Configuration** dialog box to display authentication settings.

1. Select a port from the device tree.
2. Select **Configure > FC-SP > Authentication**.

   The **Fibre Channel Security Protocol Configuration** dialog box displays. This displays the current CHAP secret, hashing algorithm, and group value.

Displaying authentication settings through BCU

Use the BCU **auth –show** command to display authentication settings.

```
auth --show <port_id>
```

where:

port_id	ID of the port for which you want to display authentication settings.

QoS and target rate limiting settings (HBA only)

Target rate limiting throttles the Fibre Channel Protocol (FCP) read traffic rate to slow-draining targets to reduce or eliminate network congestion and alleviate I/O slowdowns to faster targets. Quality of Service (QoS) works in conjunction with the QoS feature on Brocade switches to assign traffic priority (high, medium (default), low) to a given source and destination traffic flow.

Determining QoS and other settings through BCU

Use the following BCU commands to determine current status and configuration for QoS and target rate limiting settings:

- Use the following BCU command to determine Target Rate Limiting speed and enabled status.

  ```
  ratelim --query <port-id>
  ```

  where:

port_id	ID of the port for which you want to display target rate limiting settings.

- Use the following BCU command to display QoS and target rate limiting enabled status and target rate limiting default speed.

  ```
  port --query <port-id>
  ```

  where:

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

- Use the following command to display QoS status and information for a port.

  ```
  qos --query <port_id>
  ```

  where:

port_id	ID of the port for which you want to display target rate limiting settings.

- Use the following command to determine operating speed of the remote port, QoS priority, and target rate limiting enforcement:

  ```
  rport --query <port_id> <rpwwn>
  ```

where:

port_id	Specifies the ID of the port for which you want to query attributes of a remote port.
rpwwn	Remote port WWN. You can obtain the RPWWN from the BCU rport --list <port_id> command.

Determining QoS and other settings through HCM

Use HCM in the following ways to determine current status and configuration for QoS and target rate limiting settings:

- Use the **Port Properties** panel in HCM to display configured QoS parameters.
  1. Select a port in the device tree.
  2. Click the Properties tab in the right pane.

     Port Properties panel displays.
- Use the **Remote Port Properties** panel in HCM to display information on target rate limiting and QoS for the remote port.
  1. From the device tree, select a remote port (target or initiator).
  2. Click the **Remote Port Properties** tab in the right pane.

     The **Remote Port Properties** panel displays.

Persistent binding

Persistent binding is a feature of adapters that enables you to permanently assign a system SCSI target ID to a specific Fibre Channel (FC) device, even though the device's ID on the FC loop may be different each time the FC loop initializes. Persistent binding is available in the Windows and VmWare environments only.

Use the HCM or BCU to display target ID mapping for an adapter port.

BCU

Use the **pbind –list** BCU command to query the list of mappings for persistent binding on a specific port.

```
pbind --list <port_id> <pwwn>
```

where:

port_id	ID of the port for which you want to query mappings.
pwwn	Port World Wide Name

HCM

Use the **Persistent Binding** dialog box to determine SCSI target ID mappings, perform the following steps:

1. Launch the HCM.
2. Select an adapter or port from the device tree.

3. Select **Configure > Persistent Binding**.

   OR

   Right-click on an adapter or port in the device tree and select **Persistent Binding** from the list.

   The **Persistent Binding** dialog box at the host level displays.

Chapter

4

Performance optimization

In this chapter

Tuning storage drivers

This section provides resources for optimizing performance in HBAs and CNAs by tuning the unified storage drivers on Linux, Windows, Solaris, and VMware systems. To optimize performance for CNA products, also use resources under "Tuning network drivers" on page 79.

Linux tuning

Linux disk I/O scheduling reorders, delays, and merges requests to achieve better throughput and lower latency than would happen if all the requests were sent straight to the disk. Linux 2.6 has four different disk I/O schedulers: noop, deadline, anticipatory and completely fair queuing. Enabling the "noop" scheduler avoids any delays in queuing of I/O commands. This helps in achieving higher I/O rates by queuing multiple outstanding I/O requests to each disk.

To enable the noop scheduler, run the following commands on your system.

```
for i in /sys/block/sd[b-z]/queue/scheduler
do
echo noop > $i
done
```

NOTE
You must disable the default scheduler because it is not tuned for achieving the maximum I/O performance.

For performance tuning on Linux, refer to the following publications:

- *Workload Dependent Performance Evaluation of the Linux 2.6 IO Schedulers*
  Heger, D., Pratt, S., Linux Symposium, Ottawa, Canada, July 2004
- *Optimizing Linux Performance*
  HP Professional Books, ISBN: 0-13-148682-9
- *Performance Tuning for Linux Servers*
  Sandra K. Johnson, Gerrit Huizenga, Badari Pulavarty, IBM Press, ISBN: 013144753X
- *Linux Kernel Development*
  Robert Love, 2nd edition, 2005

Solaris tuning

To increase I/O transfer performance, set the following parameters on your system:

- Set the maximum device read/write directive (maxphy).
- Set the disk maximum transfer parameter (ssd_max_xfer_size).

Please refer to *Sun StorageTek SAM File System Configuration and Administration Guide* document for details of the two parameters."

Windows tuning

Windows tuning involves configuring the driver and operating system tunable parameters.

Driver tunable parameters

You can manipulate several driver parameters to increase performance.

bfa_lun_queue_depth (outstanding I/O requests per LUN)

The driver uses a default LUN queue depth value of 32. This value is chosen to reflect the average operating I/O load in most scenarios. Storport manages the I/O throttling at the per-LUN level to guarantee the configured queue depth. During performance testing with specific high-end array LUNs, it may be necessary to increase this I/O queue depth to a much larger value. Microsoft recommends a value of 96 during high-performance testing scenarios. If the queue depth is not sufficient, then you will notice performance degradation.

The queue depth can be configured at the following registry location with any value within the range 1 – 254.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bfad\Parameters\Device\bfa_lun_queue_depth

Interrupt moderation using interrupt coalescing feature

Moderating interrupts can often result in reduced CPU load on the host but, unless interrupt moderation is performed intelligently, the CPU savings might increase latency.

The default values for the Fibre Channel port interrupt attributes are configured as follows:

- Interrupt delay

  Default: 1 microsecond

  Valid Range: 0 – 1125 microseconds (Note that the value of 0 disables the delay timeout interrupt.)

- Interrupt latency

  Default: 1 micro second

  Valid Range: 0 – 225 micro \seconds (Note that the value of 0 disables the latency monitor timeout interrupt.)

Message signaled interrupts (MSI-X)

All Brocade adapters support MSI-X, an eXtended version of the MSI defined in PCI 3.0 specification. MSI-X helps improve overall system performance by contributing to lower interrupt latency and improved host CPU utilization.

MSI-X is supported in Windows Vista and Windows Server 2008.

To enable MSI-X, set the following registry key value to 0.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bfad\Parameters\Device\msix_disable
```

OS tunable parameters

Please see the section “Storage Stack Drivers” in *Disk Subsystem Performance Analysis for Windows Server 2003 optimizations* located on the following website.

http://download.microsoft.com

Please see the sections “Performance Tuning for Storage Subsystem” and “I/O Priorities” in *Performance Tuning Guidelines for Windows Server 2008* located on the following website.

http://www.microsoft.com

VMware tuning

For performance tuning on VMware, refer to the following publications on the VMware website at www.vmware.com:

- *Performance Tuning Best Practices for ESX Server 3*. Refer to the following sections:
  - Storage Performance Best Practices
  - Related Publications
- *Fibre Channel SAN Configuration Guide*. Refer to “Using ESX Server with SAN: Concepts.”

Tuning network drivers

This section provides resources for tuning network drivers for CNAs on Linux, Windows, and VMware systems. Note that the default values set for the driver parameters discussed in this section should provide optimum performance. However, you may need to modify these values depending on your network environment. Please follow your host and operating system guidelines when doing so.

Windows tuning

All Windows tunable parameters for the network driver are optimized for best performance using default values. For details on configuring parameters, refer to the “Adapter Configuration” chapter in the *Brocade Adapters Installation and Reference Manual*.

Parameters are listed in the following table.

Parameter	Default
Log Level	3
Interrupt Moderation (Set for receive interrupts)	On
Jumbo Packet Size	1500

Parameter	Default
TCP-UDP Checksum Offload	Enabled
Network Address	N/A
Receive Buffers	32
Transmit Buffers	16
Priority and VLAN	Disable
Receive Side Scaling (RSS)	Enabled
Header Data Split (HDS)	Enabled
Large Segmentation Offload V1 IPv4 (LSOv1)	Enabled
Large Segmentation Offload V2 IPv4 (LSOv2)	Enabled
Large Segmentation Offload V2 IPv6 (LSOv2)	Enabled
FlowControl, Transmit (Tx) and Receive (Rx)	Enabled
Interrupt Moderation	Enabled
VLAN ID	Disabled
Priority and VLAN Support	Enabled

Linux tuning

All Linux tunable parameters for the network driver are optimized for best performance using default values. For details on configuring these parameters, refer to the “Adapter Configuration” chapter in the *Brocade Adapters Installation and Reference Manual*.

Parameters are listed in the following table.

Parameter	Default
Interrupt moderation	Enabled
Log Level	3
Jumbo packet size	1,500 bytes
TCP=UDP checksum offload	Enabled
TCP Segmentation Offload (TSO)	Enabled
MSI-X (Message Signaled Interrupts Extended	Enabled

VMware tuning

All VMware tunable parameters for the network driver are optimized for best performance using default values. For details on configuring these parameters, refer to the “Adapter Configuration” chapter in the *Brocade Adapters Installation and Reference Manual*.

Specific recommendations for jumbo packet size and NetQueue follow.

Parameters are listed in the following table.

Parameter	Default
Jumbo Packet Size	1500
VLAN ID	Disabled
MSI-X (Message Signaled Interrupts Extended)	Enable (1)
Interrupt Moderation (Set for receive interrupts)	On
NetQueue	Disable

Jumbo packet size

Recommendations to enhance performance

Increase throughput by setting MTU to 9000 bytes.

How to change values

Refer to instructions for Windows “Network driver parameters” in Appendix A of *Brocade Adapters Installation and Reference Manual*.

References for more tuning information

Refer to the *10Gbps Networking Performance on ESX 3.5 Update 1* available through www.vmware.com.

NetQueue

NetQueue improves receive-side networking performance on servers in 10 Gigabit Ethernet virtualized environments. NetQueue provides multiple receive queues on the CNA, which allows processing on multiple CPUs to improve network performance.

MSI-X is an eXtended version of Message Signaled Interrupts defined in the PCI 3.0 specification.. All Brocade adapters support MSI-X, which helps improve overall system performance by contributing to lower interrupt latency and improved host CPU utilization. MSI-X is enabled by default in VMware ESX Server 3.5, and must remain enabled for NetQueue to function. Please make sure that bnad_msix=0 is not listed in VMware module parameters because that would disable NetQueue.

For the Brocade driver, you cannot directly configure the number of NetQueue and filters per NetQueue. By default, these values are based on the number of receive queue sets used, which is calculated from the number of CPUs in the system. You can change the number of NetQueues from the default (number of CPUs) by setting the number of receive queue sets (bnad_rxqsets_used).

Default value: Disable

Possible values: Enable, Disable

Recommendations to enhance performance

Enabling NetQueue utilizes multiple receive queues of the Brocade adapter, which can be handled by multiple CPUs on the host system, thus improving performance.

How to change values

Refer to instructions for Windows “Network driver parameters” in Appendix A of *Brocade Adapters Installation and Reference Manual*.

References for more tuning information

Refer to the *10Gbps Networking Performance on ESX 3.5 Update 1* available through www.vmware.com.

Appendix

Event Message Reference

A

This appendix provides details on event messages generated by adapter drivers. These events display in host system logs and the HCM master log. Events are organized as originating from the network driver only, storage driver only, or network and storage driver.

TABLE 9 Driver event messages

Message	Severity	Event Type	Category	Sub Category	Cause	Action
Network Driver Events						
Base port link up: Hardware Address = [Base port MAC]	Information	Network driver	10 (EthPort)	Up	Base port Ethernet link is up.	No action required.
Base port link down: Hardware Address = [Base port MAC]	Warning	Network driver	10 (EthPort)	Down	Base port Ethernet link is down.	No action required.
Base port Ethernet Link is enabled: Hardware Address = [Base port MAC]	Information	Network driver	10 (EthPort)	Enabled	Ethernet port enabled by user.	No action required.
Base port link is disabled: Hardware Address = [Base port MAC].	Warning	Network driver	10 (EthPort)	Disabled	Ethernet port disabled by the user.	No action required.
Storage Driver Events						
Authentication enabled for base port: WWN = [Base port WWN]	Information	Storage driver	8 (AUDIT)	Enabled	Authentication enabled by user command.	No action required.
Authentication disabled for base port: WWN = [Base port WWN]	Information	Storage driver	8 (AUDIT)	Disabled	Authentication disabled by user command.	No action required.
Fabric name changed for base port: WWN = [Base port WWN]	Warning	Storage driver	2 (PORT)	Changed	Fabric name changed for base port.	No action required.
Logical port WWN: [logical port WWN], Role: [initiator, target, IPFC mode etc.] is deleted.	Information	Storage driver	3 (LPORT)	Deleted	Logical port deleted.	No action required.
Logical port online: WWN = [logical port WWN], Role: [initiator, target, IPFC mode etc.]	Information	Storage driver	3 (LPORT)	Online	Logical port (base or logical) logged into fabric.	No action required.
Logical port taken offline: WWN = WWN = [logical port WWN], Role: [initiator, target, IPFC mode etc.]	Information	Storage driver	3 (LPORT)	Offline	Logical port (base or logical) logged out of fabric.	No action required.
Logical port lost fabric connectivity: WWN = [logical port WWN], Role: [initiator, target, IPFC mode etc.].	Error	Storage driver	3 (LPORT)	Offline	Logical port (base or logical) lost fabric connectivity.	Check switch and adapter configuration.
New logical port created: WWN = [logical port WWN], Role = [initiator, target, IPFC mode etc.]	Information	Storage driver	3 (LPORT)	Created	New logical port created.	No action required.

TABLE 9 Driver event messages

Message	Severity	Event Type	Category	Sub Category	Cause	Action
New virtual port created using proprietary interface: WWN = [logical port WWN], Role: [initiator, target, IPFC mode etc.].	Information	Storage driver	3 (LPORT)	Created.	New virtual port created.	No action required.
New virtual port created using standard interface: WWN = [logical port WWN], Role: [initiator, target, IPFC mode etc.]	Information	Storage driver	3 (LPORT)	Created	New virtual port created.	No action required.
QOS priority changed to [New QOS flow ID]: RPWWN = [Remote port WWN] and LPWWN = [Logical port WWN].	Information	Storage driver	4 (RPORT)	Changed	QOS priority changed.	No action required.
QOS flow ID changed to [New QOS flow ID]: RPWWN = [Remote port WWN] and LPWWN = [Logical port WWN].	Information	Storage driver	4 (RPORT)	Changed	QOS flow ID changed.	No action required.
Remote port (WWN = [remote port WWN] online for logical port (WWN = [logical port WWN]).	Information	Storage driver	4 (RPORT)	Online	Login nexus established with remote port.	No action required.
Remote port (WWN = [remote port WWN]) offlined by logical port (WWN = [logical port WWN]).	Information	Storage driver	4 (RPORT)	Offline	Login nexus with remote port terminated by logical port.	No action required.
Remote port (WWN = [remote port WWN]) connectivity lost for logical port (WWN = [logical port WWN]).	Error	Storage driver	4 (RPORT)	Offline	Login nexus with remote port is lost.	Check if remote port is having issues.
Target (WWN = [Target WWN]) is online for initiator (WWN = [Initiator WWN]).	Information	Storage driver	5 (ITNIM)	Online	SCSI IT-Nexus established between initiator and target.	No action required.
Target (WWN = [Target WWN]) offlined by initiator (WWN = [Initiator WWN]).	Information	Storage driver	5 (ITNIM)	Offline	SCSI IT-Nexus terminated by Initiator.	No action required.
Target (WWN = [Target WWN]) connectivity lost for initiator (WWN = [Initiator WWN]).	Error	Storage driver	5 (ITNIM)	Offline	SCSI IT-Nexus terminated between initiator and target.	No action required.
Virtual port deleted using proprietary interface: WWN = [logical port WWN], Role: [initiator, target, IPFC mode etc.].	Information	Storage driver	3 (LPORT)	Deleted	Virtual port deleted.	No action required.
Virtual port deleted using standard interface: WWN = [logical port WWN], Role: [initiator, target, IPFC mode etc.]	Information	Storage driver	3 (LPORT)	Deleted	Virtual port deleted.	No action required.
Virtual port login failed. Duplicate WWN = [logical port WWN] reported by fabric.	Warning	Storage driver	3 (LPORT)	Failed	Duplicate WWN reported by fabric.	Delete this vport and create with a different WWN.

TABLE 9 Driver event messages

Message	Severity	Event Type	Category	Sub Category	Cause	Action
Virtual port (WWN = [logical port WWN]) login failed. Max NPIV ports already exist in fabric/fport.	Warning	Storage driver	3 (LPORT)	Failed	Max NPIV ports already exist in fabric/fport.	Check fabric and fport configuration
Virtual port (WWN = %s) login failed.	Warning	Storage driver	3 (LPORT)	Failed	Unknown error.	Check fabric/fport configuration.
Network and Storage Driver Events						
Adapter removed: SN = [adapter serial number]	Warning	Network and storage driver	1 (Adapter)	Removed	Adapter removed.	Check PCIe slot and configuration.
Authentication successful for base port: WWN = [base port WWN or MAC]	Information	Network and storage driver	2 (Port)	Successful	Authentication successful.	No action required.
Authentication unsuccessful for base port: WWN = [base port WWN or MAC]	Error	Network and storage driver	2 (Port)	Failure	Authentication failure.	Mismatch of FC-SP configuration between switch and HBA. Also, check the authentication secret settihg.
Base port enabled: Hardware Address = [base port WWN or MAC]	Information	Network and storage driver	2 (Port)	Enabled	Base port enabled by user command.	No action required.
Base port disabled: Hardware Address = [base port WWN or MAC]	Warning	Network and storage driver	2 (Port)	Disabled	Base port disabled by user command.	No action required.
Base port online: WWN = [Base Port WWN]	Information	Network and storage driver	2 (Port)	Online	Base port logged into fabric.	No action required.
Base port offline: WWN = [Base Port WWN]	Warning	Network and storage driver	2 (Port)	Offline	Base port logged out of fabric.	No action required.
Base port (WWN = [base port WWN or MAC]) lost fabric connectivity.	Error	Network and storage driver	2 (Port)	Logout	Base port lost connection with fabric.	Check switch and HBA configuration. Also, check SFP and cable connection.
Heart Beat of IOC [IOC instance number] is good.	Information	Network and storage driver	9 (TOC)	Restart	Successful restart of firmware after a failure.	No action required.
Heart Beat of IOC [IOC instance number] has failed.	Critical	Network and storage driver	9 (TOC)	Crash	Firmware not responding.	Collect all error information and restart the firmware. Invoke bfa_supportsave.
IOC [IOC instance number] is enabled.	Information	Network and storage driver	9 (TOC)	Enabled	Adapter firmware started by user command.	No action required.

TABLE 9 Driver event messages

Message	Severity	Event Type	Category	Sub Category	Cause	Action
IOC [IOC instance number] is disabled	Warning	Network and storage driver	9 (TOC)	Disabled	Adapter firmware stopped by user command.	No action required.
New adapter found: SN = [adapter serial number] base port Hardware address = [Bae port WWN or MAC]	Information	Network and storage driver	1 (Adapter)	Added	Adapter added to host.	No action required.
New SFP found: port [base port number] Hardware Address = [Base port WWN or MAC]	Information	Network and storage driver	2 (Port)	Found	User plugged in an SFP.	No action required.
QOS negotiation failed for base port: WWN = base port WWN or MAC]	Warning	Network and storage driver	2 (Port)	Failure	QOS negotiation failed.	Check switch and HBA configuration.
SFP removed: port [base port number], Hardware Address = [Base port WWN or MAC]	Warning	Network and storage driver	2 (Port)	Removed	SFP removed.	Check if SFP is inserted properly.
SFP POM level to [aggregated SFP temperature, voltage, rx and tx power level]: port [base port number], Hardware Address = [base port WWN or MAC].	Warning	Network and storage driver	2 (Port)	Unhealthy	Change of current value against threshold of temperature, voltage and rx/tx power of SFP. POM (pluggable optical module) plugs into the SFP.	If POM level is not normal please check the SFP.

Index

E

F

H

I

L

M

N

O

P

Q

R

S

T

U

V

W