Brocade® Fabric OS® Troubleshooting and Diagnostics Reference Manual, 9.2.x

Technical Reference Manual
April 28, 2023

Table of Contents

About This Document

This book is a companion guide to be used in conjunction with the *Brocade® Fabric OS ® Administration Guide*. Although it provides many common troubleshooting tips and techniques, it does not teach troubleshooting methodology.

Troubleshooting should begin at the center of the SAN: the fabric. Because switches are located between the hosts and the storage devices and have visibility into both sides of the storage network, starting with them can help narrow the search. After eliminating the possibility of a fault within the fabric, see if the problem is on the storage side or the host side, and continue a more detailed diagnosis from there. Using this approach can quickly pinpoint and isolate problems. For example, if a host cannot detect a storage device, run the `switchshow` command to determine if the storage device is logically connected to the switch. If it is not, focus first on the switch that is directly connected to storage. Use your vendor-supplied storage diagnostic tools to better understand why the storage device is not visible to the switch. If the storage device can be detected by the switch, and the host still cannot detect the storage device, then there is still a problem between the host and the switch.

Supported Hardware and Software

The following hardware platforms are supported by Brocade Fabric OS v9.2.x.

Brocade Gen 7 (64G) Fixed-Port Switches

- Brocade G720 Switch
- Brocade G730 Switch
- Brocade 7850 Extension Switch

Brocade Gen 7 (64G) Directors

For ease of reference, Brocade chassis-based storage systems are standardizing on the term *director*. The legacy term *backbone* can be used interchangeably with the term *director*.

- Brocade X7-4 Director
- Brocade X7-8 Director

Brocade Gen 6 (32G) Fixed-Port Switches

- Brocade G610 Switch
- Brocade G620 Switch
- Brocade G630 Switch
- Brocade 7810 Extension Switch
- Brocade G648 Blade Server SAN I/O Module
- Brocade MXG610 Blade Server SAN I/O Module

Brocade Gen 6 (32G) Directors

- Brocade X6-4 Director
- Brocade X6-8 Director

Contacting Technical Support for Your Brocade® Product

If you purchased Brocade® product support from a Broadcom® OEM or solution provider, contact your OEM or solution provider for all your product support needs.

- OEM and solution providers are trained and certified by Broadcom to support Brocade products.
- Broadcom provides backline support for issues that cannot be resolved by the OEM or solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information on this option, contact Broadcom or your OEM.
- For questions regarding service levels and response times, contact your OEM or solution provider.

If you purchased Brocade product support directly from Broadcom, use one of the following methods to contact the Technical Assistance Center 24x7. For product support information and the latest information on contacting the Technical Assistance Center, go to www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

Online	Telephone
For nonurgent issues, the preferred method is to log on to the Support portal at support.broadcom.com. (You must initially register to gain access to the Support portal.) Once registered, log on and then select **Brocade Products**. You can now navigate to the following sites: • **Case Management** • **Software Downloads** • **Licensing** • **SAN Reports** • **Brocade Support Link** • **Training & Education**	For Severity 1 (critical) issues, call Brocade Fibre Channel Networking Global Support at one of the phone numbers listed at www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

Document Feedback

Quality is our first concern. We have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission or if you think that a topic needs further development, we want to hear from you. Send your feedback to documentation.pdl@broadcom.com. Provide the publication title; topic heading; publication number and page number (for PDF documents); URL (for HTML documents); and as much detail as possible.

Overview

Network Time Protocol

One of the most frustrating parts of troubleshooting is trying to synchronize a switch's message logs and port logs with those of other switches in the fabric. If you do not have Network Time Protocol (NTP) set up on your switches, trying to synchronize log files to track a problem is more difficult.

Most Common Problem Areas

Table identifies the most common problem areas that arise within SANs, and it identifies tools to use to resolve them.

Table 1: Common Troubleshooting Problems and Tools

Problem Area	Investigate	Tools
Fabric	• Missing devices • Marginal links (unstable connections) • Incorrect zoning configurations • Incorrect switch configurations	• Switch LEDs • Switch commands for diagnostics (for example, `switchshow` or `nsallshow`) • Web- or GUI-based monitoring and management software tools
Storage Devices	• Physical issues between the switch and devices • Incorrect storage software configurations	• Device LEDs • Storage diagnostic tools • Switch commands for diagnostics (for example, `switchshow` or `nsallshow`)
Hosts	• Physical issues between the switch and devices • Lower or incompatible HBA firmware • Incorrect device driver installation • Incorrect device driver configuration	• Device LEDs • Host operating system diagnostic tools • Device driver diagnostic tools • Switch commands for diagnostics (for example, `switchshow` or `nsallshow`) Also, make sure to use the latest HBA firmware recommended by the switch supplier or on the HBA supplier's website.
Storage Management Applications	• Incorrect installation and configuration of the storage devices that the software references For example, if using a volume-management application, check for: • Incorrect volume installation • Incorrect volume configuration	• Application-specific tools and resources

Questions for Common Symptoms

You first must determine what the problem is. Some symptoms are obvious, such as the switch rebooting without any user intervention; whereas other symptoms are more obscure, such as your storage having intermittent connectivity to a particular host. Whatever the symptom is, you must gather information from the devices that are directly involved with the symptom.

The following table lists common symptoms and possible areas to check. You may notice that an intermittent connectivity problem has many variables to research, such as the type of connection between the two devices, how the connection is behaving, and the port type involved.

Table 2: Common Symptoms

Symptom	Areas to Check	Chapter or Document
Blade is faulty.	Firmware or application download Hardware connections Power-on self test (POST)	General Troubleshooting Firmware Download Errors Virtual Fabrics
Blade is stuck in the "LOADING" state.	Firmware or application download	Firmware Download Errors
Configuration upload or download fails.	FTP or SCP server or USB availability	Configuration
Connectivity is intermittent.	Links Trunking Buffer credits FCIP tunnel	Connectivity ISL Trunking *Brocade Fabric OS Extension Configuration Guide*
E_Port does not come online.	Licensing Fabric parameters Zoning Hardware or link problems	Overview General Troubleshooting Connectivity Virtual Fabrics
EX_Port does not form.	Links	Connectivity Virtual Fabrics
Fabric merge fails.	Fabric segmentation	General Troubleshooting Connectivity Virtual Fabrics
Fabric segments.	Licensing Zoning Virtual Fabrics Fabric parameters Fabric merge failed	Overview General Troubleshooting Connectivity Virtual Fabrics
FCIP tunnel bounces.	FCIP tunnel, including the network between FCIP tunnel endpoints	*Brocade Fabric OS Extension User Guide*
FCIP tunnel does not come online.	FCIP tunnel, including the network between FCIP tunnel endpoints	*Brocade Fabric OS Extension User Guide*
FCIP tunnel does not form.	Licensing Fabric parameters	General Troubleshooting *Brocade Fabric OS Extension User Guide*
FCIP tunnel is sluggish.	FCIP tunnel, including the network between FCIP tunnel endpoints	*Brocade Fabric OS Extension User Guide*
FCR is slowing down.	FCR LSAN tags	General Troubleshooting
Feature is not working.	Licensing	General Troubleshooting
FICON switch does not talk to hosts.	FICON settings	*Brocade Fabric OS FICON User Guide*
Firmware download fails.	FTP or SCP server or USB availability Firmware version compatibility Unsupported features enabled Firmware versions on switch	Firmware Download Errors Virtual Fabrics
Host application times out.	FCR LSAN tags Marginal links	General Troubleshooting Connectivity
LEDs are flashing.	Links	Connectivity
LEDs are steady.	Links	Connectivity

Symptom	Areas to Check	Chapter or Document
License has issues.	Licensing	General Troubleshooting
Link is marginal.	Links	Connectivity
LSAN is slow or times out.	LSAN tagging	General Troubleshooting
No connectivity exists between the host and storage.	Cables SCSI timeout errors SCSI retry errors Zoning	Overview Connectivity ISL Trunking *Brocade Fabric OS Extension User Guide*
No connectivity exists between switches.	Licensing Fabric parameters Segmentation Virtual Fabrics Zoning (if applicable) Incompatible firmware versions	Overview General Troubleshooting Connectivity Virtual Fabrics
No light on LEDs.	Links	Connectivity
Performance problems.	Links FCR LSAN tags FCIP tunnels	General Troubleshooting Connectivity *Brocade Fabric OS Extension User Guide*
Port cannot be moved.	Virtual Fabrics	Virtual Fabrics
SCSI experiences retry errors.	Buffer credits FCIP tunnel bandwidth	*Brocade Fabric OS Extension User Guide*
SCSI experiences timeout errors.	Links HBA Buffer credits FCIP tunnel bandwidth	Connectivity ISL Trunking *Brocade Fabric OS Extension User Guide*
Switch constantly reboots.	Rolling reboot detection FIPS	Security
Switch is unable to join the fabric.	Security policies Zoning Fabric parameters Switch firmware Virtual Fabrics	Overview Connectivity Virtual Fabrics
Switch reboots during configuration upload or download.	Configuration file discrepancy	Configuration
Syslog messages are generated.	Hardware SNMP management station	General Troubleshooting Security
Trunk bounces.	Cables on the same port group SFPs Trunked ports	Security
Trunk does not form.	Licensing Cables on the same port group SFPs Trunked ports Zoning E_Port QoS configuration mismatch Virtual Fabrics (switch ports on either end being in different logical partitions)	Overview General Troubleshooting Connectivity ISL Trunking

Symptom	Areas to Check	Chapter or Document
User forgot password.	Password recovery	Security
User is unable to change switch settings.	RBAC settings Account settings	Security
Virtual Fabric does not form.	FIDs	Virtual Fabrics
Zone configuration mismatch exists.	Effective configuration	Zoning
Zone content mismatch exists.	Effective configuration	Zoning
Zone type mismatch exists.	Effective configuration	Zoning

Gathering Information for Your Switch Support Provider

To ensure the maximum availability of diagnostic-related information, consider the following important tips in advance of problems that might occur:

- Always use the `supportftp` command to set up parameters in support of automatic FTP, SFTP, or SCP transfers. It ensures that various dumps, FFDC files, and trace files are copied to the defined FTP site and are available for support teams when needed. In addition, you can use `supportftp -t` <time> to ping the remote FTP server in the background, adding an empty file to the server and verify its continued availability.
- Consider using syslog on all switches, especially director-class switches. The RASLogs are kept separately on each command processor (CP); syslog provides a means of supplying a chronological error log that can expedite diagnosis. The CPs can fail over during certain problem events, and having an integrated external log can be very helpful.
- If the installation permits, attaching a remote terminal server with logging enabled to the serial console ports of each CP of the director can provide additional advanced information to the support team. It is made available along with the `supportSave` files.

If you are troubleshooting a production system, you must gather data quickly. As soon as a problem is observed, perform the following tasks:

1. Enter the `supportSave` command to save RASLog, TRACE, supportshow, core file(s), FFDC data, and other support information from the switch, chassis, blades, and logical switches.
2. Gather console output and logs.

NOTE
To issue the `supportSave` command on the chassis, you must log in to the switch using an admin account that has chassis-access permissions. For more information about these commands and their operands, refer to the *Brocade Fabric OS Command Reference Manual*.

Setting Up Your Switch for FTP

You can use the `supportftp` command to automatically transfer trace dumps to a specified FTP site. It helps minimize trace dump overwrites on the local switch.

To enable automatic trace dump transfers to a specified FTP site, complete the following steps:

1. Connect to the switch, and log in using an account with admin permissions.
2. Enter `supportftp` to see the current FTP parameters.
3. Enter `supportftp -s` to both view and change FTP parameters interactively:

```
switch:admin> supportftp -s
Host IP Addr[xxxx::x:xxx:xxxx:xxxx]:10.20.30.40
User Name[admin]: admin
Password[********]:password
Remote Dir[support]:
```

```
Auto upload protocol[ftp]:scp
Port option for SCP/SFTP[2000]:
Auto file transfer parameters changed
```

You can use the `supportftp -e` command to enable automatic trace dump transfers to your FTP site. This helps minimize trace dump overwrites on the local switch. You can also use the `supportftp -t` command to periodically ping the FTP server and ensure that it is ready when needed for automatic transfers.

NOTE
See Automatic Trace Dump Transfers for more information on setting up automatic transfer of diagnostic files as part of the standard switch configuration.

Overview on supportSave Data Collection Process

The `supportSave` data collection process does not retain any significant sensitive data, which includes IP address, user ID, password, and end user or application data. The “end user or application data” is defined as data being transferred between a host application and a storage device in a FC network. Under a few conditions that are noted as exceptions in the following paragraphs, some sensitive data is collected. If this is concern, a customer can remove a specific file containing the sensitive data before sending out the `supportSave` data.

The `supportSave` command gathers data required for Brocade Technical Support to resolve customer support cases. The data collected by the `supportSave` process includes configuration settings for the switches, state information from the various subsystems within FOS (used for troubleshooting issues encountered with a switch), and various logs available from the switch (audit logs, RASLogs, event logs, and so on). This information is available for all users with administrator-level access to the switch.

If the following features or services are configured, user IDs, passwords, or shared secrets that are associated with these services are retained in the `*.RAS_POST.txt.gz` file of `supportSave` data:

- SNMPv1 community string
- SNMPv3 user name
- SNMPv3 auth/privacy shared secret
  - SNMPv3 secrets can be encrypted as follows:

```
snmpconfig --set snmpv3
SNMP Informs Enabled (true, t, false, f): [false]
SNMPV3 Password Encryption Enabled (true, t, false, f): [false] true
```

- TACACS+ shared secret (if the encryption option is not used with TACACS+ configuration)
- RADIUS server shared secret (if the encryption option is not used with RADIUS configuration)

The `*RAS_POST.txt.gz` file retains the IP address of FC switches in a fabric. If external servers that provide common TCP/IP network services, such as SSH, syslog, RADIUS, NTP, are configured, the server IP addresses are also retained.

The `supportSave` process may retain fragments of an FC frame in `framelog` . The FC frame captured in `framelog` do not contain a data payload. A small portion (36 bytes or less) of the data payload may be retained in `framelog` . This small portion (36 bytes or less) of the data or payload, which is up to 2112 bytes in length, will not be able to capture any significant or meaningful application data.

NOTE
It is not recommended to run the `supportSave` command when POST tests are running on the switch.

Using the supportSave Command

The `supportSave` command uses the default switch name to replace the chassis name regardless of whether the chassis name has been changed to a nonfactory setting. If Virtual Fabrics is enabled, the `supportSave` command uses the default switch name for each logical fabric.

1. Connect to the switch, and log in using an account with admin permissions.
2. Enter the appropriate `supportSave` command based on your needs:
   - If you are saving to an FTP or SCP server, enter the `supportSave` command with the following options.

     NOTE
     If the `supportSave` command is invoked without operands, it goes into interactive mode.

     - `-c`: This option uses the FTP parameters saved by the `supportftp` command. The operand is optional. If you omit the operand, specify the FTP parameters through command-line options or interactively. To display the current FTP parameters, run `supportftp` (on a dual-CP system, run `supportftp` on the active CP).

       NOTE
       The `-c` option works only if you used the `supportftp -s` command to set up the FTP server.
     - `-n`: This option runs the command without prompting for confirmation. If this operand is omitted, you are prompted for confirmation.
   - On platforms that support USB devices, you can use your Brocade USB device to save the support files. To use your USB device, enter the `supportSave` command with the following options:
     - `-U`: This option saves support data to an attached USB device. When you use this option, you must specify a target directory with the `-d` option.
     - `-d` *`remote_dir`*: This option specifies the remote directory to which the file is to be transferred. When you save to a USB device, you ensure that the remote directory is created in the `/support` directory of the USB device by default.

Refer to the *Brocade Fabric OS Command Reference Manual* for commands to mount and view the contents of the USB storage.

Changing the supportsave Timeout Value

While running the `supportsave` command, you may encounter a timeout. A timeout occurs if the system is in a busy state due to the CPU or is I/O bound due to a high level of port traffic or file access requests. A timeout can also occur on very large machine configurations or when the machine is under heavy usage. If a timeout occurs, an SS-1004 message (`SS-1004: One or more modules timed out during supportsave. Please retry supportsave with -t option to collect all logs.`) is sent to both the console and the RASLog to report the error. To avoid the timeout error, rerun the `supportsave` command with the `-t` option.

1. Connect to the switch and log in using an account with admin permissions.
2. Enter `supportsave -t` *`value`*, and specify a multiplier value from 1 through 5.

   The following example increases the `supportsave` timeout value to twice the default timeout setting.

```
device:admin> supportsave -t 2
```

Setting Up a Serial Console Port

Use the following procedure to connect to the Fabric OS using the serial port.

NOTE
If you connect the serial console port to a terminal server, ensure that flow control is disabled.

1. Connect the serial cable to the serial port on the switch and to an RS-232 serial port on the workstation.

   If the serial port on the workstation is an RJ-45 port, instead of RS-232, remove the adapter on the end of the serial cable and insert the exposed RJ-45 connector into the RJ-45 serial port on the workstation.

2. Open a terminal emulator application (such as HyperTerminal in a Windows environment or TERM, TIP, or Kermit in a UNIX environment), and configure the application as follows:
   - In a UNIX environment, enter the following string at the prompt:

     ```
     tip /dev/ttyb -9600
     ```

     You may use `ttya` at the prompt, if `ttyb` is already in use.

     ```
     tip /dev/ttya -9600
     ```

   - In a Windows environment, enter the following parameters.

Table 3: Parameters to Configure a Windows Terminal Emulator Application

Parameter	Value
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

Capturing Output from a Console

Some information (such as boot information) is output directly to the console only. To capture this information, you must connect directly to the switch through its management interface using either a serial cable or an RJ-45 connector that is specifically used for Ethernet connectivity to the management network.

1. Connect directly to the switch using a terminal utility.
2. Set the utility to capture output from the screen.

   Some utilities require this step to be performed before opening a session. Check with your utility vendor for instructions.

3. Log in to the switch using an account with admin permissions.
4. Enter the command or start the process whose console output you want to capture.

Capturing Command Output

1. Connect to the switch through a Telnet or SSH utility.
2. Log in using an account with admin permissions.
3. Set the Telnet or SSH utility to capture output from the screen.

   Some Telnet or SSH utilities require this step to be performed before opening a session. Check with your Telnet or SSH utility vendor for instructions.

4. Enter the command or start the process to capture the required data on the console.

Building a Case for Your Switch Support Provider

The questions listed in Gathering Basic Information should be printed and answered in their entirety and be ready to send to your switch support provider when you contact them. Having this information immediately available expedites the information-gathering process that is necessary to begin determining the problem and finding a solution.

Gathering Basic Information

1. What is the switch's current Fabric OS level?

   To determine the switch's Fabric OS level, enter the `firmwareshow` command and write down the information.

2. What is the switch model?

   To determine the switch model, enter the `switchshow` command and write down the value in the `Switch Type` field. Cross-reference this value with the chart located in the Switch Types and Blade IDs sections.

3. Is the switch operational? Yes or no.

4. Are one or more blades showing a "Faulty" state in the `slotshow` command output? Yes or no.

5. Impact assessment and urgency:

   - Is the switch down? Yes or no.
   - Is it a standalone switch? Yes or no.
   - Are VE, VEX, or EX ports connected to the chassis? Yes or no.
     Enter `switchshow` to determine the answer.
   - How large is the fabric?
     Enter `nsallshow` to determine the answer.
   - Do you have Virtual Fabrics enabled in the fabric? Yes or no.
     Enter `lscfg --show` to determine the answer.
   - Do you have In-band Management installed on the switch's Gigabit Ethernet ports? Yes or no.
     Enter the `portshow iproute ge x` to determine the answer.
   - Are you using NPIV? Yes or no.
     Use the `switchshow` command to determine the answer.
   - Are security policies turned on in the fabric? If so, what are they? Gather the output from the following commands:
     - `authutil --show`
     - `fddcfg --showall`
     - `seccryptocfg --show`
     - `ipfilter --show`
     - `secauthsecret --show`
     - `secpolicyshow`

6. Is the fabric redundant? If yes, what is the MPIO software? (List vendor and version.)
7. If you have a redundant fabric, did a failover occur? To verify this, you need to examine the RASLogs on both CPs and look for messages related to `hafailover` , for example, HAM-1004.
8. Is POST enabled on the switch? Use the `diagpost` command to verify if POST is enabled.
9. Which CP blade is active? (This is applicable only to chassis-based devices such as Brocade DCX 8510 Backbones and X6 Directors.) Use the `hashow` command in conjunction with the RASLogs to determine which is the active CP and which is the standby CP. They will reverse roles in a failover, and their logs are separate.

Gathering Detailed Problem Information

Obtain as much of the following information as possible before contacting the SAN technical support vendor.

Document the sequence of events by answering the following questions:

- When did the problem occur?
- Is this a new installation?
- How long has the problem been occurring?
- Are specific devices affected? If so, what are their World Wide Number (WWN) names?
- What happened before the problem?
- Is the problem reproducible? If so, what are the steps to reproduce the problem?
- What configuration was in place when the problem occurred?
- A description of the problem with the switch or the fault with the fabric.
- The last actions or changes made to the system environment:
  - Settings
  - `supportSave` output
- Host information:
  - OS version and patch level
  - HBA type
  - HBA firmware version
  - HBA driver version
  - Configuration settings
- Storage information:
  - Disk/tape type
  - Disk/tape firmware level
  - Controller type
  - Controller firmware level
  - Configuration settings
  - Storage software (EMC Control Center, Veritas SPC, and so on)
- If this is a X7 platform or X6 platform, are the CPs in sync? Yes or no.
  Enter `hashow` to determine the answer.
- List the last actions or changes made to the switch, the fabric, and the SAN or metaSAN, as well as when they occurred.
- In the Table below, list the environmental changes made to the network.

Table 4: Environmental Changes

Type of Change	Date when Change Occurred

Gathering Additional Information

The following features require you to gather additional information. This additional information is necessary in order for your switch support provider to effectively and efficiently troubleshoot your issue. Refer to the specified chapter or document for the commands used for the data you must capture:

- Configurations: see Connectivity
- Firmware downloading: see Firmware Download Errors
- Trunking: see ISL Trunking
- Zoning: see Zoning
- FCIP tunnels: see *Brocade Fabric OS Extension User Guide*
- FICON: see *Brocade Fabric OS FICON User Guide*
- `fruDump` for a quicker supportsave operation: see Brocade Fabric OS Command Reference Manual

General Troubleshooting

License Issues

Some features require licenses to work properly. To view a list of features and their associated licenses, refer to the *Brocade Fabric OS Software Licensing User Guide*, Licenses are created using a switch's license identifier so you cannot apply one license to different switches. Before calling your switch support provider, use the `license --show` command to verify that you have the correct licenses installed.

Table 5: Issues Related to Licenses

Symptom	Probable Cause and Recommended Action
A feature is not working.	Refer to the *Brocade Fabric OS Software Licensing Guide* to determine if the appropriate licenses are installed on the local switch and any connecting switches. To determine installed licenses, complete the following steps. 1. Connect to the switch and log in using an account with admin permissions. 2. Enter the `license --show` command. A list of the currently installed licenses on the switch is displayed.

Unknown. No licenses are installed.	In chassis-based systems, the license are stored on the CP blade based on the WWN. So, if you move a CP blade from one chassis to another chassis, and the new chassis already has license installed on it, the following occurs:
	1. Entering `license --show` displays the following:
	`license --show`
	`License Id : 10:00:aa:bb:cc:dd:ee:ff`
	`No licenses are installed in the system`
	2. If the CP blade is moved to a chassis as the standby CP, the active CP will sync over the active CP's license and the standby CP will work properly using the active CP's license.
	3. If the CP blade is moved to a chassis as the active CP, the license are shown as "unknown" and the CP does not work because the WWN of the new chassis will not match the license that exist on the active CP.
	To resolve this issue, do one of the following:
	– Generate new license on the active CP based on the WWN of the chassis where the active CP is located.
	– If you have a `configdb` file that was generated using the `configupload` command for this chassis before the new active CP was added, you can run the `configdownload` command against the `configdb` file, which has the license to restore the active CP. The `configdownload` command downloads the license to the new active CP.

Time Issues

The following table covers time-related issues.

Table 6: Issues Related to Time

Symptom	Probable Cause and Recommended Action
Time is not in sync.	Cause: NTP is not set up on the switches in your fabric. Solution: Set up NTP on your switches in all fabrics in your SAN and metaSAN. For more information on setting up NTP, refer to the *Brocade Fabric OS Administration Guide*.

Frame Dropping

When a frame is unable to reach its destination due to a timeout, it is discarded. You can use Frame Viewer to determine the flows that contained the dropped frames, which can help you determine which applications might be impacted. Using Frame Viewer, you can see exactly what time the frames were dropped. (The timestamps are accurate to within one second.)

You can view and filter up to 20 discarded frames per chip per second for 1200 seconds using a number of options with the `framelog` command.

Table 7: Issues Related to Frame Dropping

Symptom	Probable Cause and Recommended Action
Frames are being dropped.	Frames are timing out. Viewing frames: 1. Connect to the switch and log in using an account with admin permissions. 2. Enter `framelog --show` to determine which frames are being dropped and when.

Switch Message Logs

Switch message logs (RAS logs) contain information on events that happen on the switch or in the fabric. These logs are an effective tool in understanding what is happening in your fabric or on your switch. RAS logs are independent on director-class switches. Weekly review of the RAS logs is necessary to prevent minor problems from becoming larger or to catch problems at an early stage. There are two sets of logs. The `ipaddrshow` command provides the IP addresses of the CP0 and CP1 control processor blades and associated RAS logs.

The following common problems can occur with your system message log.

Table 8: Issues Related to Switch Message Logs (RAS Logs)

Symptom	Probable Cause and Recommended Action
Inaccurate information appears in the system message log.	In rare instances, events gathered by the Track Changes feature can report inaccurate information to the system message log. For example, a user enters a correct user name and password, but the login is rejected because the maximum number of users has been reached. However, when looking at the system message log, the login is reported as successful. If the maximum number of switch users is reached, the switch still performs correctly in that it rejects the login of additional users, even if they enter the correct user name and password. However, in this limited example, the Track Changes feature reports this event inaccurately to the system message log; it appears as though the login was successful. This scenario occurs only when the maximum number of users has been reached; otherwise, the login information displayed in the system message log reflects reality. Refer to the *Brocade Fabric OS Administration Guide* for information regarding enabling and disabling Track Changes (TC).
MQ errors appear in the switch log.	An MQ error is a message queue error. Identify an MQ error message by looking for the two letters MQ followed by a number in the error message: `2004/08/24-10:04:42, [MQ-1004], 218,, ERROR, ras007, mqRead, queue = raslog-test- string0123456-raslog, queue I D = 1, type = 2` MQ errors can result in devices dropping from the switch's Name Server or can prevent a switch from joining the fabric. MQ errors are rare and difficult to troubleshoot; resolve them by working with the switch supplier. When encountering an MQ error, issue the `supportsave` command to capture debug information about the switch; then, forward the `supportsave` data to the switch supplier for further investigation.
I2C bus errors appear in the switch log.	I2C bus errors generally indicate defective hardware or poorly seated devices or blades; the specific item is listed in the error message. Refer to the *Brocade Fabric OS Message Reference Manual* for information specific to the error that was received. Some Chip-Port (CPT) and Environmental Monitor (EM) messages contain I2C-related information. If the I2C message does not indicate the specific hardware that may be failing, begin debugging the hardware, as this is the most likely cause of the errors.

Core file or FFDC warning messages appear on the serial console or in the system log.	Issue the `supportsave` command. The messages can be dismissed by entering `supportsave -R` after all data is confirmed to be collected properly.
	Error example:
	`*** CORE FILES WARNING (10/22/08 - 05:00:01 ) ***`
	`3416 KBytes in 1 file(s)`
	`use "supportsave" command to upload`

Switch Disable Logs

Switch disable logs (RAS logs) contain information on the switch that gets disabled or persistently disabled with a reason field describing the cause of disability. This allows you to capture the reason for the faulty scenario and the corrective actions that needs to be taken. Below are the RAS logs entries that indicates the reasons for switch or blade fault scenarios.

The following are the RAS log entries and its reason for being disabled,

Table 9: Reason for Switch Disable Logs (RAS Logs)

RAS Log	Reason for Disability
EM-1034	FRU set to faulty
EM-1003	<FRU ID> has unknown hardware identifier: FRU faulted.

RAS Log	Reason for Disability
EM-1033	CP in <FRU Id> set to faulty because CP ERROR asserted.
HIL-1107	Switch faulted, <nominal voltage> (<measured voltage>) above threshold. System preparing for reset.
HIL-1108	Switch faulted, <nominal voltage> (<measured voltage>) below threshold. System preparing for reset.
EM-1057	Blade:<Slot Id> is getting reset:<Fault reason>.
BL-1002	Init Failed: slot <slot number> DISABLED because internal ports were not ONLINE, <list of internal port number not ONLINE>.
EM-1058	Switch gets reset:<Fault reason>.
EM-1062	Blade in slot <Slot Id> faulted as it exceeds the maximum support limit of <Limit> blades with Blade ID <Blade Type Id> in the chassis.
EM-1063	Blade in slot <Slot Id> faulted because it exceeds the maximum support limit of <Limit> blades with Blade IDs <Applicable blade Type IDs> in the chassis.
BL-1022	Init Failed: Switch DISABLED because internal ports were not ONLINE, <list of internal port number not ONLINE>.
EM-1005	<FRU Id> has faulted. Sensor(s) above maximum limits.
EM-1066	SAS Virtualization Services are now available <Slot number or blank for single board systems>.
EM-1008	Unit in <Slot number or Switch> with ID <FRU Id> is faulted, it is incompatible with the <type of incompatibility> configuration, check FOS firmware version as a possible cause.
EM-1012	<FRU Id> failed <state> state transition, unit faulted.
EM-1064	Blade:<Slot Id> is being powered off (based on user configuration) upon receiving a HW ASIC ERROR, reason:<Fault reason>.
BM-1009	Firmwaredownload timed-out for application processor. Faulting switch
EM-1071	Unit in <Slot number> with ID <FRU Id> is faulted, it is incompatible with the following blade id(s): <blade incompatibility list>.
EM-1072	Chassis cannot become ready since no Core Blades are available.
EM-1074	The ASIC in <FRU ID> is overheating: Shutting down.
BM-1055	Firmwaredownload timed-out for AP. Faulting switch.
EM-1100	Unit in <Slot number or Switch> with ID <FRU Id> is faulted(<Fault>). <Current attempt number> of <Total number of attempts> total attempt(s) at auto-recovery is being made. Delay is <Delay time in seconds> seconds.
EM-1101	Unit in <Slot number or Switch> with ID <FRU Id> is faulted(<Fault>). <Current attempt number> attempt(s) at auto-recovery were made without success.
EM-1134	<FRU Id> set to faulty, rc=<return code>.
EM-1227	Slot <FRU slot number> is being powered off as it was detected as faulty during previous INIT.
EM-2003	<Slot Id or Switch> has failed the POST tests. FRU is being faulted.
HAM-1001	Standby CP is not healthy, device <device name> status BAD, Severity = <severity level>.
HIL-1101	Slot <slot number> faulted, <nominal voltage> (<measured voltage>) is above threshold.
HIL-1102	Slot <slot number> faulted, <nominal voltage> (<measured voltage>) is below threshold.
HIL-1502	Slot <slot number>, high temperature (<measured temperature>). Unit will be shut down in 2 minutes if temperature remains high.
HIL-1503	Slot <slot number>, unit shutting down.
HIL-1506	High temperature (<measured temperature> C) exceeds system temperature limit. System will shut down within 2 minutes.

RAS Log	Reason for Disability
HIL-1507	High temperature warning time expired. System preparing for shutdown.
HIL-1508	Fan faulty warning time expired. System preparing for shutdown.
HIL-1509	High temperature (<measured temperature> C). Warning time expired. System preparing for shutdown.
HIL-1514	Blade in slot <slot number> is shutting down.
HIL-1515	High temperature (<measured temperature> C) exceeds system temperature limit. System will shut down soon.
HIL-1518	<number of failed and/or absent fans> failed and/or absent fan(s) exceeds system threshold. System will shut down within 2 minutes.
HIL-1603	<failure count> fans out of service. System is shutting down immediately.
HIL-1611	MISMATCH in PSU-FAN Air Flow direction. Replace PSU with fan air flows in same direction. System will be shut down in 2 minutes.
HIL-1612	MISMATCH in PSU-FAN Air Flow direction. System shut down.
PLAT-1000	<Function name> <Error string>.
PLAT-1072	The chassis is disabled because no Core Blades are available. Insert/replace one or both Core Blades and run chassisenable.
RTE-1004	Faulting blade <Slot number> due to missing routes. Use slotpoweroff and slotpoweron to recover the blade.
SWCH-1008	<area string> are port swapped on ports that do not support port swap. Slot <slot number> will be faulted.

Switch Boot

The following table covers device booting issues.

Table 10: Issues Related to Device Booting

Symptom	Probable Cause and Recommended Action
Enterprise-class platform reboots after initial bootup.	This issue can occur during an enterprise-class platform bootup with two CPs. If any failure occurs on the active CP before the standby CP is fully functional and has obtained HA sync, the standby CP may not be able to take on the active role to perform failover successfully. In this case, both CPs reboot to recover from the failure.

Rolling Reboot Detection

A rolling reboot occurs when a switch or enterprise-class platform has continuously experienced unexpected reboots of one or both control processor blades (CPs). This behavior continues until the system detects the rolling reboot. Once the Rolling Reboot Detection (RRD) occurs, the switch is put into a stable state so that only minimal `supportsave` output need be collected and sent to your service support provider for analysis. Not every type of reboot reason activates the Rolling Reboot Detection feature. For example, issuing the `reboot` command multiple times in itself does not trigger rolling reboot detection, but quickly power-cycling the chassis repeatedly will trigger the RRD process. After five events within the RRD window, the RRD process will first attempt to disable the switch persistently. If a subsequent reboot still occurs, the RRD process will then disable Fabric OS in order to allow improved diagnostic access.

The following message is displayed when the RRD feature is activated and the switch is persistently disabled.

```
************************************************************
* Fabric OS has detected frequent switch reboot condition.   *
* The switch has been disabled as a preventive action. If    *
```

```
 * the switch reboots again Rolling Reboot Detection will     *
 * halt the switch from loading Fabric OS.                    *
 *                                                            *
 *                                                            *
 * Please use 'switchcfgpersistentenable' to enable the       *
 * switch, once the problem is resolved.                      *
 ************************************************************
```

ATTENTION
If a rolling reboot is caused by a Linux kernel panic, the RRD feature is not activated.

Reboot Classification

There are two types of reboots that occur on a switch and enterprise-class platform: expected and unexpected. Expected reboots occur when the reboots are initialized by commands; these types of reboots are ignored by the Rolling Reboot Detection (RRD) feature. They include the following commands:

- `reboot`
- `hafailover`
- `fastboot`
- `firmwaredownload`

The RRD feature is activated and halts rebooting when an unexpected reboot reason is shown continuously in the reboot history within a certain period of time. For example, the switch reboots five times in 300 seconds. The period of time depends on the switch, but typically the period is 10 minutes. The following reboots are considered unexpected reboots:

- Reset
  A reset reboot may be caused by one of the following:
  – Power-cycling the switch or CP
  – Linux `reboot` command
  – Hardware watchdog timeout
  – Heartbeat-loss-related reboot
- Software fault: kernel panic
  – If the system detects an internal fatal error from which it cannot safely recover, it outputs an error message to the console, dumps a stack trace for debugging, and then performs an automatic reboot.
  – After a kernel panic, the system may not have enough time to write the reboot reason, causing the reboot reason to be empty. This is treated as a reset case.
- Software fault
  – Software watchdog
  – ASSERT
- Software recovery failure
  This is an HA bootup-related issue and happens when a switch is unable to recover to a stable state. The HASM log contains more details and specific information on this type of failure, such as one of the following:
  – Failover recovery failed: Occurs when failover recovery fails and the CP must reboot.
  – Failover when standby CP unready: Occurs when the active CP must fail over, but the standby CP is not ready to take over mastership.
  – Failover when LS trans incomplete: Occurs when a logical switch transaction is incomplete.
- Software bootup failure
  – System bring up timed out: The CP failed to come up within the time allotted.
  – LS configuration timed out and failed: The logical switch configuration failed and timed out.

After RRD is activated, admin-level permission is required to log in. Enter the `supportshow` or `supportsave` command to collect a limited amount of data to resolve the issue.

Restrictions

The following restrictions apply to the RRD feature:

- RRD works only on CFOS-based systems and is not available on AP blades.
- RRD works only during the 30 minutes immediately after the switch boots. If the switch does not reboot for 30 minutes, RRD is deactivated.

Collecting Limited supportSave Output about the Rolling Reboot Detection

1. Log in to the switch using an admin account.

   A user account with admin privileges can collect limited `supportSave` output only.

2. After you see the message in the following example, press **Enter**.
3. Enter the `supportSave` command to go into interactive mode. Or, if you are using a USB device, enter `usbstorage -e` .
4. Respond to the prompts.
5. Once the `supportSave` command had completed, contact your service support provider to provide them with the data.

   The following message is an example of the output.

```
Fabric OS Version 9.1.0
switch login: admin
Password: <hidden text>
************************************************************
*                                                          *
* Fabric OS has detected frequent switch reboot condition.   *
* Following actions can be taken to recover the switch:      *
* - take off or replace the bad blades.                      *
* - use supportSave to collect supportSave data.             *
*                                                          *
*                                                          *
************************************************************
Please change passwords for switch default accounts now.
Use Control-C to exit or press 'Enter' key to proceed.
```

FC-FC Routing Connectivity

This section describes tools that you can use to troubleshoot Fibre Channel routing connectivity and performance.

Generating and Routing an ECHO

The FC-FC Routing Service enables you to route the ECHO generated when an `fcping` command is issued on a switch, providing `fcping` capability between two devices in different fabrics across the FC router.

The `fcping` command sends a Fibre Channel ELS ECHO request to a pair of ports. It performs a zone check between the source and the destination. In addition, two Fibre Channel Extended Link Service (ELS) requests are generated. The first ELS request is from the domain controller to the source port identifier. The second ELS request is from the domain

controller to the destination port identifiers. The ELS ECHO request elicits an ELS ECHO response from a port identifier in the fabric, and it validates link connectivity.

Use the `fcping` command to validate link connectivity to a single device or between a pair of devices.

ATTENTION
There are some devices that do not support the ELS ECHO request. In these cases, the device either does not respond to the request or sends an ELS reject. When a device does not respond to the ELS request, further debugging is required; however, do not assume that the device is not connected.

On the edge Fabric OS switch, make sure that the source and destination devices are properly configured in the LSAN zone before entering the `fcping` command. This command performs the following functions:

- Checks the zoning configuration for the two ports specified.
- Generates an ELS ECHO request to the specified source port and validates the response.
- Generates an ELS ECHO request to the specified destination port and validates the response.

```
device:admin> fcping 0x020800 22:00:00:04:cf:75:63:85
        Source:         0x020800
        Destination:    22:00:00:04:cf:75:63:85
        Zone Check:     Zoned
Pinging 0x020800 with 12 bytes of data:
        received reply from 0x020800: 12 bytes time:1159 usec
        received reply from 0x020800: 12 bytes time:1006 usec
        received reply from 0x020800: 12 bytes time:1008 usec
        received reply from 0x020800: 12 bytes time:1038 usec
        received reply from 0x020800: 12 bytes time:1010 usec
        5 frames sent, 5 frames received, 0 frames rejected,0 frames timeout
        Round-trip min/avg/max = 1006/1044/1159 usec
```

Regardless of the device's zoning configuration, the `fcping` command sends the ELS frame to the destination port. A destination device can take any one of the following actions:

- Send an ELS Accept to the ELS request.
- Send an ELS Reject to the ELS request.
- Ignore the ELS request.

For details about the `fcping` command, refer to the *Brocade Fabric OS Command Reference Manual*.

Example of one device that accepts the request and another device that rejects the request:

```
device:admin> fcping 10:00:00:00:c9:29:0e:c4 21:00:00:20:37:25:ad:05
Source: 10:00:00:00:c9:29:0e:c4
Destination: 21:00:00:20:37:25:ad:05
Zone Check: Not Zoned
Pinging 10:00:00:00:c9:29:0e:c4 [0x20800] with 12 bytes of data:
received reply from 10:00:00:00:c9:29:0e:c4: 12 bytes time:1162 usec
received reply from 10:00:00:00:c9:29:0e:c4: 12 bytes time:1013 usec
received reply from 10:00:00:00:c9:29:0e:c4: 12 bytes time:1442 usec
received reply from 10:00:00:00:c9:29:0e:c4: 12 bytes time:1052 usec
received reply from 10:00:00:00:c9:29:0e:c4: 12 bytes time:1012 usec
5 frames sent, 5 frames received, 0 frames rejected, 0 frames timeout
Round-trip min/avg/max = 1012/1136/1442 usec
Pinging 21:00:00:20:37:25:ad:05 [0x211e8] with 12 bytes of data:
Request rejected by 21:00:00:20:37:25:ad:05: Command not supported: time: 1159 usec
Request rejected by 21:00:00:20:37:25:ad:05: Command not supported: time: 1006 usec
Request rejected by 21:00:00:20:37:25:ad:05: Command not supported: time: 1008 usec
```

```
Request rejected by 21:00:00:20:37:25:ad:05: Command not supported: time: 1038 usec
Request rejected by 21:00:00:20:37:25:ad:05: Command not supported: time: 1010 usec
5 frames sent, 0 frames received, 5 frames rejected, 0 frames timeout
Round-trip min/avg/max = 0/0/0 usec
```

Example using `fcping` with a single destination (in this example, the destination is a device node WWN):

```
device:admin> fcping 20:00:00:00:c9:3f:7c:b8
Destination: 20:00:00:00:c9:3f:7c:b8
Pinging 20:00:00:00:c9:3f:7c:b8 [0x370501] with 12 bytes of data:
received reply from 20:00:00:00:c9:3f:7c:b8: 12 bytes time:825 usec
received reply from 20:00:00:00:c9:3f:7c:b8: 12 bytes time:713 usec
received reply from 20:00:00:00:c9:3f:7c:b8: 12 bytes time:714 usec
received reply from 20:00:00:00:c9:3f:7c:b8: 12 bytes time:741 usec
received reply from 20:00:00:00:c9:3f:7c:b8: 12 bytes time:880 usec
5 frames sent, 5 frames received, 0 frames rejected, 0 frames timeout
Round-trip min/avg/max = 713/774/880 usec
```

Superping

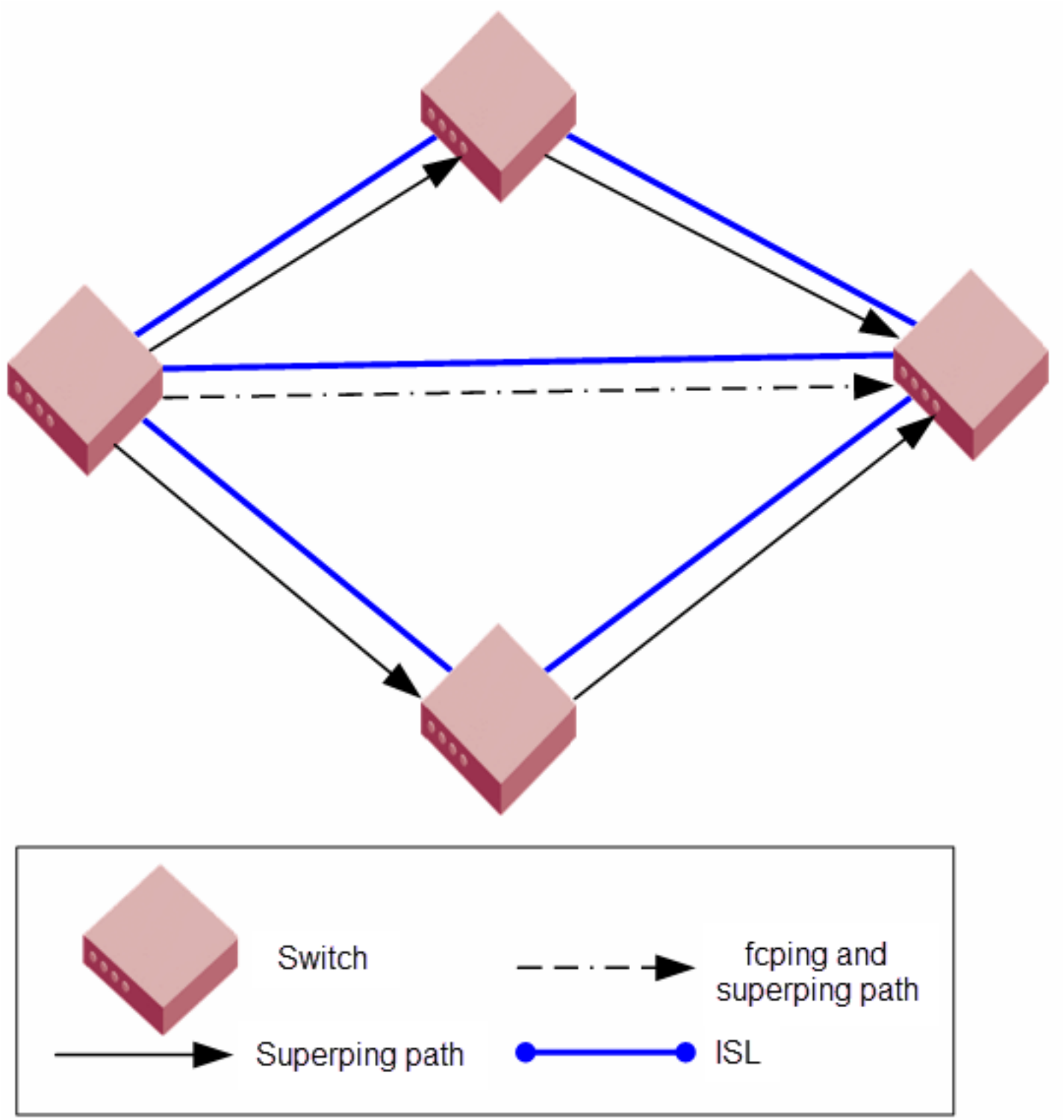
Superping refers to the `fcping --allpaths` command, which is a diagnostic tool used to test all least-cost ISLs between a source and destination switch. When you run the command, you are provided with a list of all available least-cost paths from a source domain to a destination device. Superping isolates links with potential failures so that you can investigate these ISLs to determine the exact links.

Superping works by sending ECHO frames to a destination device and outputting the status of each ISL that it traverses whether or not the response from the destination device is received. Each ECHO frame can choose any path from multiple available paths in the fabric to reach the destination device. This utility allows you to do the following:

- Run a sanity test that exercises all ISLs and internal links in different paths that route to the destination device.
- Determine the least-cost path to aid in designing fabric redundancy.
- Determine the specific ISLs and internal links with failures.
- Exercise all ISL links in the base fabric for a logical fabric configuration.

The number of actual paths covered when using the superping feature depends on two other parameters that you can specify optionally. When you enter `fcping --allpaths` without any other options, superping covers all ISLs in the routes between source and destination, as shown in Figure.

Figure 1: Superping and fcping Paths



In the following example, superping is invoked using the `fcping --allpaths` command to destination domain 165. The following example displays each hop in "Domain1/Index1 -> Domain2/Index2" format. To reach destination domain 165 from source domain 3, there are two unique end-to-end paths. In the first path, the frame traverses from egress port index

205 in source domain 3 to ingress port index 25 in domain 207. in domain 207, the frame traverses from egress port index 42 to ingress port index 3 in domain 101. In domain 101, the frame goes from egress port index 16 to ingress port index 99 in domain 165.

```
device:admin> fcping --allpaths 165
Pinging(size:12 bytes) destination domain 165 through all paths
PATH SWITCH1-->           SWITCH2-->           SWITCH3            SWITCH4              STATUS
-------------------------------------------------------------------------------------------
1.   (3/EMB, 3/205)[128] (207/25,207/42)[128] (101/3,101/16)[128] (165/99,165/0)[128]  SUCCESS
2.   (3/EMB, 3/204)[128] (207/27,207/42)[128] (101/3,101/16)[128] (165/99,165/0)[128]  SUCCESS
```

Superping can isolate links with failures so that you can further investigate these ISLs to determine the exact links with errors.

NOTE
Superping provides an indication of whether all ISLs are covered. If all ISLs are not covered, you can increase the coverage count and maximum retries to transmit, so that complete coverage of all ISLs is achieved.

Consider the following example in which a few errors are recorded on ISLs 3/205 to 2/25, 3/204 to 2/27, 2/42 to 101/3, and 2/1 to 101/8. The potential faulty link is internal port 0/284 in domain 2 with a maximum of 100 percent failure.

```
ISL COVERAGE
-------------
SNO             ISL                     STATUS
-----------------------------------------------------------------------------
 1      3/123[128]--> 165/96[128]       SUCCESS(5/5)
 2      3/205[128]--> 2/25[128]         FAILURE(7/50)
 3      3/204[128--> 2/27[128]          FAILURE(11/50)
 4      165/99[128]--> 101/16[128]      SUCCESS(5/5)
 6      2/42[128]--> 101/3[128]         FAILURE(10/67)
 7      2/1[128]--> 101/8[128]          FAILURE(8/33)

INTERNAL PORT COVERAGE
-----------------------
SNO     DOMAIN  INTRNL_PORT     STATUS
-----------------------------------------------------------------------------
 1        2[128]  0/272         SUCCESS(40/40)
 2        2[128]  0/276         SUCCESS(44/44)
 3        2[128]  0/280         SUCCESS(30/30)
 4        2[128]  0/284         FAILURE(20/20) <== 100% failure
```

When an ECHO frame is dropped, all ISLs in the path are marked as failed. It is not possible to determine the exact ISL link that dropped the frame. Consequently, all ISLs in the path record some failures. The ISL with the actual error has the maximum percentage of failures, since this ISL, when selected in any possible path, causes the ECHO frame to be dropped and accumulates a higher failure percentage.

Restrictions

- You are not allowed to reconfiguration the Fabric while using the Superping feature. It is assumed that the fabric is stable before the `fcping --allpaths` command is issued.
- The control path for interswitch communication should be available, even if the data path for device-to-device communication may have resource starvation.
- When issued in a fabric with trunk ports, only the trunk master index is output to the user (for example, individual coverage statistics for each trunk member are not available).
- Superping requires that the Fibre Channel ECHO ELS frame be supported by end devices.
- This feature is not supported in interopMode 2 or 3.
- In frame redirection configurations, where there is a physical host, physical target, virtual initiator, and virtual target, superping identifies only the path from the physical host to the physical target regardless of whether the data path consists of the path from the physical target to the virtual target through the virtual initiator.

NOTE
The `fcping --allpaths` command to a domain can take a long time to complete.

Routing and Statistical Information

The `pathinfo` command displays routing and statistical information from a source port index on the local switch to a destination port index on another switch. This routing information describes the full path that a data stream travels between these ports, including all intermediate switches.

ATTENTION
Using the `pathinfo` command when exchange-based routing is turned on can provide different paths with each attempt.

The routing and statistics information is provided by every switch along the path, based on the current routing-table information and statistics calculated continuously in real time. Each switch represents one hop.

When using the `pathinfo` command across fabrics connected through an FC router, the command represents backbone information as a single hop. The command captures details about the FC router to which ingress and egress EX_Ports are connected, but it hides the details about the path that the frame traverses from the ingress EX_Ports to the egress EX_Ports in the backbone.

To use `pathinfo` across remote fabrics, you must specify both the fabric ID (FID) and the domain ID of the remote switch. Optionally, you can specify the source port ID (PID) and destination PID. You cannot use the `pathinfo` command to obtain source port information across remote FCR fabrics. When obtaining path information across remote fabrics, the destination switch must be identified by its domain ID. Identifying the switch by name or WWN is not accepted.

To display basic path information to a specific domain in command line mode:

```
device:admin> pathinfo 5
Hop  In Port  Domain ID (Name)                          Out Port    BW   Cost
------------------------------------------------------------------------------
0       2          1 (sw0)                                6       4G    500
1      23          2 (sw0)                                8       4G    500
2       4          3 (sw0)                                3       4G    500
3      12          4 (sw0)                               18       4G  10000
4       4          7 (switch_3)                           0       4G    500
5      26          5 (switch_3)                           E       -     -
```

To display basic and extended statistics in interactive mode:

```
device:admin> pathinfo
Max hops: (1..127) [25]
```

```
Fabric Id: (1..128) [-1]
Domain|Wwn|Name: [] 8
Source port: (0..15) [-1]
Destination port: (0..255) [-1]
Source pid: (0x0..0xefff00) [ffffffff] 0x061600
Destination pid: (0x0..0xefff00) [0] 0x01f001
Basic stats (yes, y, no, n): [no] y
Extended stats (yes, y, no, n): [no] y
Trace reverse path (yes, y, no, n): [no]
Source route (yes, y, no, n): [no]
Timeout: (1000..30000) [10000]
Target port is Embedded
Hop  In Port  Domain ID (Name)                          Out Port    BW   Cost
------------------------------------------------------------------------------
0       2         1 (sw0)                                  6       4G    500
1      23         2 (sw0)                                  8       4G    500
2       4         3 (sw0)                                  3       4G    500
3       2         4 (sw0)                                 24       4G  10000
4       3         7 (switch_3)                             2       4G    500
5      27         5 (switch_3)                            24       -     -
 Reverse path
6      24         5 (switch_3)                            27       4G    500
7       2         7 (switch_3)                             3       4G    500
8      24         4 (sw0)                                  2       4G    500
9       3         3 (sw0)                                  4       4G  10000
10      8         2 (sw0)                                 23       4G    500
11      6         1 (sw0)                                  2        -    -
(output truncated)
```

For more information on the `pathinfo` command, refer to the *Brocade Fabric OS Command Reference Manual*.

Performance Issues

The following table covers performance issues.

Table 11: Issues Related to Performance

Symptom	Probable Cause and Recommended Action
General in FCR performance and scalability slow down.	Issue: As LSAN zone databases get bigger, it takes more switch resources to process them. Solution: Use the enforce tag feature to prevent a backbone switch from accepting unwanted LSAN zone databases into its local database.
Host application times out.	Issue: FCR tends to take a long time (more than 5 seconds) to present and set up paths for the proxy devices. Certain hosts can do discovery much faster, and, as a result, they end up timing out. Solution: Use the speed tag feature to always present the target proxy to the host. This helps sensitive hosts to do a quick discovery without timing out or causing an application failure.

FCR Migration

This section describes the steps to troubleshoot issues after enabling migration mode.

When an FCR switch is enabled for migration mode, the traffic that is destined toward remote fabrics is migrated on alternative IFLs in the edge fabric going to the other FCR switches in the backbone fabric. The migration mode allows

you to proceed with decommission actions leading to the removal of the FCR switch from the backbone fabric. Once the traffic migration is completed, you must decommission the older FCR switch. For more information on migration mode and switch decommissioning, refer to the *Brocade Fabric OS Administration Guide*.

NOTE
The migration mode is supported only in edge-to-edge topologies.

Verification of FCR Migration Mode Success

1. Verify if migration mode is enabled by using the `fcrconfigure --show` command.
2. After migration mode is checked, verify the `portperfshow` command output on all EX_Ports and ensure that there is no traffic flowing through any of the EX_Ports.
3. Verify the `lsdbshow` output in the edge fabric switch, and verify that the link cost (`linkcost`) between a front domain and a translate domain has changed from 10,000 to 10,001.

Common Issues

1. Traffic flows through EX_Ports on an FCR switch enabled with migration mode (`Portperfshow` shows traffic on EX_Ports).
2. The `fcrconfigure --enable -migrationmode` command fails.

- **Traffic Flows through EX_Ports on an FCR Switch Enabled with Migration Mode (Portperfshow Shows Traffic on EX_Ports)**
  In a migration-mode-enabled switch, if the user still sees traffic on EX_Ports, do the following:
  – Verify if all switches in the backbone fabric have FOS 9.1.0 or a later version. If not, consider doing the following:
    • Disable migration mode.
    • Upgrade all switches to FOS 9.1.0 in the backbone fabric.
    • Enable migration mode again.
  – Check to see that there is no backbone-to-edge-fabric device sharing using the `fcrproxydevshow` command.
    • Migration mode is not supported in a backbone-to-edge-fabric topology; rather it is expected to have some distribution for backbone-to-edge device sharing.
  – Ensure that there are no new EX_Port or E_Port connections or topology changes after migration mode is enabled.
    • If a user added EX_Ports or E_Ports after migration mode is enabled, traffic or I/O errors may occur. Consider the following troubleshooting steps:
      • Disable and enable migration mode again to recover from this state.
      • Do not add EX_Ports or E_Ports after migration mode is enabled.
  – Verify if any alternative paths are available from different FCR switches for the EX_Ports (in migration-mode-enabled FCR) using the `fcrrouteshow` command output.
    • Have a one-to-one duplicate EX_Port connection for a seamless migration. Migration mode works if it has an alternative path for each edge fabric that is connected to the migration-enabled FCR switch. For better performance, have an one-to-one alternative connection in the newly added FCR switch going to the edge fabric switch. If there is no alternative path, consider the following steps:
      • Disable migration mode.
      • Add the alternative IFL connection to enable migration mode again.
      • Enable migration mode on the FCR switch.
  – Verify if `lsdbshow` output for a front domain to a translate domain reports a new cost of 10,001. If the output still shows the link cost as 10,000, there is a possibility of a `linkstate` record update failure. Consider the following troubleshooting steps:
    • Disable migration mode and enable it again.
    • Collect a supportSave and contact support.
- **fcrconfigure --enable -migrationmode Command Failure**
  This command returns an error in the following scenarios:

  - When you try to enable a non-VF FCR switch on backbone-to-edge device sharing.
    - Remove the backbone-to-edge device sharing for the command to succeed.
  - If you try to apply the same configuration.

Blade Troubleshooting Tips

This section refers to the following specific types of blades inserted into the Brocade X6 and X7 directors:

- FC blades or port blades contain only Fibre Channel ports: Brocade FC32-48, FC 32-64, FC64-48, FC32-G7-48 and FC64-64.
- AP blades such as the SX6 contain extra processors, some with specialized ports, and have the Fabric OS firmware downloaded to them automatically in the chassis.
- CP blades have a control processor (CP) used to control the entire switch; they can be inserted only into slots 1 and 2 on both the Brocade Gen 6 and Gen 7 directors.
- CR32-8 and CR32-4 core blades provide ICL functionality between two Brocade X6 directors. CR32-8 blades can be inserted only into slots 7 and 8 on the Brocade X6-8.

  NOTE

  The blades are physically interchangeable between chassis but will fault if not supported in that chassis.

  CR32-4 blades can be inserted only into slots 5 and 6 on the Brocade X6-4.
- CR64-8 and CR64-4 core blades provide ICL functionality between two Brocade X7 directors. CR64-8 blades can be inserted only into slots 7 and 8 on the Brocade X7-8. CR64-4 blades can be inserted only into slots 5 and 6 on the Brocade X7-4.

Blade Fault Autorecovery

If a blade is faulty, it should attempt an autorecovery once. The autorecovery is triggered for the specified slot faults provided that the autorecovery feature is enabled, only one attempt is made for autorecovery, and if it does not happen successfully, you have to recover the blade by other alternative ways or contact support if needed. Autorecovery is disabled by default. Enable the autorecovery feature using the `configurechassis` command.

```
device:admin> configurechassis
        Configure...
          cfgload attributes (yes, y, no, n): [no]
          Custom attributes (yes, y, no, n): [no]
          system attributes (yes, y, no, n): [no] y
          system.blade.bladeFaultOnHwErrMsk: (0x0..0x7fffffff) [0x0]
          system.cpuLoad: (10..121) [121]
          system.i2cTurboCnfg: (0..2) [1]
          system.Enable.bladeAutoRecovery (yes, y, no, n): [yes] no
          fos attributes (yes, y, no, n): [no]
```

The following table covers blade-related issues.

Table 12: Issues Related to Blades

Symptom	Probable Cause and Recommended Action
The blade is faulty. (Use the `slotshow` command to confirm.)	If the port or application blade is faulty, enter the `slotpoweroff` and `slotpoweron` commands for the port or application blade. If the port or application blade still appears to be faulty, remove it and re-insert it into the chassis.
The AP blade is stuck in the "LOADING" state. (Use the `slotshow` command to confirm.)	If the blade remains in the loading state for a significant period of time, the firmware download times out. Remove the blade and re-insert it. When it boots, autoleveling is triggered and the firmware download is attempted again.

Connectivity

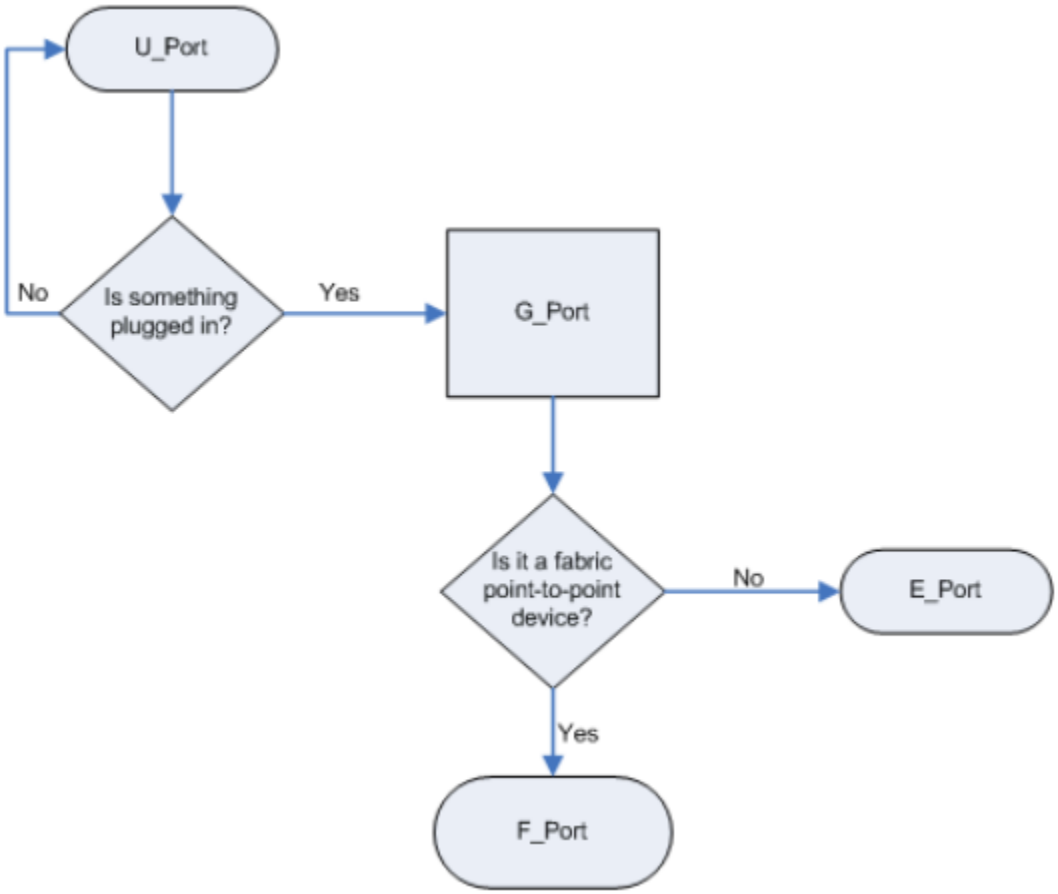
Port Initialization and FCP Auto-Discovery Process

The steps in the port initialization process represent a protocol used to discover the type of connected device and establish the port type and port speed. The possible port types are as follows:

- U_Port—Universal FC port. The base Fibre Channel port type. All unidentified or uninitiated ports are listed as U_Ports.
- L_Port/FL_Port—Fabric loop port. Connects public loop devices.
- G_Port—Generic port. Acts as a transition port for nonloop fabric-capable devices.
- E_Port—Expansion port. Assigned to ISL links.
- F_Port—Fabric port. Assigned to fabric-capable devices.
- EX_Port—A type of E_Port. It connects a Fibre Channel router to an edge fabric. From the point of view of a switch in an edge fabric, an EX_Port appears as a normal E_Port. It follows applicable Fibre Channel standards like other E_Ports. However, the router terminates EX_Ports rather than allowing different fabrics to merge as would happen on a switch with regular E_Ports.
- M_Port— Mirror port. A mirror port allows you to configure a switch port to connect to a port to mirror specific source port and destination port traffic passing through any switch port. A M_Port is supported between F_Ports only.
- VE_Port—Virtual E_Port. A Gigabit Ethernet switch port that is configured for an FCIP tunnel is called a VE_Port (virtual E_Port). However, with a VEX_Port at the other end, it does not propagate fabric services or routing topology information from one edge fabric to another.

Figure shows the process behind port initialization. Understanding this process can help you determine where a problem resides. For example, if your switch cannot form an E_Port, you understand that the process never got to that point or does not recognize the switch as an E_Port. Possible solutions would be to look at licensing and port configuration. Verify that the correct licensing is installed and that the port is not configured as a loop port, a G_Port, or the port speed is not set.

Figure 2: Simple Port Initialization Process



The FCP auto-discovery process enables private storage devices that accept a process login (PRLI) to communicate in a fabric.

If device probing is enabled, the embedded port commences with a port login (PLOGI) and attempts a PRLI into the device to retrieve information to enter into the Name Server. This enables private devices that do not perform a fabric login (FLOGI), but accept a PRLI, to be entered in the Name Server and receive full fabric citizenship.

A fabric-capable device registers information with the Name Server during a FLOGI. These devices typically register information with the Name Server before querying for a device list. The embedded port will still conduct a PLOGI and attempt a PRLI with these devices.

To display the contents of a switch's Name Server, use the `nsShow` or `nsAllShow` command. For more information about these Name Server commands, refer to the *Brocade Fabric OS Command Reference Manual*.

Link Issues

The following table covers link-related issues, as indicated by port-status LEDs.

Table 13: Link Issues Related to Port-Status LEDs

Symptom	Probable Cause and Recommended Action
Port LEDs are flashing.	Depending on the rate of the flash and the color of the port LED, this could mean several things. To determine what is happening on either the port status LED or the power status LED, refer to the hardware installation guide or reference manual for that switch. There is a table that describes the purpose of the LEDs and explains the current behavior as well as suggested resolutions.
Port LEDs are steady.	The color of the port LED is important in this instance. To determine what is happening on either the port status LED or the power status LED, refer to the hardware installation guide or reference manual for that switch. There is a table that describes the purpose of the LEDs and explains the current behavior as well as suggested resolutions.
No light is emitted from port LEDs.	If there is no light coming from the port LED, no signal is being detected. Check your cable and SFP to determine the physical fault.

Connection Problems

Determine if the problem is the target or the host and then continue to divide the suspected problem path in half until you can pinpoint the problem. One of the most common solutions is zoning. Verify that the host and target are in the same zone. For more information on zoning, see Zoning.

Checking the Physical Connection

- Check the cables that are running to and from the host and storage to the switch.
  This path includes the patch panel. Verify that none of the cables is damaged, including indentations or bent cables.
- Check the SFP on the HBAs and switches.
  Verify that they are in good working condition. You can do this by swapping the current SFP with a known working SFP.
- Clean the optics.
  There are many kits on the market for cleaning fiber optics. You want to find a product that does not leave residue from a lint-free wipe or from the solvent.

Checking the Logical Connection

1. Enter the `switchShow` command.
2. Review the output from the command and determine if the device successfully logged in to the switch.
   - A device that is logically connected to the switch is registered as an F_Port, E_Port, EX_Port, VE_Port, or N_Port.
   - A device that is *not* logically connected to the switch is registered as a G_Port or U_Port, if NPIV is not on the switch.
3. Enter the `slotShow -m` command to verify that all blades are enabled and not faulty, disabled, or in some other nonavailable state.
4. Perform the appropriate actions based on how your missing device is connected:
   - If the missing device is logically connected, proceed to the next troubleshooting procedure (Checking the Name Server).
   - If the missing device is *not* logically connected, check the device and everything on that side of the data path. See also Link Failures for additional information.
     When you check the path, also verify the following factors for the host:

- The host OS is configured correctly.
- The third-party vendor multi-pathing input/output (MPIO) software, if it is being used, is configured correctly.
- The HBA and storage device and the driver and firmware are compatible with the switch based on the compatibility matrix.
- The driver settings and binaries are up to date.
- The device Basic Input Output System (BIOS) settings are correct.
- The HBA configuration is correct according to manufacturer's specifications.
- The SFPs in the HBA are compatible with the host's HBA.
- The SFP on the switch is compatible with the switch.
- The switch settings related to the host are configured correctly.

When you check the path, also verify the following factors for the target:

- The driver settings and binaries are up to date.
- The device BIOS settings are correct.
- The HBA configuration is correct according to the manufacturer's specifications.
- The SFPs in the HBA are compatible with the target HBA.
- The switch settings related to the target are configured correctly.

Checking the Name Server

1. Enter the `nsshow` command on the switch to determine if the device is attached:

```
switch:admin> nsshow
The Local Name Server has 9 entries {
Type Pid       COS PortName               NodeName                 TTL(sec)
*N   021a00;   2,3;20:00:00:e0:69:f0:07:c6;10:00:00:e0:69:f0:07:c6; 895
    Fabric Port Name: 20:0a:00:60:69:10:8d:fd
NL   051edc;   3;21:00:00:20:37:d9:77:96;20:00:00:20:37:d9:77:96; na
    FC4s: FCP [SEAGATE ST318304FC      0005]
    Fabric Port Name: 20:0e:00:60:69:10:9b:5b
NL   051ee0;   3;21:00:00:20:37:d9:73:0f;20:00:00:20:37:d9:73:0f; na
    FC4s: FCP [SEAGATE ST318304FC      0005]
    Fabric Port Name: 20:0e:00:60:69:10:9b:5b
NL   051ee1;   3;21:00:00:20:37:d9:76:b3;20:00:00:20:37:d9:76:b3; na
    FC4s: FCP [SEAGATE ST318304FC      0005]
    Fabric Port Name: 20:0e:00:60:69:10:9b:5b
NL   051ee2;   3;21:00:00:20:37:d9:77:5a;20:00:00:20:37:d9:77:5a; na
    FC4s: FCP [SEAGATE ST318304FC      0005]
    Fabric Port Name: 20:0e:00:60:69:10:9b:5b
NL   051ee4;   3;21:00:00:20:37:d9:74:d7;20:00:00:20:37:d9:74:d7; na
    FC4s: FCP [SEAGATE ST318304FC      0005]
    Fabric Port Name: 20:0e:00:60:69:10:9b:5b
NL   051ee8;   3;21:00:00:20:37:d9:6f:eb;20:00:00:20:37:d9:6f:eb; na
    FC4s: FCP [SEAGATE ST318304FC      0005]
Fabric Port Name: 20:0e:00:60:69:10:9b:5b
NL   051eef;   3;21:00:00:20:37:d9:77:45;20:00:00:20:37:d9:77:45; na
    FC4s: FCP [SEAGATE ST318304FC      0005]
    Fabric Port Name: 20:0e:00:60:69:10:9b:5b
N    051f00;   2,3;50:06:04:82:bc:01:9a:0c;50:06:04:82:bc:01:9a:0c; na
    FC4s: FCP [EMC     SYMMETRIX       5267]
    Fabric Port Name: 20:0f:00:60:69:10:9b:5b
```

2. Look for the device in the Name Server (NS) list, which lists the nodes that are connected to that switch. This allows you to determine if a particular node is accessible on the network.
   - If the device is not present in the NS list, the problem is between the device and the switch. There may be a timeout communication problem between edge devices and the name server, or there may be a login issue. First check the edge device documentation to determine if there is a timeout setting or parameter that can be reconfigured. Also, check the port log for NS registration information and FCP probing failures (using the `fcpprobeshow` command). If these queries do not help solve the problem, contact the support organization for the product that appears to be inaccessible.
   - If the device is listed in the NS, the problem is between the storage device and the host. There may be a zoning mismatch or a host/storage issue. Proceed to Zoning.
3. Enter the `portloginshow` command along with the port number to check the port login status.
4. Enter the `fcpprobeshow` command along with the port number to display the FCP probing information for the devices attached to the specified F_Port or L_Port. This information includes the number of successful logins and SCSI INQUIRY commands sent over this port and a list of the attached devices.
5. Check the port log to determine whether the device sent the FLOGI frame to the switch and the switch probed the device.

Link Failures

A link failure occurs when a server, storage, or switch device is connected to a switch, but the link between the devices does not come up. This prevents the devices from communicating to or through the switch.

Use the `switchShow` command to find the reason for link failures. If the `switchShow` command or LEDs indicate that the link has not come up properly, use one or more of the following procedures.

The port negotiates the link speed with the opposite side. The negotiation usually completes in one or two seconds; however, sometimes the speed negotiation fails.

Determining Successful Speed Negotiation

NOTE
Skip this procedure if the port speed is set to a static speed through the `portCfgSpeed` command.

1. Enter the `portcfgshow` command to display the port speed settings of all ports.
2. Enter the `switchshow` command to determine if the port has module light.
3. Enter the `portcfgspeed` command to change the port speed to 4G, 8G, 10G, 16G, or 32G, depending on what speed can be used by both devices. This should correct the negotiation by setting to one port speed.
4. Enter the `portlogshow` or `portlogdump` command. Check the events area of the output:

   The following example shows the `portlogdump` output. The output of the `portlogdump` command is very similar.

```
device:admin> portlogdump
time          task    event  port  cmd  args
----------------------------------------------------------------
14:38:51.976  SPEE    sn     200   NC   00000001,00000000,00000001
14:39:39.227  SPEE    sn     200   NC   00000002,00000000,00000001
```

   - In the event column, “sn” indicates a speed negotiation.
   - In the cmd column, “NC” indicates that the negotiation has completed.

   If these fields do not appear, proceed to Step 6.

5. If the fields in Step 5 do not appear, correct the negotiation by entering the `portcfgspeed` command with a speed option. Valid values are:
   - 0 - Auto Negotiate
   - 4 - 4G
   - 8 - 8G
   - 10 - 10G
   - 16 - 16G
   - 25 - 25G
   - 32 - 32G
   - 40 - 40G
   - 53 - 53G
   - 64 - 64G
   - ax - Auto Negotiate plus enhanced retries

Checking for a Point-to-Point Initialization Failure

1. Enter `switchshow` to confirm that the port is active and has a module that is synchronized.

   If a fabric device or another switch is connected to the switch, the switch port must be online.

2. Enter either the `portlogshow` command or the `portlogdump` command.

   Verify that the event area for the event entry is “pstate”. The command entry “AC” indicates that the port has completed point-to-point initialization.

```
device:admin> portlogdumpport 4
time          task      event    port  cmd  args
-----------------------------------------------
11:38:21.726  INTR      pstate   4     AC
```

3. Skip over the loop initialization phase.

   After becoming an active port, the port becomes an F_Port or an E_Port depending on the device on the opposite side. If the opposite device is a host or target device, the port becomes an F_Port. If the opposite device is another switch, the port becomes an E_Port.

   If there is a problem with the host or target device, enter `portcfggport` to force the port to try to come up as point-to-point only.

Correcting a Port That Has Come Up in the Wrong Mode

1. Enter `switchshow` .
2. Check the output from the `switchshow` command, and follow the suggested actions in Table.

Table 14: Suggested Actions Based on `switchshow` Command Output

Output	Suggested Action
Disabled	If the port is disabled because of persistent-disable or security reasons, attempt to resolve the issue and then enter the `portenable` command or, if persistently disabled, the `portcfgpersistentenable` command.
Bypassed	The port may be testing.
Loopback	The port may be testing.

Output	Suggested Action
E_Port	If the opposite side is not another switch, the link has come up in a wrong mode. Check the output from the `portlogshow` or `portlogdump` commands, and identify the link initialization stage where the initialization procedure went wrong.
F_Port	If the opposite side of the link is a private loop device or a switch, the link has come up in a wrong mode. Check the output from the `portlogshow` or `portlogdump` commands.
G_Port	The port has not come up as an E_Port or F_Port. Check the output from the `portlogshow` or `portlogdump` commands, and identify the link initialization stage where the initialization procedure went wrong.

NOTE
If you are unable to read a port log dump, contact your switch support provider for assistance.

Marginal Links

A marginal link involves the connection between the switch and the edge device. Isolating the exact cause of a marginal link involves analyzing and testing many of the components that make up the link (including the switch port, switch SFP, cable, edge device, or edge device SFP). Troubleshooting a marginal link can involve inspecting the error counters described in Troubleshooting a Marginal Link or running diagnostics on a link, a port, or an end-to-end path.

You can use the `portloopbacktest` command to verify the functional operation of a path on a switch. This test sends frames from a given port's transmitter and loops them back into the same port's receiver. The loopback is done at the parallel loopback path. The path traversed in this test does not include the media or the fiber cable.

Only one frame is transmitted and received at any given time. An external cable is not required to run this test. The port LEDs will flicker green rapidly while the test is running.

The following table shows the different loopback modes that you can use when using `portloopbacktest` to test a marginal link.

Table 15: Loopback Modes

Loopback Mode	Description
1	Port loopback (loopback plugs). See, D_Port Loopback Plug Configurations for more details.
2	External Serializer/Deserializer (SerDes) loopback.
5	Internal (parallel) loopback (indicates no external equipment).
7	Back-end bypass and port loopback.
9	Back-end bypass and internal loopback.
11	Back-end bypass and external loopback.

NOTE
Mode-8 is not supported on Gen 6 platforms except the Brocade 7810 Extension Switch. Instead, mode-11 has been introduced.

Troubleshooting a Marginal Link

Marginal links can cause intermittent problems in fabrics and reduce performance levels. To locate and troubleshoot marginal links, complete the following steps.

1. Run the standard D_Port tests.
2. Enter `porterrshow` .

   The following is typical output from this command.

```
device:admin> porterrshow
        frames  enc  crc  crc   too  too  bad  enc disc link loss loss frjt fbsy
       tx   rx  in   err g_eof shrt long eof  out c3   fail sync sig
     ========================================================================
  0:  665k 7.0k   0    0    0    0    0    0    6    0    0    1    2    0    0
  1:    0    0    0    0    0    0    0    0    0    0    0    0    2    0    0
  2:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
  3:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
  4:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
  5:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
  6:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
  7:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
  8:   78   60    0    0    0    0    0    0    7    0    0    3    6    0    0
  9:   12    4    0    0    0    0    0    0    3    0    0    1    2    0    0
 10:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
 11:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
 12:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
 13:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
 14:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
 15:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
 16:  665k 7.4k   0    0    0    0    0    0    6    0    0    1    2    0    0
(output truncated)
```

3. Examine the output to determine if there are a relatively high number of errors (such as CRC errors or ENC_OUT errors) or if there are a steadily increasing number of errors to confirm a marginal link. You should sample the data every five minutes until you see the counters increment.
   - The frames tx and frames rx values are the number of frames being transmitted and received.
   - The crc_err counter records frames with CRC errors. If this counter goes up, the physical path should be inspected. Check the cables to and from the switch, patch panel, and other devices. Check the SFP by swapping it with a known good working SFP.
   - The crc_g_eof counter records frames with CRC errors and a good EOF. The first port that detects a CRC error marks the frame with a bad EOF and passes the frame on to its destination. Subsequent ports in the path also detect the CRC error, and the crc_err counter increments on these ports. However, because the first port marked the frame with a bad EOF, the good EOF counter on the subsequent ports does not increment. The marginal link associated with the port with an increasing good EOF counter is the marginal link and the source of the errors.
   - The enc_out counter records errors that occur outside the frame and usually indicates a bad primitive. To determine if you are having a cable problem, take snapshots of the port errors using `porterrshow` every 5 to 10 minutes. If you notice the crc_err counter go up, you have a bad or damaged cable or device in the path.

     NOTE

     ICLs will see enc_out errors when ports on one side of the link are disabled.
   - The disc_c3 counter records discarded class 3 errors, which means that the switch is holding onto the frame longer than the hold time allows. One problem this could be related to is ISL oversubscription.

4. If you suspect a marginal link, isolate the areas by moving the suspected marginal port cable to a different port on the switch. Reseating the SFPs may also cure marginal port problems.

   If the problem stops or goes away, either the switch port or the SFP is marginal (proceed to Step 6).

   If the problem does not stop or go away, proceed to Step 5.

5. Perform the following steps to rule out cabling issues:
   a) Insert a new cable in the suspected marginal port.
   b) Enter the `porterrshow` command to determine if a problem still exists.
      - If the `porterrshow` output displays a normal number of generated errors, the issue is solved.
      - If the `porterrshow` output still displays a high number of generated errors, follow the troubleshooting procedures for the host or storage device in Device Login Issues on Fabric Switches.

6. If there are no cabling issues, run `portloopbacktest` on the marginal port. You will need an adapter to run the loopback test for the SFP. Alternatively, you can run the test on the marginal port using the loopback mode lb=5.

   Use the modes shown in Marginal Links to test the port. Refer to the *Brocade Fabric OS Command Reference Manual* for additional information on this command.

7. Check the results of the loopback test and proceed as follows:
   - If the loopback test failed, the port is bad. Block the port, replace the port blade, or replace the switch as needed.
   - If the loopback test did not fail, the SFP is bad and should be replaced.

Device Login Issues on Fabric Switches

A correct login is when the port type matches the device type that is plugged in. The following example shows that the device connected to Port 1 is a fabric point-to-point device and is correctly logged in as an F_Port.

```
switch:admin> switchshow
switchName:   brcd_G620
switchType:   162.0
switchState:  Online
switchMode:   Native
switchRole:   Subordinate
switchDomain: 1
switchId:     fffc01
switchWwn:    10:00:00:00:00:00:00:00
zoning:       OFF
switchBeacon: OFF
FC Router:    OFF
FC Router BB Fabric ID: 1
Area Port Media Speed State          Proto
==========================================================
  0   0   --    N32   No_Module
  1   1   --    N16   Online         FC  F-Port  10:00:00:05:1e:8f:c1:31
  2   2   --    N32   No_Module
  3   3   --    N32   No_Module
(output truncated)
 61  61   --    N32   No_Module
 62  62   --    N32   No_Module
 63  63   --    N32   No_Module
 64  64   id    N32   Online          E-Port  10:00:00:05:1e:34:d0:05 "1_d1" (Trunk master)
 65  65   --    N32   No_Module
 66  66   --    N32   No_Module
```

```
67  67   id    AN    No_Sync
68  68   id    N16   Online          L-Port  13 public
69  69   --    N32   No_Module
70  70   --    N32   No_Module
71  71   id    N16   Online          L-Port  13 public
72  72   --    N32   No_Module
73  73   --    N32   No_Module
74  74   --    N32   No_Module
75  75   --    N32   No_Module
76  76   id    N16   Online          E-Port  10:00:00:05:1e:34:d0:05 "1_d1" (upstream)(Trunk master)
77  77   id    N16   Online          F-Port  10:00:00:06:2b:0f:6c:1f
78  78   --    N32   No_Module
79  79   id    N16   Online          E-Port  10:00:00:05:1e:34:d0:05 "1_d1" (Trunk master)
```

Pinpointing Problems with Device Logins

1. Log in to the switch as admin.
2. Enter the `switchShow` command, and check the login state.
3. Enter the `portCfgShow` command to see if the port is configured correctly.

   In some cases, you may find that the port has been locked as an L_Port and the device attached is a fabric point-to-point device such as a host or switch. This would be an incorrect configuration for the device, and therefore the device cannot log in to the switch.

   To correct this type of problem, unlock the port using the `portCfgLport [[`*slot*`]/`*port*`] 0` command. The `portCfgDefault` command may cause other settings to be changed.

```
switch:admin> portcfgshow
Ports of Slot 0    0  1  2  3    4  5  6  7    8  9 10 11   12 13 14 15
-----------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+--
Speed             AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Trunk Port        ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Long Distance     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
VC Link Init      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked L_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked G_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Disabled E_Port   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
ISL R_RDY Mode    .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
RSCN Suppressed   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Persistent Disable.. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
NPIV capability   ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
                  where AN:AutoNegotiate, ..:OFF, ??:INVALID,
                  SN:Software controlled AutoNegotiation.
```

4. Enter the `portErrShow` command; then, check for errors that can cause login problems. A steadily increasing number of errors can indicate a problem. Track errors by sampling the port errors every five or ten minutes until you see the problem occur again.
5. Enter the `portFlagsShow` command; then, check to see how a port has logged in and where a login failed (if a failure occurred):

```
switch:admin> portflagsshow
Port SNMP      Physical   Flags
--------------------------------
```

```
0 Offline      In_Sync    PRESENT U_PORT LED
1 Online       In_Sync    PRESENT ACTIVE F_PORT G_PORT U_PORT LOGICAL_ONLINE LOGIN NOELP LED ACCEPT
2 Offline      No_Light   PRESENT U_PORT LED
3 Offline      No_Module  PRESENT U_PORT LED
4 Offline      No_Module  PRESENT U_PORT LED
5 Offline      No_Light   PRESENT U_PORT LED
6 Offline      No_Module  PRESENT U_PORT LED
7 Offline      No_Module  PRESENT U_PORT LED
8 Offline      No_Light   PRESENT U_PORT LED
9 Offline      No_Light   PRESENT U_PORT LED
10 Offline     No_Module  PRESENT U_PORT LED
11 Offline     No_Module  PRESENT U_PORT LED
12 Offline     No_Module  PRESENT U_PORT LED
13 Offline     No_Module  PRESENT U_PORT LED
14 Online      In_Sync    PRESENT ACTIVE F_PORT G_PORT U_PORT LOGICAL_ONLINE LOGIN NOELP LED ACCEPT
15 Online      In_Sync    PRESENT ACTIVE E_PORT G_PORT U_PORT SEGMENTED LOGIN LED
```

6. Enter the `portLogDumpPort` command; then, view the device-to-switch communication.

```
switch:admin> portlogdumpport 8 | more
time         task       event   port cmd  args
-----------------------------------------------
Thu Nov  6 16:52:39 2008
16:52:39.066 PORT       scn       8    1  00010004,4302000f,02000000
16:52:39.066 PORT       scn       8    2  ce3dfab0,d9672800,00000002
16:52:39.066 PORT       scn       8    2  ce3dfab0,d9672800,00000080
16:52:39.066 PORT       scn       8    5  00000000,00000000,00000002
16:52:39.066 PORT       scn       8    1  00010004,4302000f,00000002
16:52:39.066 PORT       scn       8    1  00010004,4302000f,02000000
16:52:39.071 PORT       ioctl             88010004  1,0 * 4
16:52:42.311 SPEE       sn        8   WS  00000000,00000000,00000000
16:52:42.558 SPEE       sn        8   NM  00000000,00000000,00000000
16:52:42.558 SPEE       sn        8   NF  00000000,00000000,00000000
16:52:42.558 SPEE       sn        8   NC  00000001,00000000,00000000
16:52:42.559 LOOP       loopscn   8  LIP  8002
16:52:42.559 LOOP       loopscn   8  LIP  f7f7
16:52:42.572 LOOP       loopscn   8  LIM  0
16:52:42.572 PORT       Tx3       8   12  22000000,00000000,ffffffff,11010000
16:52:42.572 PORT       Rx3       8   12  22000000,00000000,ffffffff,11010000
16:52:42.572 PORT       Tx3       8   20  22000000,00000000,ffffffff,11020000
16:52:42.572 PORT       Rx3       8   20  22000000,00000000,ffffffff,11020000
16:52:42.572 PORT       Tx3       8   20  22000000,00000000,ffffffff,11030000
16:52:42.572 PORT       Rx3       8   20  22000000,00000000,ffffffff,11030000
```

NOTE
See Port log for overview information about `portLogDump` .

Device Login Issues on Access Gateways

Hosts might have problems logging in to the fabric through an Access Gateway under the following conditions:

- Hosts and Target port are connected to an Access Gateway.
- F_Ports on an Access Gateway have NPIV logins.
- Different hosts log in and log out of the same Access Gateway F_Port.
- The Access Gateway Persistent AL_PA feature is enabled.
- Devices are connected to an Access Gateway port configured as N_Ports.
- More than 126 logins are attempted via an F_Port configured for the default number of logins (126).
- The `porttrunkarea` command is configured on an edge switch, but the trunking license is missing on the Access Gateway device.
- Link-level issues exist between an edge switch and the Access Gateway.
- Static mapping is configured for F_Ports but the relevant N_Port is disabled.
- Other Access Gateway policy specific features, such as port grouping and advance device security, are the cause for device login issues on an Access Gateway.

To resolve this issue, follow these steps:

1. Identify all affected F_Ports with duplicate AL_PA entries, and do the following for each port.
2. Enter `ag --printalpamap` *`port_#`* to print the AL_PA map.
3. Enter `portdisable` *`port_#`* to disable all affected F_Ports with duplicate AL_PA entries.
4. Enter `ag --clearalpamap` *`port_#`* to clear the AL_PA map.
5. Enter `portenable` *`port_#`* to re-enable the specified port.

Troubleshooting the FC-LAG

This section describes the procedure and techniques that can be used to troubleshoot problems related to FC-LAG feature.

Checking the FC-LAG connectivity

Use `fclag --show` to check if the FC-LAG is in good condition. By default, the admin status should be enabled and the link status should be UP. In addition, at least one of the member ports should be in the Link Status UP state, as shown in the following example:

```
Device:admin> fclag --show
FC-LAG Name: test
FC-LAG Port-WWN: f1:f5:7c:02:20:98:01:90
FC-LAG Admin Status: ENABLED
FC-LAG Link Status: UP
FC-LAG Port-Index: 400
Member ports: 2
Port 10: Admin Status ENABLED, Link Status UP
Port 11: Admin Status ENABLED, Link Status UPTotal number of FC-LAG(s) = 1
```

If the FC-LAG link status is not in the UP state, check the status of the FC-LAG port index using the `portshow 400` command. In addition, check the output using the, `switchshow` command to verify if the member port status is displayed correctly and the ports are brought up correctly.

If all port statuses look good, then the FC-LAG has been brought up correctly. If not, try the following troubleshooting steps:

1. Ensure that the FC-LAG member ports are configured correctly on both the Brocade and Cisco side. Most of the times, the FC-LAG is not up due to misconfiguration.
2. Verify and clear any misconfiguration as follows:

- Ensure that all ports are of the same speed.
- Ensure that the FC-LAG physical links are connected to a supported platform.
- Ensure that the all FC-LAG links lead to the same switch.
- Ensure that the number of supported FC-LAGs is not exhausted.

3. If the FC-LAG does not come up, use the following commands:

```
Device:admin> fclag --disable kcm61
FC-LAG 'kcm61' is disabled.
Device:admin> fclag --enable kcm61
FC-LAG 'kcm61' is enabled.
```

4. If the FC-LAG port does not come up, you can delete the FC-LAG port using the `fclag --delete` command and then re-create the FC-LAG port. If the FC-LAG port still does not come up, try clearing the configuration completely using the `fclag --clearall` command and re-entry the configuration.
5. If after all these steps, you cannot successfully bring up the FC-LAG, take a supportSave and contact your customer service representative.

Media-Related Issues

This section provides procedures that help pinpoint any media-related issues in the fabric, such as bad cables and SFPs. The tests listed in Table are a combination of structural and functional tests that can be used to provide an overview of the hardware components and help identify media-related issues.

- *Structural* tests perform basic testing of the switch circuit. If a structural test fails, replace the main board or port blade.
- *Functional* tests verify the intended operational behavior of the switch by running frames through ports or bypass circuitry.

Table 16: Component Test Descriptions

Test Name	Checks
portTest	Isolate problems to a single replaceable element, near-end terminal equipment, far-end terminal equipment, or transmission lines. Diagnostics can be performed every day or on demand.
spinFab	Tests switch-to-switch ISL cabling and trunk group operations.

The following procedures are for checking switch-specific components.

Testing the External Transmit and Receive Path of a Port

1. Connect to the switch and log in as admin.
2. Connect external loopback cables to the port that needs to be tested.
3. Disable the switch/chassis using `chassisdisable` command followed by `portloopbacktest -lb_mode 1 -ports <bladeportnumber>`.

Testing the Internal Components of a Switch

1. Connect to the switch and log in as admin
2. Disable the switch/chassis using `chassisdisable` command, followed by `portloopbacktest -lb_mode 2` command where 2 is the operand that causes the test to run on the internal switch components (Serdes level loopback).

Testing Components to and from an HBA

To test components to and from an HBA, complete the following steps.

1. Connect to the switch and log in as admin.
2. Enter the `porttest` command (refer to the *Brocade Fabric OS Command Reference Manual* for information on the command options).

   See Table for a list of additional tests that can be used to determine the switch components that are not functioning properly. Refer to the *Brocade Fabric OS Command Reference Manual* for additional command information.

Table 17: Switch Component Tests

Test	Function
`portbeacon`	Sets port beaconing mode.
`portloopbacktest`	Performs a functional test of the port N-to-N path. Verifies the functional components of the switch.
`turboramtest`	Verifies that the on-chip SRAM located in the ASIC is using the Turbo-Ram BIST circuitry. This allows the BIST controller to perform the SRAM write and read operations at a much faster rate.

Media Piracy

Media piracy proofing increase the highest level of media (SFPs) security so that only genuine Brocade branded media is used in Brocade switches. The falsely branded SFPs are detected and flagged as “pirated media" so that you can replace them with genuine Brocade branded SFPs. If you don't take corrective action after repeated warnings, the port will be disabled with the appropriate reason code which potentially bring down the media operation. Piracy proofing is applicable only to GEN7 SFPs but supports all Brocade switch platforms that provide I2C bus provision.

Segmented Fabrics

Fabric segmentation is generally caused by one of the following conditions:

- Incompatible fabric parameters (see Reconciling Fabric Parameters Individually)
- Incompatible zoning configuration (see Zoning)
- Domain ID conflict (see Reconciling Fabric Parameters Individually)
- Fabric ID conflict (see Virtual Fabrics)
- Incompatible security policies
- Incorrect fabric mode
- Incorrect policy distribution
- Incompatible software features

A number of settings control the overall behavior and operation of the fabric. Some of these settings, such as the domain ID, are assigned automatically by the fabric and can differ from one switch to another in the fabric. Other parameters, such as the BB credit, can be changed for specific applications or operating environments, but they must be the same among all switches to allow the formation of a fabric.

In general, the following fabric parameters must be identical on each switch for fabrics to merge. However, the following table summarizes the scenarios when the fabrics are not segmented (but merged) even when these fabric parameters are not identical.

Table 18: Segmented Fabric Scenarios

Fabric Parameter	LISL	XISL	ISL
Domain ID	Not segmented (merged)	Segmented	Segmented
R_A_TOV	Segmented	Segmented	Segmented
E_D_TOV	Segmented	Segmented	Segmented
Data field size	Segmented	Segmented	Segmented
Sequence level switching	Not segmented (merged)	Segmented	Segmented
Disable device probing	Not segmented (merged)	Not segmented (merged)	Segmented
Suppress class F traffic	Segmented	Segmented	Segmented
Per-frame route priority	Not segmented (merged)	Segmented	Segmented
Long-distance fabric	Not segmented (merged)	Segmented	Segmented
Virtual Channel parameters	Not segmented (merged)	Not segmented (merged)	Segmented

NOTE
The long-distance fabric parameter does not need to be identical on Brocade G620 Switches and Brocade X6 Directors.

Reconciling Fabric Parameters Individually

1. Log in as admin to one of the segmented switches.
2. Enter the `configShow -pattern "fabric.ops"` command.
3. Log in as admin to another switch in the same fabric.
4. Enter the `configShow -pattern "fabric.ops"` command.
5. Compare the two switch configurations line by line and look for differences. Do this by comparing the two Telnet windows or by printing the `configShow -pattern "fabric.ops"` output. Also, verify that the fabric parameter settings (see the list of fabric parameters in Segmented Fabrics) are the same for *both* switches.
6. Connect to the segmented switch after the discrepancy is identified.
7. Disable the switch by entering the `switchDisable` command.
8. Enter the `configure` command to edit the appropriate fabric parameters for the segmented switch.
9. Enable the switch by entering the `switchEnable` command.

   Alternatively, you can reconcile fabric parameters by entering the `configUpload` command for each switch and uploading a known good configuration file. This option requires that the two switches be the same model.

Downloading a Correct Configuration

You can restore a segmented fabric by downloading a previously saved correct backup configuration to the switch. Downloading in this manner reconciles any discrepancy in the fabric parameters and allows the segmented switch to rejoin the main fabric. For details on uploading and downloading configurations, refer to the *Brocade Fabric OS Administration Guide*.

Reconciling a Domain ID Conflict

If a domain ID conflict appears, the conflict is reported only at the point where the two fabrics are physically connected. However, there may be several conflicting domain IDs, which appear as soon as the initial conflict is resolved.

Typically, the fabric automatically resolves domain conflicts during fabric merges or builds unless Insistent Domain ID (IDID) is configured. If IDID is enabled, switches that cannot be programmed with a unique domain ID are segmented. Check each switch that has IDID configured and make sure that their domain IDs are unique within the configuration.

Repeat the following procedure until all domain ID conflicts are resolved.

1. Enter `fabricshow` on a switch from one of the fabrics.
2. In a separate Telnet window, enter `fabricshow` on a switch from the second fabric.
3. Compare the `fabricshow` output from the two fabrics. Note the number of domain ID conflicts; there may be several duplicate domain IDs that must be changed.

   Determine which switches have domain overlap, and change the domain IDs for each of those switches.

4. Choose the fabric on which to change the duplicate domain ID; connect to the conflicting switch in that fabric.
5. Enter `switchdisable` .
6. Enter `configure` .
7. When the `Fabric Parameters` prompt displays, enter `y` and press `Enter` .
8. When the `Domain` prompt displays, enter the new domain ID number and press `Enter` .
9. Press `Enter` for all remaining prompts to accept their default settings.

CAUTION
Do not press **Ctrl+C** as this will exit the configuration without saving it.

10. Enter `switchenable` .

    This enables the joining switch to obtain a new domain ID as part of the process of coming online. The fabric principal switch allocates the next available domain ID to the new switch during this process.

11. Repeat Step 4 through Step 10 if additional switches have conflicting domain IDs.

    The following example illustrates setting the domain ID.

```
Device:admin> switchdisable
2020/02/19-01:31:37, [MFIC-1003], 25498, FID 128, WARNING, cassian_81, Effective Insistent domain ID for
 the fabric changed from OFF to ON.
Device:admin> configure

Configure...

  Fabric parameters (yes, y, no, n): [no] y

    Domain: (1..239) [1] 10
    WWN Based persistent PID (yes, y, no, n): [no]
    R_A_TOV: (4000..120000) [10000]
    E_D_TOV: (1000..5000) [2000]
    WAN_TOV: (0..30000) [0]
    MAX_HOPS: (7..19) [7]
    Data field size: (256..2112) [2112]
    Sequence Level Switching: (0..1) [0]
    Disable Device Probing: (0..1) [0]
    Suppress Class F Traffic: (0..1) [0]
    Per-frame Route Priority: (0..1) [0]
    BB credit: (1..27) [16]
    Disable FID Check (yes, y, no, n): [no]
    Insistent Domain ID Mode (yes, y, no, n): [yes]
    Disable Default PortName (yes, y, no, n): [no]
    Display FDMI Host Name (yes, y, no, n): [no]
    Dynamic Portname (on, off): [off]
    Edge Hold Time(Low(80ms), Medium(220ms), High(500ms), UserDefined(80-500ms): (80..500) [220]
    Remote Fosexec feature: (on, off): [off]
    High Integrity Fabric Mode (yes, y, no, n): [no]
  F-Port login parameters (yes, y, no, n): [no]
  D-Port Parameters (yes, y, no, n): [no]
  RDP Polling Cycle(hours)[0 = Disable Polling]: (0..24) [1]
  Zoning Operation parameters (yes, y, no, n): [no]
```

```
    RSCN Transmission Mode (yes, y, no, n): [no]
    System services (yes, y, no, n): [no]
    Portlog events enable (yes, y, no, n): [no]
    cfgload attributes (yes, y, no, n): [no]

WARNING: The domain ID will be changed. The port level zoning may be affected
```

Reconciling Incompatible Software Features

Earlier releases of software may not be supported in new versions of Fabric OS. This may be due to a software feature changing or new services being supported. If you suspect that you are trying to introduce a switch into a fabric that has an older version of software, check the release notes to verify that any features on that switch are supported in the fabric with the newer software.

In Fabric OS 7.0.0 and later, an ESC frame is used to exchange fabric parameters to detect Virtual Fabric FID conflicts. If at any point during the ESC frame exchange, a link with incompatible parameters is detected, the switch running Fabric OS 7.0.0 or later does not join the existing fabric. To fix this issue, refer to the *Brocade Fabric OS Administration Guide* for more information on that specific software feature.

Configuration

Configuration Upload and Download Issues

It is important to maintain consistent configuration settings on all switches in the same fabric because inconsistent settings (such as inconsistent PID formats) can cause fabric segmentation. As part of standard configuration maintenance procedures, back up all important configuration data for every switch on a host computer server for emergency reference and possible download purposes.

If the configuration download fails, you must examine the following aspects:

- Did you download the correct file for the switch?
- Is the switch logically partitioned and was the correct FID used?
- Was the switch changed recently with logical switch management such that FIDs may no longer correspond?

> **NOTE**
> For information about Virtual Fabrics using Fabric OS 7.2.4 or later, refer to the *Brocade Fabric OS Administration Guide*.

The following table covers configuration upload and download issues.

Table 19: Issues Related to Configuration Uploading and Downloading

Symptom	Probable Cause and Recommended Action

The configuration upload fails.	Configuration upload failures may be due to one or more of the following reasons:
	• The FTP, SFTP, or SCP server's host name is not known to the switch.
	Verify with your network administrator that the switch has access to the FTP server.
	• The USB path is not correct.
	If your platform supports a USB memory device, verify that it is connected and running. Verify that the path name is correct by using the `usbstorage -l` command.
	Example of the `usbstorage -l` command:
	`device:admin> usbstorage -l`
	`firmwarekey\ 0B 2019 Aug 15 15:13`
	`support\ 106MB 2019 Aug 24 05:36`
	`support1034\ 105MB 2019 Aug 23 06:11`
	`config\ 0B 2019 Aug 15 15:13`
	`firmware\ 380MB 2019 Aug 15 15:13`
	`FW_v6.0.0\ 380MB 2019 Aug 15 15:13`
	`Available space on usbstorage 74%`
	• The FTP, SFTP, or SCP server's IP address cannot be contacted.
	Verify that you can connect to the FTP server. Use your local PC to connect to the FTP server or ping the FTP server. Example of a successful ping:
	`C:\> ping 192.001.001.001`
	`Pinging 192.001.001.001 with 32 bytes of data:`
	`Reply from 192.001.001.001: bytes=32 time=5ms TTL=61`
	`Ping statistics for 192.001.001.001:`
	`Packets: Sent = 4, Received = 4, Lost = 0 (0%loss),`
	`Approximate round trip times in milli-seconds:`
	`Minimum = 4ms, Maximum = 5ms, Average = 4ms`
	If your ping is successful from your computer, but you cannot reach it from inside your data center, there could be a block on the firewall to not allow FTP connections from inside the data center. Contact your network administrator to determine if this is the cause and to resolve it by opening the port on both inbound and outbound UDP and TCP traffic. Example of a failed ping:
	`C:\> ping 192.001.001.001`
	`Pinging 192.001.001.001 with 32 bytes of data:`
	`Request timed out.`
	`Request timed out.`
	`Request timed out.`
	`Request timed out.`
	`Ping statistics for 192.001.001.001:`
	`Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),`

The configuration upload fails.	If your ping fails, you should verify the following: • The ports are open on the firewall. • The FTP server is up and running. • You have configured Admin Domain on the switch. A message such the following is displayed: `2019/11/08/-05:17:34, [ZONE-1069], 28, FID 128, WARNING, SW6510_35_111, Admin Domains are not supported in Fabric OS 8.1.0 (Event:AD_Update, AD4).`

Symptom	Probable Cause and Recommended Action

The configuration upload fails.	• You do not have configuration upload permission on the switch.
	There may be some restrictions based on Role-Based Access Control settings. For more information on these types of restrictions, refer to the *Brocade Fabric OS Administration Guide*.
	• You do not have permission to write to the directory on the FTP, SFTP, or SCP server. For an unsuccessful login to the FTP server, the output should be similar to the following:
	`C:\> ftp 192.001.001.001`
	`Connected to 192.001.001.001`
	`220 Welcome to Services FTP service.`
	`User (10.10.10.10:(none)): userFoo`
	`331 Please specify the password.`
	`Password: <hidden>`
	`530 Login incorrect.`
	`Login failed.`
	• If your login to the FTP, SFTP, or SCP server fails, verify that the user name and password combination that you used is correct.
	• On a switch enabled with Virtual Fabrics, you do not have the chassis role permission set on your user account. You will need to change this permission or use an account that does have this permission and then retry the upload.
	Implement one change at a time, then issue the command again. By implementing one change at a time, you can determine what works and what does not work. Knowing which change corrected the problems will help you avoid this problem in the future.

The configuration download fails.	Configuration download failures may be due to one or more of the following reasons: • The FTP, SFTP, or SCP server's host name is not known to the switch. Verify with your network administrator that the switch has access to the FTP server. • The USB path is incorrect. If your platform supports a USB memory device, verify that it is connected and running. Verify that the path name is correct. It should be the relative path from `/usb/usbstorage/brocade/configdownload` or use the absolute path. • The FTP, SFTP, or SCP server's IP address cannot be contacted. Verify that you can connect to the FTP server. Use your local PC to connect to the FTP server or ping the FTP server. • There was a reason to disable the switch. Note, however, that you must disable the switch for some configuration downloads. For more information on how to perform a configuration download without disabling a switch, refer to the *Brocade Fabric OS Administration Guide*. • You do not have permission on the host to perform configuration download. There may be some restrictions if you are using Role-Based Access Control. For more information on these types of restrictions, refer to the *Brocade Fabric OS Administration Guide*. • The configuration file that you are trying to download does not exist on the host. • The configuration file that you are trying to download is not a switch configuration file. • If you selected the (default) FTP protocol, the FTP server is not running on the host. • The configuration file that you are trying to download uses incorrect syntax. • The user name and password combination that you used are incorrect.
The switch reboots during the configuration download.	When you run `configdownload -vf`, having both CPs reboot is normal. This option downloads the Virtual Fabrics-related data. After the reboot, you can continue following the instructions. Otherwise, try the command again without the `-vf` operand to download the regular configuration data. This does not cause a reboot. However, a notice that `A switch reboot is required for the changes to take effect.` is displayed, and you will need to reboot the device. There is no reliable mechanism to determine which parameters may or may not require a reboot. To ensure that all configuration changes are applied correctly, always reboot the switch after a configuration download.

Symptom	Probable Cause and Recommended Action
The configuration did not seem to change after the configuration download process finished.	Verify that the switch was rebooted by checking the system log. On a enterprise-class platform, verify that both CPs rebooted by checking the system log. If any error occurs during the download, such as an error about a particular key, it is important to enter `configdefault` and then run the `configdownload` command again.

Gathering Additional Information

When you are analyzing the problem, be sure to capture the output from the commands that you issue from both the switch and your computer.

Send this output and all logs to your switch support provider.

Messages Captured in the Logs

Issuing the `configDownload` command generates both RASLog and Audit log messages.

The following messages are written to the logs:

- `configDownload completed successfully ...` (RASLog and Audit log)
- `configUpload completed successfully ...` (RASLog)
- `configDownload not permitted ...` (Audit log)
- `configUpload not permitted ...` (RASLog)
- `(Warning) Downloading configuration without disabling the switch was unsuccessful.` (Audit log)

Non-interactive Configuration Commands

Use `configure` and `configureChassis` to make non-interactive configuration changes using the `configure --query/--set/--show/--default` commands. The command syntax is displayed below:

```
configure --query [-module module_name [-key key_name]]
configure --show [-module module_name [-key key_name]]
configure --set  -module module_name -key key_name -value value
configure --default  -module module_name -key key_name
```

Brocade Configuration Form

Print and use the following table as a hard-copy reference to record the configuration information for the various blades, switches, and chassis.

Table 20: Brocade Configuration and Connection

Brocade Configuration Settings	Value
IP address	
Gateway address	
Chassis configuration option	
Management Connections	
Serial cable tag	
Ethernet cable tag	
Configuration Information	

Brocade Configuration Settings	Value
Domain ID	
Switch name	
Ethernet IP address	
Ethernet subnet mask	
Total number of local devices (`nsshow`)	
Total number of devices in the fabric (`nsallshow`)	
Total number of switches in the fabric (`fabricshow`)	

Firmware Download Errors

Firmware Download Issues

CAUTION
After you start the firmware download process, do not enter any disruptive commands that interrupt the process (such as reboot). The entire firmware download and commit process can take more than 30 minutes. If there is a problem, wait for the timeout (30 minutes for network problems) before entering the `firmwaredownload` command again. Disrupting the process can render the switch inoperable and require you to seek help from your switch service provider. Do not disconnect the switch from power during the process because the switch could become inoperable when it reboots.

The following table describes common firmware download issues and their recommended actions.

Table 21: Issues Related to Firmware Downloading

Symptom	Probable Cause and Recommended Action
The firmware download times out.	The timeout can be caused by an excessively slow network. If it takes more than 30 minutes to download firmware on a switch or on each CP in a director, the firmware download process times out. If a timeout occurs on a switch, the firmware download process synchronizes the two partitions on the switch by starting a firmware commit operation. If a timeout occurs on a director, the firmware download process synchronizes the firmware on the two partitions on the CP blades by starting a firmware commit operation on each CP. Wait at least 15 minutes for the commit operation to complete and then use the `firmwareshow` command to verify that the partitions are synchronized. In some older versions of firmware, the firmware commit operation may not be started automatically on the switch (or on the standby CP in the director). In this case, you can manually enter the `firmwarecommit` command on the switch (or on the standby CP in the director) to synchronize the partitions. After the firmware commit operation completes, re-issue the `firmwaredownload` command to upgrade the system. To avoid timeouts, ensure that you are using the highest connection speeds supported on your device for downloads. Use the 1GbE management port connection if supported.

The server is inaccessible, or the firmware path is invalid.	• The FTP or SCP server's host name is not known to the switch.
	Verify with your network administrator that the switch has access to the FTP server.
	Verify that the path to the FTP or SCP server is accessible from the switch. For more information on checking your FTP or SCP server, see Configuration.
	• The USB path is not correct.
	If your platform supports a USB memory device, verify that it is connected and running using the `usbstorage -e` command. If USB memory is connected, you are notified, and commands such as `usbstorage -l` will work if the device is running. If the device is running, verify that the path name is correct using `usbstorage -l` .
	The entire firmware directory must be loaded onto the USB device under the "firmware" directory before using the USB device for firmware download.
	Here is an example of the `usbstorage -l` command output:
	`switch:admin> usbstorage -l`
	`config\ 307kB 2022 Jan 07 10:31`
	`firmware\ 380MB 2018 Oct 30 14:40`
	`firmwarekey\ 0B 2007 Sep 28 15:33`
	`support\ 15MB 2019 Feb 19 15:27`
	`support supportsave\ 0B 2019 May 21 06:46`
	`FW_v9.1.0\ 190MB 2022 Jan 07 10:31`
	`Available space on usbstorage 74%`
	Here is an example of an error message:
	`switch:admin> firmwaredownload`
	`Download from USB [No]: y`
	`Firmware filename: v9.1.0`
	`Server IP: 127.1.1.1, Protocol IPv4`
	`Checking system settings for firmwaredownload..`
	`Failed to access usb://127.1.1.1//usb/usbstorage/Brocade/firmware/v9.1.0/release.plist`
	`Cannot access the firmware on USB device.`
	`Please check the firmware path.`

Symptom	Probable Cause and Recommended Action

You cannot download the requested firmware.	The firmware that you are trying to download on the switch is incompatible. Check the firmware version against the switch type. If the firmware is incompatible, retrieve the correct firmware version and try again.
	Example of error message:
	`switch:admin> firmwaredownload`
	`Server Name or IP Address: 192.000.000.000`
	`User Name: userFoo`
	`File Name: /users/home/userFoo/firmware/v8.1.0`
	`Network Protocol(1-auto-select, 2-FTP, 3-SCP) [1]: 2`
	`Password: <hidden>`
	`Server IP: 192.000.000.000, Protocol IPv4`
	`Checking system settings for firmwaredownload...`
	`Cannot download the requested firmware because the firmware doesn't support this platform. Please enter another firmware path.`

You cannot download an Interop fabric on a switch with Interop mode turned on.	On a single CP system, the Interop fabric does not support Coordinated Hot Code Load.

You receive a `firmware download is already in progress` message.	The firmware download process has already been started, and it is in progress. Wait until it completes. You can use the `firmwaredownloadstatus` and `firmwareshow` commands to monitor its progress. If the problem persists, contact your switch support provider. This error commonly occurs when the application blades are upgrading or a commit operation is in progress.
	Example of a firmware download already in progress:
	`switch:admin> firmwaredownload`
	`Server Name or IP Address: 192.000.000.000`
	`User Name: userFoo`
	`File Name: /users/home/userFoo/firmware/v9.1.0`
	`Network Protocol(1-auto-select, 2-FTP, 3-SCP) [1]: 2`
	`Password: <hidden>`
	`Server IP: 192.000.000.000, Protocol IPv4`
	`Checking system settings for firmwaredownload...`
	`Sanity check failed because firmwaredownload is already in progress.`

Firmwaredownload failed due to non-acceptance of this product's End User License Agreement.	This is caused due to non acceptance of End User License Agreement (EULA). `-acceptEULA` is added to firmwaredownload command line as an indication for confirmation of the user's acceptance of EULA. You can use `-showEULA` to show the actual EULA contents. Below are the Firmware Upgrade/Downgrade behavior across platforms: • Firmware upgrade from a non-EULA FOS version to a EULA configured FOS version (pre-FOS v9.0.0) will continue to work as is without the need to accept the end user license agreement. • Firmware upgrade from a non-EULA FOS version (pre-FOS v9.0.0) to FOS v9.0.0 and later, you must accept the end user license agreement to proceed with the firmware upgrade or the upgrade will be aborted. • Firmware upgrade from a EULA-to-EULA configured FOS version (pre-FOS v9.0.0 or FOS v9.0.0 and later), you must accept the end user license agreement or bypass using `-acceptEULA` command option. • Firmware upgrade or downgrade from a EULA configured FOS version to a non-EULA version, you must accept the end user license agreement or bypass using `-acceptEULA` command option.

Troubleshooting with the firmwaredownload Command

NOTE
Do not run mixed firmware versions on CPs.

A network diagnostic script and preinstallation check is a part of the firmware download procedure. The script and preinstallation check performs troubleshooting and automatically checks for any blocking conditions. If the firmware download fails, refer to the *Brocade Fabric OS Message Reference* for details about error messages. Also see Considerations for Downgrading Firmware.

If a firmware download fails in a director, the `firmwaredownload` command synchronizes the firmware on the two partitions of each CP by starting a firmware commit operation. Wait at least 15 minutes for this commit operation to complete before attempting another firmware download. Use the `firmwaredownloadstatus` command to determine the commit status if needed.

If the firmware download fails in a director or enterprise-class platform, the CPs may end up with different versions of firmware and be unable to achieve HA synchronization between the two blades. In such cases, issue the `firmwaredownload -s` command on the standby CP; the single mode option (`-s`) allows you to upgrade the firmware on the standby CP to match the firmware version running on the active CP. This situation can also occur during a CP replacement in which the replacement CP has a lower firmware version. HA should be disabled and the firmware should be updated on the replacement CP before any other operations are considered.

Then, reissue the `firmwaredownload` command to download the desired firmware version to both CPs. For example, if CP0 is running Fabric OS 9.0.x on the primary and secondary partitions, and CP1 is running Fabric OS 9.1.x or Fabric OS 9.2.x on the primary and secondary partitions, a valid TruFOS certificate is required to reissue the `firmwaredownload` command or `firmwaresync` command on the active CP to copy the currently active firmware to the standby CP.

NOTE
Some of the messages include error codes (as shown in the following example). These error codes are for internal use only, and you can disregard them.

```
Port configuration with EX ports enabled along with trunking for port(s) 63, use
 the portCfgEXPort, and portCfgTrunkPort commands to remedy this. Verify blade is
 ENABLED. (error 3)
```

Gathering Additional Information

You should follow these best practices for firmware download before you start the procedure:

- Keep all session logs.
- Enter the `supportSave` or `supportShow` command before and after entering the `firmwareDownload` command.
- If a problem persists, package all information (the Telnet session logs and serial console logs, output from the `supportSave` command) for your switch support provider. Make sure that you identify what information was gathered before and after issuing the `firmwareDownload` command.

USB Error Handling

Table outlines how the USB device handles errors under specific scenarios and details what actions you should take after the errors occur.

Table 22: USB Error Handling

Scenario Under which Download Fails	Error Handling	Action
An access error occurs during firmware download because of the removal of the USB device, because of a USB device hardware failure, and so on.	The firmware download times out, and a commit is started to repair the affected partitions of the CPUs.	None.
The USB device is not enabled.	The firmware download fails with an error message.	Enable the USB device using the `usbstorage -e` command, and retry firmware download.

Considerations for Downgrading Firmware

The pre-installation check of the `firmwaredownload` command detects all blocking conditions that can prevent a successful downgrade, and it warns you about all these conditions. The error messages displayed by the `firmwaredownload` command state the blocking conditions and the corresponding commands to correct them. You must address all these blocking conditions before proceeding. Refer to the *Brocade Fabric OS Administration Guide* for more information regarding individual features and commands.

To avoid failure of a firmware downgrade, verify that the firmware you are downgrading to supports all blades in the chassis and that the switch, blades, or chassis supports all features that you are currently using. If not, you must disable or remove those features that are not supported.

Preinstallation Messages

NOTE
The system messages in this section are for illustration purposes only. They do not represent the entire range of possible error messages appropriate to a wide variety of installation scenarios.

The system messages in this section may be displayed if an exception is encountered during firmware download. For example, the following message is displayed when you upgrade from Fabric OS v9.0.x to 9.2.0:

```
Cannot upgrade directly to 9.2.x. Please upgrade to 9.1.x or higher first and then upgrade to 9.2.x
```

The following examples show feature-related messages that you may see if you upgrade to Fabric OS v9.2.0 or downgrade from Fabric OS v9.2.0:

```
Cannot downgrade to 9.0.x or lower. Please downgrade to 9.1.x first and then download the desired firmware
 version

Cannot upgrade directly to 9.2.x. Please upgrade to 9.1.x or higher first and then upgrade to 9.2.x

Non disruptive firmwaredownload is not supported when firmwaredownload with two versions apart. Please try to
 use \"firmwaredownload\" with single mode option enabled.

Non disruptive firmwaredownload is not supported when firmwaredownload with two versions apart. Disruptive
 firmware download is disallowed when auto-boot option is enabled. Please disable auto-boot and try again.

Firmwaredownload is not allowed since the switchState is Faulty. Use "switchShow" to see the switch state.
 Please recover the switch before proceeding.

Firmwaredownload is not allowed because some extension features did not pass firmwaredownload pre-checks (see
 above). Please address these issues before proceeding.

There are extension certificates, CSRs, or private keys whose filenames have unsupported characters. Supported
 characters are as follows:a-zA-Z0-9~@%_+:-Please use the cli "seccertmgmt delete" to delete these files and
 then recreate them before upgrading to v8.2.1 or higher.

The following item(s) need to be addressed before downloading the specified firmware:
Error: Firmwaredownload is not allowed as the authentication protocol SHA512 is configured for snmpv3 users.
 Please reconfigure the user with SHA/MD5 using "snmpconfig --set snmpv3" or delete the corresponding user
 before downgrade.

In MAPS, user-defined rules are present for IP_EXTN_FLOW. These rules will not be monitored in pre-8.2.0 FOS
 version.
```

TruFOS Validation

From the Fabric OS v9.1.0 release, Trusted FOS (TruFOS) Certificate validation is enforced. Any firmware upgrade from 9.1.0 to any firmware or from any firmware to 9.1.0 will enforce TruFOS validation. A valid TruFOS certificate must be installed on the system to upgrade the firmware.

If the `firmwaredownload` command is executed without the proper TruFOS validation, the following error message is displayed:

```
Firmwaredownload failed. TruFOS certificate validation Failed or validation tool failed
```

NOTE
An expired TruFOS cannot be installed. If TruFOS is expired, the switch will be marginal, and another TruFOS Certificate must be installed to clear the marginal state.

Support for Firmware Patch

From the Fabric OS v9.2.0 release, the firmware patch feature is supported. This allows the switch to update the firmware by applying a patch on top of the current firmware using the `firmwarepatch` command.

Fabric OS Compatibility Considerations:

Below are the limitations that need to be considered during the firmware installation:

- The patch package is installed only on the local CP and multiple patch installation is not supported.
- During the firmware upgrade or downgrade process, you need to check if the downloaded firmware is compatible with the patch. If it is in the exception list, then remove the patch applied on the switch before proceeding with the firmware download.
- When a new firmware version is uploaded, the patch updated files are overwritten and will be removed during the post install script execution process.

Blade Types

Where blades are incompatible with a firmware download, they must be removed or powered off before a firmware download begins, as noted in the following table.

Table 23: Issues Related to Blade Types

Message	Probable Cause and Recommended Action
`Downgrade is not allowed as FC64-64 blade is present. Please remove the blade and retry firmwaredowngrade.`	An attempt was made to downgrade a system running Fabric OS 9.2.x to 9.1.0 with Brocade FC64-64 blades installed. Since the blade is already present in the Fabric OS9.2.0, the firmware download operation will fail. Use the `slotshow` command to display which slots these blades occupy. Physically remove the blades from the chassis, and then retry the firmware download operation.

SFP Blocking Conditions

When SFP types are incompatible with a firmware download, they must be removed before a firmware download begins and a retry operation must be performed. From Fabric OS 9.1.1, there are some SFP types that block firmware downgrading to previous releases.

The following are examples of messages that are related to incompatible SFPs, when downgrading and resolution steps to perform before reissuing the firmware download.

- Firmware migration is not allowed since the 64G LWL secure SFP is not supported. Remove the 64G LWL secure SFP and retry `firmwaredownload`. The SFP is present on ports 0, 1, 2, and 3.
- Firmware migration is not allowed since the 64G ELWL secure SFP is not supported. Remove the 64G ELWL secure SFP and retry `firmwaredownload`. The SFP is present on ports 8 and 9.
- Firmware migration is not allowed since the 32G ELWL secure SFP is not supported. Remove the 32G ELWL secure SFP and retry `firmwaredownload`. The SFP is present on ports 10, 11, and 12.
- Downgrading is not allowed since the 64G SFP is present on ports 41,42. Remove the 64G SFP and retry `firmwaredownload`.

Firmware Versions

The system messages in this section refer to the differences between the current firmware and the firmware that you are applying to the switch.

The following information should be considered regarding firmware upgrades and downgrades for Fabric OS 9.2.0:

- Both disruptive and non-disruptive direct upgrades and downgrades from Fabric OS v9.0.x to Fabric OS v9.2.0 are not supported. Migrate to Fabric OS v9.1.x first.
- Non-disruptive upgrades from Fabric OS v9.0.x or 9.1.x to Fabric OS v9.2.0 are a two-step process: first upgrade to 9.1.x and then upgrade to 9.2.0.
- Use `firmwaredownload -s` for upgrades and the `-s` option is disruptive to switch traffic.

Refer to the current *Brocade Fabric OS Software Upgrade Guide* for details on firmware download options. The “Supported Upgrade Paths” section of this guide provides details on upgrading between Fabric OS v9.0.x and 9.2.0.

> **NOTE**
> The firmware upgrade and downgrade guidelines described in these sections are generally applicable for most releases. Users are advised to always refer to the Fabric OS release notes for the most current upgrade and downgrade information.

The following table covers firmware version-related issues.

Table 24: Issues Related to Firmware Versions

Message	Probable Cause and Recommended Action
`Cannot upgrade directly to 9.2.x. Please upgrade to 9.1.x or higher first and then upgrade to 9.2.x`	An attempt was made to upgrade to Fabric OS v9.2.0 from a version earlier than 9.1.x. If the switch is running Fabric OS v9.0.x, you are not allowed to upgrade directly to 9.2.0. Upgrade your switch to Fabric OS version 9.1.x before upgrading to 9.2.0.
`Cannot downgrade to 9.0.x or lower. Please downgrade to 9.1.x first and then download the desired firmware version.`	An attempt was made to downgrade from Fabric OS v9.2.0 to 9.0.x or lower. If the switch is running Fabric OS v9.2.0, you are not allowed to downgrade directly to 9.0.x or lower. Downgrade your switch to Fabric OS v9.1.x first, and then downgrade to the desired firmware version.

Security

User Account Management

The most common error when managing user accounts is not setting up Role-Based Access Control (RBAC). Errors such as a user not being able to run a command or modify switch settings are usually related to what role the user has been assigned. If a user is unable to modify switch settings, check the RBAC permissions for that user.

Password Issues

The following table describes various ways to recover forgotten passwords.

Table 25: Issues Related to Passwords

Symptom	Probable Cause and Recommended Action
The user forgot the password.	If you do not know the password, you must contact your service support provider to recover admin passwords.
The user cannot log in to the boot PROM.	To recover a lost boot PROM password, contact your switch service provider. You must have previously set a recovery string to recover the boot PROM password. This does not work on lost or forgotten passwords in the account database.

NOTE
For Gen 7 and Gen 6 switches loaded with 9.1.0 or later, secure-boot-enabled systems, you do not require a password to enter the Boot PROM CLI. This is because all legacy Boot PROM CLI commands are disabled in secure boot mode. You are allowed to use `sboot fospasswdreset` to reset or recover the password if the password is lost.

Password Recovery Options

The following table describes the options available when one or more types of passwords are lost.

Table 26: Password Recovery Options

Topic	Solution
If all the passwords are forgotten, what is the password recovery mechanism? Are these procedures nondisruptive recovery procedures?	Contact your switch service provider. A nondisruptive procedure is possibly available.
How to recover a boot PROM password?	Contact your switch service provider and provide the recovery string.
How to recover a user or admin password?	See Password Issues for more information on recovering these passwords.

Device Authentication

The following table covers device authentication issues.

Table 27: Issues Related to Device Authentication

Symptom	Probable Cause and Recommended Action
The switch is unable to authenticate the device.	Issue: When the device authentication policy is set to ON, the switch expects a FLOGI with the FC-SP bit set. If this bit is not set, the switch rejects the FLOGI with reason LS_LOGICAL_ERROR (0x03) in the switch log with the explanation of `Authentication Required` (0x48), and it disables the port. Solution: Turn on the authentication in the device (by default the device authentication policy in the switch is already ON). If the device is not capable of doing authentication, set the device authentication policy in the switch to OFF to bring up the port without authentication.
The switch is unable to form an F_Port.	Regardless of the device authentication policy mode on the switch, the F_Port is disabled if the DH-CHAP protocol fails to authenticate. If the HBA sets the FC-SP bit during FLOGI and the switch sends a FLOGI accept with the FC-SP bit set, then the switch expects the HBA to start the AUTH_NEGOTIATE. From this point forward until the AUTH_NEGOTIATE is completed, all ELS and CT frames, except the AUTH_NEGOTIATE ELS frame, are blocked by the switch. During this time, the Fibre Channel driver rejects all other ELS frames. The F_Port does not form until the AUTH_NEGOTIATE is completed. It is the HBA's responsibility to send an Authentication Negotiation ELS frame after receiving the FLOGI accept frame with the FC-SP bit set.

Protocol and Certificate Management

This section provides information and procedures for troubleshooting standard Fabric OS security features such as protocol and certificate management.

If you receive messages in the browser or in a popup when logging in to the target switch using HTTPS, see the following table for actions that you can take to correct the problem.

NOTE
Do not use DSA and md5 certificates for certificate signing.

The following table covers SSL messages and related actions.

Table 28: SSL Messages and Actions

Message	Action
`The page cannot be displayed.`	Issue: The SSL certificate is not installed correctly, or HTTPS is not enabled correctly. Solution: Make sure that the certificate has not expired, that HTTPS is enabled, and that certificate file names are configured correctly.
`The security certificate was issued by a company you have not chosen to trust.`	The certificate is not installed in the browser. Install it as described in the *Brocade Fabric OS Administration Guide*.
`The security certificate has expired or is not yet valid.`	Issue: Either the certificate file is corrupted or it needs to be updated. Solution: Click **View Certificate** to verify the certificate content. If it is corrupted or out of date, obtain and install a new certificate.
`The name on the security certificate is invalid or does not match the name of the site file.`	Issue: The certificate is not installed. Solution: Install it as described in the *Brocade Fabric OS Administration Guide*.

Message	Action
`This page contains both secure and nonsecure items. Do you want to display the nonsecure items?`	Issue: The page contains both secure and nonsecure items. Solution: Click **No** in this popup. The session opens with a closed lock icon on the lower-right corner of the browser, indicating an encrypted connection.
`Invalid cipher. Web server failed to restart.`	Issue: Indicates that the HTTPS certificates are present, but they have not been created. Solution: The certificate type and the configured ciphers need to be aligned to permit connections to the switch.

Generating and Storing a Certificate Signing Request

This feature allows you to generate and store a certificate signing request (CSR) with HTTPS as an example. Generating a new CSR will not remove the installed certificate and key to maintain the HTTPS state. The key and the certificate will be replaced when the newly signed certificate is imported. For more information on generating and storing a certificate signing request, refer to the *Brocade Fabric OS Administration Guide*.

Gathering Additional Information

For security-related issues, use the following guidelines to gather additional data for your switch support provider.

- Use the `supportSave -n` command.
- If not sure about the problem area, use `supportSave -n` to collect data from all switches in the fabric.
- If you think it may be related to E_Port authentication, use the `supportSave -n` command to collect data from both switches of the affected E_Port.
- If you think this is a policy-related issue, FCS switch, or other security server-related issue, then use `supportSave -n` to collect data from the primary FCS switch and all affected switches.
- If login-related, then also include the following information:
  - Does the login problem appear on a serial, CP IP, or switch IP address connection?
  - Is it CP0 or CP1?
  - Is the CP in active or standby?
  - Is it the first time login after `firmwareDownload` and reboot?

SNMP Issues

This table describes symptoms with associated causes and recommended actions for SNMP-related issues.

Table 29: Issues Related to SNMP

Symptom	Probable Cause and Recommended Action
The SNMP management station server is unable to receive traps from the fabric.	There are several causes related to this generic issue. You must verify the following: • There are no port filters in the firewalls between the fabric and the SNMP management station. • If your SNMP management station is a dual-homed server, check that the routing tables are set up correctly for your network. If you continue to have problems, run `supportsave` , gather that output along with a MIB browser snapshot of the problem (like an Adventnet screen snapshot) for a MIB variable, and contact your switch support provider.

FIPS

The following table describes symptoms and associated causes and recommended actions for problems related to FIPS.

Table 30: Issues Related to FIPS

Symptom	Probable Cause and Recommended Action
When FIPS is turned on, the switch constantly reboots.	When FIPS is turned on, the switch runs conditional tests each time it is rebooted. These tests run random number generators and are executed to verify the randomness of the random number generator. The conditional tests are executed each time before the random number provided by the random number generator is used. The results of all self-tests, for both power-up and conditional, are recorded in the system log or are output to the local console. This includes logging both passing and failing results. If the tests fail on your switch, the switch may go into a reboot loop because the cryptography of the switch can no longer be validated or trusted. In this case, the switch would have to be recovered by reinstalling of Fabric OS.

Virtual Fabrics

General Virtual Fabrics Troubleshooting

All of the following constraints apply when the Virtual Fabrics feature is enabled:

- The base fabric works only in Brocade native mode, not in an interoperable mode.
- The base switch does not have any devices. The base fabric can have devices in remote Layer 2 switches; traffic between those devices is supported.
- Only one base switch can be configured per Virtual Fabric.
- Since an individual base switch cannot have devices, the entire base fabric does not have any devices as well. The devices can be in other logical partitions that are configured on the same switch or remote switches.
- A nonbase switch in a Virtual Fabrics-capable chassis must not be part of a fabric that serves as a base fabric for some other logical fabric traffic. Although software does not detect or prevent users from deploying such a configuration, such a configuration is not supported.
- ICL ports can be in the base or default switch only. If the extended ISL (XISL) is turned off, you can connect ICLs to other logical switches.
- A default switch can be configured as a base switch in fixed-port switches, but not in a Brocade backbone. The fabric IDs of default switches cannot be manually changed.
- The default switch can participate in a logical fabric using XISLs. In Brocade backbones, the default switch does not participate in a logical fabric and is a purely Layer 2 logical switch.
- EX_Ports are supported in the base switch and cannot be part of any other switch other than the base switch.
- EX_Ports cannot connect to a fabric that has a logical switch with the Allow XISL use mode on. The port is disabled with the reason "Conflict: XISL capability domain."
- External device sharing is supported through EX_Ports. Internal device sharing (sharing a device in a logical fabric with other fabrics without having an EX_Port) is not supported.
- A logical fabric cannot have EX_Ports that use XISLs and cannot serve as a backbone to any EX_Port traffic. Similarly, the default switch cannot be part of a fabric that serves as a backbone to any EX_Port traffic.
- Traffic Isolation (TI) zones with no failover option are not supported in logical fabrics. TI zones defined in the base fabric for logical fabric traffic must allow failover. (Traffic Isolation (TI) is not supported from FOS 9.1.0 and later).

NOTE
The `configure` command has a "Disable FID check" fabric parameter option, which can be used to disable the FID check for FICON logical switches.

Fabric Identification Issues

The following table covers fabric identification issues.

Table 31: Issues Related to Fabric Identification

Symptom	Probable Cause and Recommended Action
E_Ports that directly connect two logical switches do not form or are disabled.	The FIDs on each of the logical switches must be the same. Enter `lscfg --show` to view the current FIDs on the chassis, and then enter `lscfg --change -newfid` to change the FID.
Invalid FID.	FIDs for switches may be from 1 through 128 as long as they are not already in use, except for EX_Ports, which are assigned FIDs from 1 through 127 only. Enter `lscfg --show` to verify whether the FID is in use. If it is, use another FID.

Symptom	Probable Cause and Recommended Action
The FID is currently in use.	You may not create two or more logical switches with the same FID. Use the `lscfg--show` and `fcrfabricshow` commands to view FIDs in use.

Logical Fabric Issues

The following table covers logical fabric issues.

Table 32: Issues Related to Logical Fabrics

Symptom	Probable Cause and Recommended Action
Logical port <port_number> disabled.	This message indicates that an Logical ISL (LISL) was disabled because of some protocol conflict or security or policy violation. This can result in possible traffic issues. You should resolve the cause of the conflict and re-enable the LISL by entering `lfcfg --lislenable`.
The switch with domain <domain> with firmware version <fw_version> has joined the FID <fid> fabric and may not be compatible with XISL use.	This message indicates the specified switch in the logical fabric that is using XISLs is running an incompatible firmware version and must be upgraded to Fabric OS 6.2.0 or later.
Logical port segmented.	Ensure that the fabwide policy, zoning, and defzone settings are consistent on the logical switches to be joined.

Base Switch Issues

All logical switches in a fabric should have the same base switch attribute. If a base switch is connected to a nonbase switch, you must take the appropriate action to resolve the conflict.

The following table covers base-switch-related issues.

Table 33: Issues Related to Base Switches

Symptom	Probable Cause and Recommended Action
EX_Port is disabled with reason "Export in non base switch."	An EX_Port must be in the base switch. 1. Enter `lscfg --create -b` to create a base switch. 2. Enter `lscfg --config -slot -port` to move the port to the base switch. 3. If the port is not intended to be used as an EX_Port, enter `portcfgdefault` to reset the port to its default configuration.
An EX_ or VEX_Port is disabled with reason "Conflict: XISL capability domain."	Use the `configure` command to set “Allow XISL use” to OFF on all logical switches in the connecting edge fabric.
E_Ports connecting two logical switches are disabled.	If a base switch is directly connected to a nonbase switch, all E_Ports to that logical switch are disabled.
The fabric ID and base switch are conflicted.	If there is a fabric ID conflict and a base switch conflict that exist between two switches, the fabric ID conflict is detected first. Enter `lscfg --change -newfid` to change the FID.
A base switch already exists on this system.	Only one base switch is allowed on a platform. To remove the current base switch and then create a new one, complete the following steps. 1. Enter `lscfg --delete`. 2. Enter `lscfg --create -b`.

Logical Switch Issues

CAUTION
When a logical switch is created, all configuration for the logical switch is set to factory defaults. When a logical switch is deleted, all configuration for the logical switch is deleted permanently and is not recoverable.

The following table covers logical switch issues.

Table 34: Issues Related to Logical Switches

Symptom	Probable Cause and Recommended Action
The indicated slot is empty.	When `lscfg` was run, an empty slot was specified. Re-issue the command with the appropriate slot number.
Validation of switch configuration changes is not supported on this platform.	This platform is unknown to the logical switch subsystem.
The given slot number is not valid on this platform.	You are specifying a slot number that is not valid on the platform, for example, slot 0 on a Brocade X6-8 or slot 12 on a Brocade X6-4.
A slot must be enabled to configure ports.	You may attempt to configure ports only on enabled blades (blades may be faulted).
Unable to determine the slot type.	The slot type is not known to the logical switch. Verify the slot and try again.
There are no ports on this slot.	There are no configurable ports on the slot indicated by the `lscfg` command. Verify the ports and try again.
Unable to remove ports from their current switch.	When moving ports to a switch, you must first remove them from the switch in which they reside. This error message is displayed if this step fails.
A non-GE blade is within the slot range.	You are attempting to configure a Gigabit Ethernet (GE) port on a slot that does not contain GE ports.
A port or ports are already in the current switch.	You may not move a port to the same switch.
The maximum number of switches for this platform has been reached.	Each platform that supports Virtual Fabrics has a maximum number of supported logical switches. The platform has reached this limit. Director platforms support eight logical switches and fixed-port switches support four logical switches.
Unable to create the switch.	There was an error while creating the switch.
A port or ports cannot be moved to the requested switch because it would exceed the 256 area limit for this switch.	The area limit would be exceeded if the `lscfg` command were allowed.
A port or ports cannot be moved to the requested switch because it may exist only in a base or default switch.	You are attempting to move ports on a core blade into a non default or non base switch.

Switch Configuration Blade Compatibility

The following table covers switch configuration blade compatibility issues.

Table 35: Issues Related to Switch Configuration Blade Compatibility

Symptom	Probable Cause and Recommended Action

A slot in the chassis displays FAULTY(91) in the `slotshow` output.	When an enterprise-class platform comes up or when a blade is inserted, the switch configuration is checked based on the blade type. If the configuration does not match the blade type, the blade is faulted. This is displayed as FAULTY(91) in the output of the `slotshow` command.
	Enter `lscfg -restore_slot_to_default` to correct the problem.
	Once the configuration discrepancy has been fixed, enter `slotpoweroff` followed by `slotpoweron` to recover.
	The following example shows this procedure.
	`device:admin > lscfg -restore_slot_to_default 1`
	`device:admin >slotpoweroff 1`
	`device:admin >slotpoweron 1`
	`Slot Blade Type ID Model Name Status`
	`----------------------------------------------`
	`2 SW BLADE 97 FC16-32 ENABLED`
	`3 SW BLADE 96 FC16-48 ENABLED`
	`4 SW BLADE 96 FC16-48 ENABLED`
	`5 CORE BLADE 98 CR16-8 ENABLED`
	`6 CP BLADE 50 CP8 ENABLED`
	`7 CP BLADE 50 CP8 ENABLED`
	`8 CORE BLADE 98 CR16-8 ENABLED`
	`10 SW BLADE 96 FC16-48 ENABLED`
	`11 AP BLADE 75 FX8-24 ENABLED`
	`12 SW BLADE 97 FC16-32 ENABLED`

Gathering Additional Information

For Virtual Fabrics-related issues, use the following guidelines to gather additional data for your switch support provider:

- Use the `supportSave` command.
- If you are not sure about the problem area, use the `supportSave` command on all chassis and logical switches in the fabric.
- If you think the issue may be related to E_Port authentication, use the `supportSave -n` command on both switches or logical switches of the affected E_Port.

ISL Trunking

Trunking Link Issues

This section describes trunking link issues that can arise and the recommended actions to correct the problems.

You can use the `islshow` command to find the incompatible and segmented ISL links. To know the reason for incompatibility and segmentation, use the `switchshow` command on both ends of the ISL link.

The following table covers trunking link-related issues.

Table 36: Issues Related to Trunking Links

Symptom	Probable Cause and Recommended Action

A link that is part of an ISL trunk failed.	Use the `trunkdebug` command to troubleshoot the problem, as shown in the following procedure.
	1. Connect to the switch and log in as admin.
	2. Enter `trunkdebug` *`port_1 port_2`*.
	— *port_1* - The area number or index of port 1.
	— *port_2* - The area number or index of port 2.
	Use the `switchshow` command to determine the area or index numbers for the port values. Both operands are required.
	This example shows that port 3 is not configured as an E_Port:
	`device:admin> trunkdebug 126, 127`
	`port 126 is not E/EX port`
	`port 127 is not E/EX port`
	This example shows that port 3 is configured as an E_Port:
	`device:admin> trunkdebug 100, 101`
	`port 100 and 101 connect to the switch 10:00:00:05:1e:34:02:45`
	The `trunkdebug` command displays the possible reason that two ports cannot be trunked. Possible reasons are:
	• The switch does not support trunking.
	• A trunking license is required.
	• Trunking is not supported in switch interoperability mode.
	• Port trunking is disabled.
	• The port is not an E_Port.
	• The port is not 2G, 4G, 8G, 10G, or 16G.
	• The port connects to a switch other than the one you want.
	To correct this issue, connect additional ISLs to the switch with which you want to communicate.
	• The ports are not the same speed or they are set to an invalid speed.
	Manually set port speeds to a speed that is supported on both sides of the trunk.
	• The ports are not set to the same long-distance mode.
	Set the long-distance mode to the same setting on all ports on both sides of the trunk.
	• Local or remote ports are not in the same port group.
	Move all ISLs to the same port group. The port groups begin at port 0 and are in groups of four or eight, depending on the switch model. Until this is done, the ISLs do not trunk.
	• The difference in the cable length among trunked links is greater than the allowed difference.

Buffer Credit Issues

This table describes the issues related to a trunk bouncing online and offline or hosts not being able to talk to a storage device.

Table 37: Issues Related to Buffer Credits

Symptom	Probable Cause and Recommended Action
Trunk goes offline and online (bounces).	A port that is disabled at one end because of buffer under allocation causes all disabled ports at the other end to become enabled. Some of these enabled ports become disabled because of a lack of buffers, which in turn triggers ports to be enabled once again at the other end. While the system is stabilizing the buffer allocation, it warns that ports are disabled because of a lack of buffers, but it does not send a message to the console when buffers are enabled. The system requires a few passes to stabilize the buffer allocation. Ultimately, the number of ports for which buffers are available come up and stabilize. You should wait for stabilization and then proceed with correcting the buffer allocation situation.

Getting Out of Buffer-Limited Mode

Perform any of the following actions to get out of buffer-limited mode when occurs on LD_Ports:

- Change the LD port speed to a lower speed (of non buffer limited ports).
- Change the LD port's estimated distance to a shorter distance (of non buffer limited ports).
- Change LD back to L0 (of non buffer limited ports).
- If you are in buffer-limited mode on the LD port, increase the estimated distance.
- Enable any of these changes on the buffer-limited port or switch by issuing the commands `portDisable` and `portEnable` .

Zoning

Zoning Corrective Action

The following overview provides a basic starting point to troubleshoot your zoning problem.

1. Verify that you have a zone problem.
2. Determine the nature of the zone conflict.
3. Take the appropriate steps to correct the zone conflict.

   To correct a merge conflict without disrupting the fabric, first verify that it was a fabric merge problem, then edit the zone configuration members, and then reorder the zone member list if necessary.

   The newly changed zone configuration is not effective until you issue the `cfgEnable` command. This should be done during a maintenance window because it may cause disruption in large fabrics.

Verifying a Fabric Merge Problem

1. Enter the `switchShow` command to validate that the segmentation is due to a zone issue.
2. Review Segmented Fabrics to view the different types of zone discrepancies and determine what might be causing the conflict.

Segmented Fabrics

This section discusses fabric segmentation. Fabric segmentation occurs when two or more switches are joined by ISLs and do not communicate to each other. Each switch appears as a separate fabric when you use the `fabricshow` command.

Table 38: Issues Related to Fabric Segmentation

Symptom	Probable Cause and Recommended Action
Port gets segmented due to a zone conflict.	Occurs even when one of the following is true. • Zoning is enabled in both fabrics, and the zone configurations are different in each fabric. • The name of a zone object in one fabric is also used for a different type of zone object in the other fabric. A zone object is any device in a zone. • The definition in one fabric is different from the definition of a zone object with the same name in the other fabric. To resolve the conflict, ensure that the following are true: • The effective cfg (zone set) on each end of the segmented ISL is identical. • Any zone object with the same name has the same entries in the same sequence.
Fabric segmentation is caused by a "configuration mismatch."	Occurs when zoning is enabled in both fabrics and the zone configurations are different in each fabric.
Fabric segmentation is caused by a "type mismatch."	Occurs when the name of a zone object in one fabric is also used for a different type of zone object in the other fabric. A zone object is any device in a zone.
Fabric segmentation is caused by a "content mismatch."	Occurs when the definition in one fabric is different from the definition of a zone object with the same name in the other fabric.

Zone Conflicts

To resolve zone conflicts, users should examine the zone database contents on each switch and should determine what zone objects are in conflict. Once the conflicts are determined, users must edit the zoning database on one of the switches until all conflicts are resolved. Once resolved, users can reattempt to merge the switches by toggling the ISL.

In cases where determining the zone conflicts might be difficult or cumbersome, users may opt to resolve such conflicts by clearing the zone database on one of the conflicting switches and having that switch (or fabric) import the desired zone database from an existing switch (or fabric). Note that this method of zone conflict recovery could result in loss of connectivity for any devices that are currently connected to the switch (or fabric) that is being cleared of its zone database.

To perform this method of recovery, please see the Correcting a Fabric Merge Problem Quickly section.

TheTable summarizes commands that are useful for debugging zoning issues.

Table 39: Commands for Debugging Zoning

Command	Function
`aliadd`	Use to add members to a zone alias.
`alicreate`	Use to create a zone alias.
`alidelete`	Use to delete a zone alias.
`aliremove`	Use to remove members from a zone alias.
`alishow`	Use to display zone aliases.
`cfgadd`	Use to add zone members to a zone configuration.
`cfgclear`	Use to clear the zoning database.
`cfgcreate`	Use to create a zone configuration.
`cfgdelete`	Use to delete the zone configuration.
`cfgdisable`	Disables the active (effective) configuration.
`cfgenable`	Enable and Activate (make effective) the specified configuration.
`cfgremove`	Use to remove zone members from a zone configuration.
`cfgsave`	Use to save changes to the zone configuration database.
`cfgshow`	Displays the zoning configuration.
`cfgsize`	Use to display the zone database size.
`cfgtransabort`	Use to abort the current zoning transaction without committing it.
`cfgtransshow`	Use to display the ID of the current zoning transaction.
`defzone --noaccess`	Sets the default zone access mode to No Access, initializes a zoning transaction (if one is not already in progress), and creates the reserved zoning objects.
`license --show`	Displays current license keys and associated (licensed) products.
`switchshow`	Displays currently enabled configuration and any E_Port segmentations resulting from zone conflicts.
`zoneadd`	Use to add a member to an existing zone.
`zonecreate`	Use to create a zone. Before a zone becomes active, the `cfgsave` and `cfgenable` commands must be used.
`zonedelete`	Use to delete zones.
`zonehelp`	Displays help information for zone commands.
`zoneremove`	Use to remove zone member aliases from the zone database.
`zoneshow`	Displays zone information.

For more information about setting up zoning on your switch, refer to the *Brocade Fabric OS Administration Guide*.

Correcting a Fabric Merge Problem Quickly

If there are devices attached to the switches on which you need to perform these recovery steps, ensure that these switches are in DefZone NoAccess so as not to cause any RSCN storms and bog down the NameServer.

1. Determine which switches have the incorrect zoning configuration; then log in to the switches as admin.
2. Enter the `switchDisable` command on all problem switches.
3. Enter the `cfgDisable` command on each switch.
4. Enter the `cfgClear` command on each switch.
5. Enter the `cfgSave` command on each switch to commit the change.

   ATTENTION

   The `cfgClear` command clears the zoning database on the switch where the command is run.
6. Enter the `switchEnable` command on each switch once the zoning configuration has been cleared.

   This forces the zones to merge and populates the switches with the correct zoning database. The fabrics then merge.

Changing the Default Zone Access

Sometimes, a zone conflict can be attributed to a mismatch of the default zone mode. One example is if an existing switch (or fabric) has an enabled zone configuration with a default zone mode set to "all access" and a new switch having no zone objects with a default zone mode set to "no access". In this case, the suggested recovery modifies the default zone mode of the existing switch to "no access" and retry the merge. The steps to modify the default zone mode are as follows:

1. Connect to the switch and log in using an account with admin permissions.
2. Display the current default zone mode setting by using the `defZone --show` command.
3. Modify the default zone mode setting by issuing the `defZone --<allaccess | noaccess>` command to change the default zone.
4. Enter the `cfgSave` command to save the current configuration.

Editing Zone Configuration Members

1. Log in as admin to one of the switches in a segmented fabric.
2. Enter the `cfgShow` command and print the output.
3. Start another Telnet session and connect to the next fabric as an admin.
4. Enter the `cfgShow` command and print the output.
5. Compare the two fabric zone configurations line by line and look for an incompatible configuration.
6. Connect to one of the fabrics.
7. Run zone configure commands to edit the fabric zone configuration for the segmented switch (see Zone Conflicts for specific commands).

   If the zoneset members between two switches are not listed in the same order in both configurations, the configurations are considered a mismatch, resulting in the switches being segmented in the fabric.

   For example:

   [cfg1 = z1; z2] is different from [cfg1 = z2; z1], even though the members of the configuration are the same.

NOTE
For FOS 9.0 switch sorting is done automatically. Two switches having 9.0.0 and same configuration objects created or updated locally with members in any order will always merge successfully. The Fabric segmentation due to sort-order conflict can occur if there are any zone transaction done from the low-level switches in the fabric (earlier than v9.0.0).

Reordering the Zone Member List

1. Obtain the output from the `cfgShow` command for both switches.
2. Compare the order in which the zone members are listed. Members must be listed in the same order.
3. Rearrange zone members so that the configuration for both switches is the same. Arrange zone members in alphabetical order, if possible.

Checking for Fibre Channel Connectivity Problems

Enter the `fcPing` command to:

- Generate an Extended Link Service (ELS) frame ECHO request to the source port specified, and validate the response.
- Generate an ELS ECHO request to the destination port specified, and validate the response.

Regardless of the device's zoning, the `fcPing` command sends the ELS frame to the destination port. A device can take any of the following actions:

- Send an ELS Accept to the ELS request.
- Send an ELS Reject to the ELS request.
- Ignore the ELS request.

Some devices do not support the ELS ECHO request. In these cases, the device either does not respond to the request or sends an ELS reject. When a device does not respond to the ELS request, further debugging is required and it can be done with a help of an analyzer. However, do not assume that the device is not connected to the Fibre Channel.

The following example is sample output from the `fcPing` command in which one device accepts the request and another device rejects the request:

```
switch:admin> fcping 10:00:00:00:c9:29:0e:c4 21:00:00:20:37:25:ad:05
Source:      10:00:00:00:c9:29:0e:c4
Destination: 21:00:00:20:37:25:ad:05
Zone Check:  Not Zoned
Pinging 10:00:00:00:c9:29:0e:c4 [0x20800] with 12 bytes of date:
received reply from 10:00:00:00:c9:29:0e:c4: 12 bytes time:1162 usec
received reply from 10:00:00:00:c9:29:0e:c4: 12 bytes time:1013 usec
received reply from 10:00:00:00:c9:29:0e:c4: 12 bytes time:1442 usec
received reply from 10:00:00:00:c9:29:0e:c4: 12 bytes time:1052 usec
received reply from 10:00:00:00:c9:29:0e:c4: 12 bytes time:1012 usec
5 frames sent, 5 frames received, 0 frames rejected, 0 frames timeout
Round-trip min/avg/max = 1012/1136/1442 usec
Pinging 21:00:00:20:37:25:ad:05 [0x211e8] with 12 bytes of data:
Request rejected
Request rejected
Request rejected
Request rejected
Request rejected
5 frames sent, 0 frames received, 5 frames rejected, 0 frames timeout
```

```
Round-trip min/avg/max = 0/0/0 usec
```

The following example is sample output from the `fcPing` command in which one device accepts the request and another device does not respond to the request:

```
switch:admin> fcping 0x020800 22:00:00:04:cf:75:63:85
Source:      0x20800
Destination: 22:00:00:04:cf:75:63:85
Zone Check:  Zoned
Pinging 0x020800 with 12 bytes of data:
received reply from 0x020800: 12 bytes time:1159 usec
received reply from 0x020800: 12 bytes time:1006 usec
received reply from 0x020800: 12 bytes time:1008 usec
received reply from 0x020800: 12 bytes time:1038 usec
received reply from 0x020800: 12 bytes time:1010 usec
5 frames sent, 5 frames received, 0 frames rejected, 0 frames timeout
Round-trip min/avg/max = 1006/1044/1159 usec
Pinging 22:00:00:04:cf:75:63:85 [0x217d9] with 12 bytes of data:
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
5 frames sent, 0 frames received, 0 frames rejected, 5 frames timeout
Round-trip min/avg/max = 0/0/0 usec
```

Checking for Zoning Problems

1. Enter the `cfgActvShow` command to determine if zoning is enabled.
   - If zoning is enabled, the problem may be caused by zoning enforcement (for example, two devices in different zones cannot detect each other).
   - If zoning is disabled:
     – The first recommended course of action is to configure and activate a zone configuration containing the devices that are unable to communicate.
     – If for some reason, configuring and activating a zone configuration is not desired, then changing the DefZone mode to AllAccess can be done to allow for device connectivity but should be done so only if the user is knowledgeable with zoning and accepts that once the AllAccess policy is made effective, that all online devices in the fabric will be able to communicate with each other. Changing the DefZone mode to AllAccess is not advisable in fabrics with a large number of online devices (over 120 devices).

       NOTE
       Changing the DefZone mode from NoAccess to AllAccess can cause an RSCN storm in the fabric and can affect switch performance especially in fabrics with a large number of online devices.
2. Confirm that the specific edge devices that must communicate with each other are in the same zone.
   - If they are not in the same zone and zoning is enabled, proceed to Step 3.
   - If they are in the same zone, perform the following tasks:

- Enter the `portCamShow` command on the host port to verify that the target is present.
- Enter the `portCamShow` command on the target port to verify that the host is present.
- Enter the `nsZoneMember` command with the port ID for the zoned devices on the host and target to determine whether the name server is aware that these devices are zoned together.

3. Resolve zoning conflicts by putting the devices into the same zoning configuration.

Gathering Additional Information

Collect the data from the `supportSave -n` command. Then collect the data from the `cfgTransShow` command. For the problematic port, collect the data from the `filterPortShow` command.

FICON

Firmware Management in a FICON Environment

You can use either the CLI, Web Tools, or Brocade SANnav Management Portal to upgrade or downgrade your Fabric OS firmware. Registered users can log in on the Broadcom website at http://www.broadcom.com and can follow the links for downloads to access firmware.

Firmware is downloaded in a .gz or .zip file. Brocade SANnav Management Portal contains built-in intelligence that unbundles the necessary files, making it unnecessary to unbundle a package. With Web Tools or the CLI, it is necessary to decompress or extract the files from the package first.

For more information, refer to the firmware download process overview in the *Brocade Fabric OS Upgrade Guide*.

Firmware Download Disruption

NOTE
Extension Hot Code Load (HCL) supports serial upgrades. The recommended practice is to perform firmware upgrades on switches at the local site, followed by upgrades on the switches at the remote site.

Downloading new firmware is not a disruptive process except in the following cases:

- During the firmware download process, a failover to the backup processor occurs. Any outstanding CUP commands are lost, which results in a timeout. To avoid this, the CUP should be set offline before starting a firmware download. The CUP may be set back online after a successful firmware download.
- The Brocade X7-4 and X7-8 chassis with the SX6 blade installed support the Extension HCL feature.
- The Brocade X6-4 and X6-8 chassis with the SX6 blade installed support the Extension HCL feature.

Nondisruptive Firmware Upload and Download

All systems maintain a primary partition and a secondary partition of nonvolatile storage areas. The following overview of the firmware download process illustrates the use of the two partitions:

1. The firmware is downloaded to the secondary partition.
2. The current secondary and primary partitions are swapped.
3. The CP then reboots. In dual-CP systems (Brocade X7 and X6 FICON directors), the backup CP is rebooted with the new firmware and an HA failover is automatically invoked.
4. Once rebooted, the primary code image is copied to the secondary partition.

Considerations for Fixed-Port Switches

Unlike director-class products, fixed-port switches have only one control processor (CP), so they behave differently during Fabric OS hot code upgrades. This can impact FICON operations if best practices are not followed.

During the code upload process, the CP reboots the operating system and reinitiates the Fabric OS. In this process, the FICON CUP may delay in responding during failover, this time is sufficiently long to result in a timeout request, and this is a disruptive operation. However, under such conditions, the FICON CUP returns a "Busy" response to the host from the time the `firmwaredownload` command is initiated until the firmware commit completes. During this time, the FICON CUP cannot fulfill any of the host requests, and most "write" operations from alternate managers are also rejected.

During this time, data traffic continues to flow uninterrupted, unless a response from the CP is required. If a response from the CP is required, for path and device validation for instance, Interface Control Checks (IFCCs) are possible. Any IFCCs should be recovered automatically by the IBM z Systems host, with no required user action.

It does not mean that the switches are not appropriate for FICON. Fully qualified FICON switch deployments continue to be sold and supported. It is important to follow the best practices of performing the firmware upgrade during scheduled maintenance windows when traffic is minimized, IFCCs can be tolerated, and the CUP is varied offline.

Configuration Restoration in a FICON Environment

The following table describes the behavior of the `configUpload` and `configDownload` commands and the IPL file function when the ASM bit is set on or off. In general, if the switch is operating in a FICON CUP environment and the ASM (Active=Saved) bit is set on, then the switch ignores the IPL file downloaded when you restore a configuration.

NOTE
In Fabric OS 9.0.0 and later, you can enable FMS mode only in a FICON logical switch. Therefore, you cannot download (`configDownload`) a configuration with FMS mode enabled in a non-FICON logical switch.

NOTE
To collect all information necessary for FICON, you must enter the `configupload` command multiple times with different command line options.

- `configupload –vf`
- `configupload -all`
- `configupload –map`

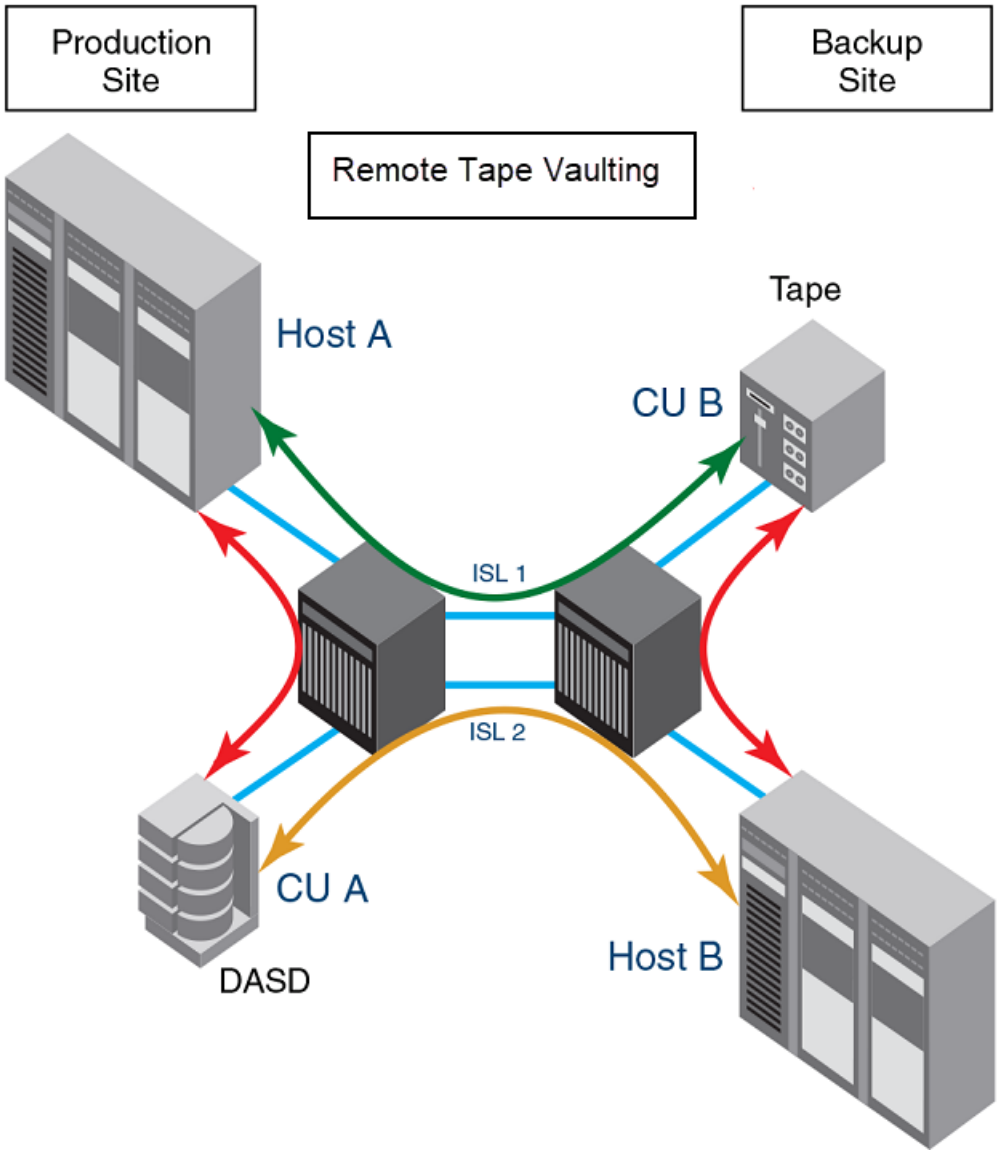
Table 40: Backup and Restoration in a FICON CUP Environment

ASM Bit	Command	Description
on or off	`configUpload`	The IPL file will be uploaded with the default **PDCM** configuration specifically, and no prohibits are present in the uploaded file. The other configuration attributes (blocked state, Port Address Names) will be retained.
on	`configDownload`	The IPL file saved on the switch that is also present in the FICON_CUP section of the configuration file will be overwritten. This overwrites with the exception that the default PDCM configuration (no prohibits) will be downloaded regardless of whether prohibits exist in the uploaded configuration. The configuration is re-established with values that may be different from the values in the switch IPL file.
off	`configDownload`	The IPL file present on the switch that is also present in the FICON_CUP section of the configuration file will be overwritten. This overwrites with the exception that the default PDCM configuration (no prohibits) will be downloaded regardless of whether prohibits exist in the uploaded configuration. The configuration is re-established with values that may be different from the values in the switch IPL file.

Remote Tape Vaulting Topology

The following figure shows a cascaded topology that can be used to support an operation's recovery site. In this environment, host and storage systems exist at both sites, which are connected by two switches cascaded together. The storage differs between the sites. In the production site, DASD storage is used to support fast access for production applications. In the backup site, tape storage is used to support archival operations for system restoration.

Figure 3: Typical Remote Tape Vaulting Topology



The host in the production site operates the application that reads data from the DASD and writes it to the remote tape. The path to the remote site must be isolated to support the bandwidth requirements needed to write the data to the remote tape. The host in the backup site needs access to the DASD in the production site to support a hot recovery scenario in the event the production host goes down. Supporting these two functions requires the ability to define overlapping zones that isolate the tape traffic from the DASD traffic and allow local access to the DASD ports.

Monitoring and Alerting Policy Suite

The Monitoring and Alerting Policy Suite (MAPS) is an optional storage area network (SAN) health monitor supported on all switches running Fabric OS7.2.0 or later. MAPS allows you to enable each switch to constantly monitor itself for potential faults and automatically alerts you to problems before they become costly failures.

MAPS tracks various SAN fabric metrics and events. Monitoring fabric-wide events, ports, and environmental parameters enable early fault detection and isolation as well as performance measurements. When using MAPS in a FICON environment, usually you should not enable the Slow-Drain Device Quarantining (SDDQ) feature. Refer to the *Brocade Monitoring and Alerting Policy Suite Administrator's Guide* for more information.

MAPS provides the following set of predefined monitoring policies that allow you to immediately use MAPS on activation:

- dflt_conservative_policy
- dflt_moderate_policy
- dflt_aggressive_policy

It is recommended that all IBM z Systems customers enable MAPS after upgrading to a Fabric OS version supporting MAPS and use the default aggressive policy (dflt_aggressive_policy). This policy contains rules with very strict thresholds. For details on enabling MAPS and monitoring policies, refer to the *Brocade Monitoring and Alerting Policy Suite Administrator's Guide*.

Port Fencing

Occasionally, bad optics and cables can cause errors to occur at such a rapid rate that error processing and RSCN transmission and processing result in fabric performance problems. Port fencing allows you to limit the number of errors that a port can receive by forcing a port offline when certain error thresholds are met.

The port fencing feature is configured through MAPS. For more information on configuring port fencing, refer to the *Brocade Monitoring and Alerting Policy Suite Administrator's Guide*.

It is recommended that you use the port decommissioning/recommissioning feature to the maximum extent possible in place of port fencing.

NOTE
As of March 2017, IBM no longer supports I/O Operations (IOOps) within Systems Automation v3.6. For additional information, refer to the IBM developerWorks wikis and search for “Important Announcement to all System Automation for z/OS I/O Operations (IOOps) users,” which provides details about port decommissioning functions and required use.

Defining Port Fencing

The following overview defines port fencing.

1. (*Optional*) Clear all alarms.
2. Define threshold levels.
3. Define the alarm action.
4. Activate alarming.

NOTE
Establish a Telnet session using a tool such as PuTTy that allows the number of columns to be increased. This is because some of the displays use more than the standard 80 columns supported by programs such as HyperTerminal. The recommended number of columns is 120.

Port Fencing Settings for FICON Environments

For typical FICON environments, port fencing is set only for CRC errors and invalid words. The default of 1000 errors per minute is a little high for CRC errors and invalid words. A more common setting is 50 errors per minute. This is high

enough to ignore occasional errors and transient errors due to recabling but low enough to stop problematic optics from causing fabric issues. By default, the alarms are set to fence the port, log an alert, send an email message, and set an SNMP trap. In most FICON environments, only fencing the port and logging the alert are desired. The following are the default thresholds:

- Low - 0
- High - 1000 errors per minute

FICON Information

You can display link incidents, registered listeners, node identification data, and FRU failures, as described in the following sections.

Link Incidents

The Registered Link Incident Report (RLIR) ELS contains the link incident information sent to a listener N_Port. To display link incidents, connect to the switch, log in as a user, and enter one of the following commands:

- For the local switch: `ficonShow rlir`
- For all switches defined in the fabric: `ficonShow rlir fabric`

Identifying Ports

The `ficonShow rlir` command displays, among other information, a tag field for the switch port. You can use this tag to identify the port on which a FICON link incident occurred. The tag field contains the port index of the switch port, in hexadecimal format. The following example shows the top portion of command output, which shows a link incident for the switch port at domain ID 120, port 93 (785d in hex):

```
switch:admin> ficonshow rlir

{
 {Fmt  Type PID    Port   Incident Count  TS Format   Time Stamp
  0x18 F    785d00   93               1  Time server Thu Apr 22 09:13:32 2004
  Port Status:          Link not operational
  Link Failure Type:    Loss of signal or synchronization
Registered Port WWN     Registered Node WWN      Flag  Node Parameters
  50:05:07:64:01:40:16:03 50:05:07:64:00:c1:69:ca  0x10  0x200115 (output truncated)
```

For complete examples of output from this command, refer to the `ficonShow` command in the *Brocade Fabric OS Command Reference*.

Registered Listeners

To display registered listeners for link incidents, connect to the switch, log in as a user, and enter one of the following commands:

- For the local switch: `ficonShow lirr`
- For all switches defined in the fabric: `ficonShow lirr fabric`

For an example of local Link Incident Record Registration (LIRR) database output, refer to the `ficonShow` command in the *Brocade Fabric OS Command Reference*.

When you configure an LIRR entry and it is current, it is marked with `-C` . If the Management Server marks an entry as current based on order, it is marked with `-C` . If the Management Server marks an entry as secondary, it is marked with `-S` . The following output is an example of output with the `-C` and `-S` flags.

```
Switch Port WWN Listener Type
20:2d:00:60:69:80:1e:4e Conditional-C
20:0d:00:60:69:80:1e:4f Conditional-S
```

If the LIRR is configured, a valid port number displays as shown in the following example.

```
Current LIRR device port number: 27 (0x1b)
```

If the LIRR is not configured, the following displays:

```
Current LIRR device port number is not configured.
```

Node Identification Data

To display node identification data, connect to the switch, log in as a user, and enter one of the following commands:

- For the local switch: `ficonShow switchrnid`
- For all switches defined in the fabric: `ficonShow switchrnid fabric`
- For all devices registered with the local switch: `ficonShow rnid`
- For all devices registered with all switches defined in the fabric: `ficonShow rnid fabric`

FRU Error Reporting

Field-replaceable unit (FRU) error information, such as FRU failures and fan and power supply removals and insertions, is stored in error reports as sense data. All FRUs in a chassis have an assigned number that is included in this data. Each CUP instance retains a database of ten FRU error reports. All error reports are sent to host LPARs that have appropriate current reporting paths established with the CUP.

Error reports are added to the database as they occur, and then they are removed when sent. If the database fills up, new reports are discarded and not delivered.

Error Data

The following examples show error data available from the host. The number identifying the failed Brocade FRU (see FRU Numbers) is derived from a single bit from byte 29 as the high-order bit and four bits from byte 30 or 31 as the low-order bits. Refer to the data marked with “vv” in the second lines of the following examples, and note that “vv” is not part of the actual output. The FRU numbers are decoded for display as the FRU names, which display in the third lines of the following examples.

```
IOS000I 1065,AB,EQC,**,8200,,,*MASTER*, 200                      vv
       1000A000000000467000100000000000000000000000000000000000008000
*IRD000E 1065,002032-001 LEVEL=1 FRU(S)=SLOT8

 IOS000I 1065,AB,EQC,**,8200,,,*MASTER*, 286                     vv
       1000A000000000467000000000000000000000000000000000000000088000
*IRD000E 1065,002032-001 LEVEL=0 FRU(S)=FAN1

 IOS000I 1065,AB,EQC,**,8200,,,*MASTER*, 461                     vv
       1000A000000000467000000000000000000000000000000000000000084000
*IRD000E 1065,002032-001 LEVEL=0 FRU(S)=PWR4

 IOS000I 1065,AB,EQC,**,8200,,,*MASTER*, 496                     vv
       1000A000000000467000000000000000000000000000000000000000089000
*IRD000E 1065,002032-001 LEVEL=0 FRU(S)=FAN2

 IOS000I 1065,AB,EQC,**,8200,,,*MASTER*, 502                     vv
```

```
       1000A0000000046700000000000000000000000000000000000000081000
 *IRD000E 1065,002032-001 LEVEL=0 FRU(S)=PWR1

  IOS000I 1065,AB,EQC,**,8200,,,*MASTER*, 568                    vv
       1000A0000000046700000000000000000000000000000000000008F000
 *IRD000E 1065,002032-001 LEVEL=0 FRU(S)=WWN-CRD

  IOS000I 1065,AB,EQC,**,8200,,,*MASTER*, 662                    vv
       1000A0000000046700010000000000000000000000000000000000A000
 *IRD000E 1065,002032-001 LEVEL=1 FRU(S)=SLOT10

  IOS000I 1061,A8,EQC,**,8200,,,*MASTER*, 697                    vv
       1000A0000000046700010000000000000000000000000000000007000
 *IRD000E 1061,002032-001 LEVEL=1 FRU(S)=SLOT7
```

FRU Numbers

The following Brocade FRU numbers are provided for error reports and associated FRU names that display in error reports. Note that the FRU number does not display in the error reports, but its associated FRU name does display.

- 1 = SLOT1
- 2 = SLOT2
- 3 = SLOT3
- 4 = SLOT4
- 5 = SLOT5
- 6 = SLOT6
- 7 = SLOT7
- 8 = SLOT8
- 9 = SLOT9
- 10 = SLOT10
- 11 = SLOT11
- 12 = SLOT12
- 17 = PWR1
- 18 = PWR2
- 19 = PWR3
- 20 = PWR4
- 24 = FAN1
- 25 = FAN2
- 26 = FAN3
- 30 = CHASSIS
- 31 = WWN-CRD

Common FICON Issues

Any information that you need to verify that FICON has been set up correctly can be found in the Configuration Restoration in a FICON Environment sections.

Symptom	Probable Cause and Recommended Action
Cascading: No path - Entry Link is ".." message.	This typically occurs when one or more of the required high-integrity feature requirements for cascading have not been met. Check the following: • Review each step in the Configuring FICON procedure in the *Brocade Fabric OS Administration Guide*, and validate that all features are configured properly. • Validate that the CUP is online for each FICON director or switch in the fabric with the data center's system programmer.
Path to a device does not come online.	No connection to device. Make sure that binding or zoning does not prevent the connection. Validate the following with the data center's system programmer: • Correct switch addresses (not switch IDs) are used in link statements. The link statements use the first 2 bytes of CUP Port Address, which in FICON consist of the domain ID of the switch in hex followed by the address (or area) 0xFE (which is reserved for the switch Control Unit port in FICON), for the domain and area bytes of the Link Address respectively. . For example - – CNTLUNIT CUNUMBR=BF46, X – PATH=(CSS(2),EC,EE), X – UNITADD=((00,1)),UNIT=2032, X – LINK=(CSS(2),C4FE,C4FE) – IODEVICE ADDRESS=(BF46),CUNUMBR=(BF46),UNIT=2032,UNITADD=00 .. where the domain ID of the switch is 0xC4 • The switch ID, used in the CHPID statements, was defined with the correct switch address. • All addressing (link statements) uses two-byte addressing on the channel if two-byte addressing has been previously used on that channel. This is necessary even when the specified path is not cascaded.
Frames are being dropped between two FICON units.	The distance between devices is impacting data. When planning cable needs, the following criteria must be considered: • Distance considerations • Fiber Optic Sub Assembly (FOSA) type (SW or LW) • Cable specifications (SM or MM) • Patch panel connections between FOSA ports (link loss 0.3-5.0 dB per) • Maximum allowable link budget (dB) loss For cabling, the most important factor of a Fibre Channel link is the selection of the FOSA and matching cable type to support the required distance. Both ends of the optical link must have the matching FOSA (SFP) types.

Symptom	Probable Cause and Recommended Action

Channel path with two-byte addressing does not come online.	The fabric is not configured properly, cable connections are not correct, or a cable is the wrong type.
	Find out what CHPID the operator is attempting to bring online. In FICON environments, only the egress ports are defined in the IOCDS. The CHPID number of the channel appears in the node list, but only if the channel path has logged in. If the channel path does not come online, it may not have completed a Fibre Channel fabric login. If this is the case, you must rely on customer documentation to determine the switch port to which the channel is connected.
	Next, find out what type of error message the operator is getting. An IOS error message is reported when there is an error external to the host; an IEE error message indicates that something is wrong internal to the host.
	Fabric Not Configured Properly
	• Make sure that the insistent domain ID is set and that the domain IDs are unique for all switches in the fabric.
	• Make sure that the same binding method is used on all switches in the fabric.
	• Scroll through the node list and make sure that there are no invalid attachments.
	• Make sure that the re-routing delay is turned off.
	Cabling
	Validate that cables are connected where intended.
	When using multimode fiber, make sure that all fiber is either all 50µ or all 62.5µ. A common mistake is to mix 50µ and 62.5µ fiber cables, which cause errors at patch panels.
	Example of a Boxed Channel
	In the following example, the CHPIDs with two-byte addressing did not come online. In response, the CHPID was configured offline and then reconfigured back online. MVS console commands and responses (lines beginning with "IEE" are responses, and all other lines are entries).
	`CF CHP(60),OFFLINE`
	`IEE503I CHP(60),OFFLINE`
	`IEE712I CONFIG PROCESSING COMPLETE`
	`CF CHP(60),ONLINE`
	`IEE754I NOT ALL PATHS BROUGHT ONLINE WITH CHP(60)`
	`IEE502I CHP(60),ONLINE`
	`IEE712I CONFIG PROCESSING COMPLETE`

Symptom	Probable Cause and Recommended Action

	The following line displays the status of the CHPID with the "D M =" command. All other lines are responses.
	
	`D M=CHP(60)`
	`IEE174I 03.29.45 DISPLAY M 021`
	`CHPID 60: TYPE=1D, DESC=FICON INCOMPLETE, ONLINE`
	`DEVICE STATUS FOR CHANNEL PATH 60`
	`0 1 2 3 4 5 6 7 8 9 A B C D E F`
	`006 . $@ . . . . . .`
	`SWITCH DEVICE NUMBER = NONE`
	`ATTACHED ND = NOT KNOWN`
	`PHYSICAL CHANNEL ID = 01F0`
	`********** SYMBOL EXPLANATIONS`
	`**********`
	`+ ONLINE @ PATH NOT VALIDATED - OFFLINE . DOES NOT EXIST`
	`* PHYSICALLY ONLINE $ PATH NOT OPERATIONAL`
	The responses "NOT ALL PATHS BROUGHT ONLINE" after attempting to configure the CHPID online and "FICON INCOMPLETE" in the display example indicate that the channel did not come online. You can determine this because the IEE error types are shown and combined with the validation that there was no attempt to do a basic FLOGI (no light displayed on the port view [LED], and no Fibre Channel frames were received).

Unable to "vary online" FICON CUP port on the switch.	The FICON CUP port cannot go online. Use the `haFailover` command on the FICON director. This is the only known fix as there is no known firmware solution.

Troubleshooting FICON

This section provides information-gathering and troubleshooting techniques necessary to fix your problem.

General Information to Gather for All Cases

The following information must be gathered for all FICON environments:

- The output from the standard support commands (`portLogDump` , `supportSave` , and `supportShow`), the Fabric Manager event log, or Brocade SANnav Management Portal logs.
  By default, the FICON group in the `supportShow` output is disabled. To enable the capture of FICON data in the `supportShow` output, enter the `supportShowCfgEnable ficon` command. After you get confirmation that the configuration has been updated, output from the following commands will be collected and displayed for the `supportShow` command:

  - `ficonCupShow fmsmode`
  - `ficonCupShow modereg`
  - `ficonDbg dump rnid`
  - `ficonDbg log`
  - `ficonShow lirr`
  - `ficonShow rlir`
  - `ficonShow rnid`
  - `ficonShow switchrnid`
  - `ficuCmd dump -A`
- The type of mainframe involved including the make, model, and driver levels in use.
- The type of storage array installed. Many arrays emulate a certain type of IBM array, and the make, model, and firmware of the array in use must be provided.
- Other detailed information for protocol-specific problems:
  - Port data structures, displayed using the `ptDataShow` command.
  - Port registers, displayed using the `ptRegShow` command.

The following actions must be performed to troubleshoot all FICON environments:

- Use the `configUpload` command to gather configuration files. Provide the IOCDS mainframe file.
  This defines how all mainframe ports are configured.
- Verify that Dynamic Load Sharing (DLS) has been disabled with the `dlsReset` command.
  If DLS is enabled, traffic on existing ISL ports may be affected when one or more new ISLs are added between the same two switches. Specifically, adding a new ISL may result in dropped frames as routes are adjusted to take advantage of the bandwidth provided. By disabling DLS, you ensure that there are no dropped frames. In the `supportShow` output, search for "route.stickyRoutes" and check for a value of 1 or enter the `dlsShow` command.
- Verify that IOD is enabled using the `iodSet` command to ensure in-order delivery.
  In the output from `supportShow` or `supportSave` , search for "route.delayReroute" and check for a value of 1 as this indicates that the feature is turned on. Alternately, you can enter the `iodShow` command.

Switched Point-to-Point Topology Checklist

Verify the following in your FICON environment to ensure proper functionality of the feature:

- Fabric OS v8.2.x or a later release is installed on the Brocade switch or director.
- An appropriate management tool is being used, such as Brocade SANnav Management Portal.
- FICON channels and devices are connected to ports in a FICON logical switch.
- All required licenses are enabled for your FICON configuration.
- The switch or director does not have a special mode setting turned on for FICON.
- The Brocade Advanced features software package license (Trunking, Fabric Watch, Extended Fabric) is activated.

NOTE
There is no requirement to have a secure fabric in a switched point-to-point topology.

Cascaded Topology Checklist

Verify the following in your FICON environment to ensure proper functionality of the feature:

- Fabric OS v6.1.0 or later is installed on the Brocade switch or director.
- An appropriate management tool is used, such as Brocade SANnav Management Portal.
- All required licenses are activated to enable your FICON configuration.
- The switch or director does not have a special mode setting enabled for FICON.

In addition to device-based routing, lossless, and in-order frame delivery (IOD), the dynamic load-sharing feature is enabled.
- If you have a fabric for intermix mode of operations, separate zones for FICON and FCP devices are configured.
- A maximum of three hops exist for both FCP and FICON devices (mainframe channel device connectivity rule).
- FICON channels and devices are connected to ports in a FICON logical switch.
- The CHPID link path is defined using the two-byte address format.
- The FICON channel connectivity to the storage CU port does not exceed three hops.
- Proper security policies are enabled. See Configuring FICON in the *Brocade Fabric OS Administration Guide*.
- The Brocade Advanced features software package license (Trunking, Fabric Watch, Extended Fabric) is activated.

Gathering Additional Information for FICON

Collect information for your support provider as mentioned in the Gathering Basic Information and Gathering Detailed Problem Information. In addition, gather the following FICON-specific information.

- Did the problem occur during an initial installation or was everything functioning before the problem?
- What was changed immediately before the problem occurred?
- Is the switch properly configured for a FICON environment?
  Refer to the most recent version of the Fabric OS release notes for notes on FICON setup and configuration.
- Is this a switched point-to-point or cascaded environment?
- Is the FICON group enabled for `supportShow` ?
  Enter the `supportShow` command and verify that FICON is enabled under "supportshow groups enabled." If it is not enabled, use the `supportShowCfgEnable ficon` command.

Link Information

Gather information about the physical status of the link.

- Use the `portshow` command to display port operational information on Brocade extension switches and blades.
- Use the `sfpshow` command to display status of the optics.

Refer to the *Brocade Fabric OS Command Reference* for complete descriptions of the `portshow` and the `sfpshow` command syntax and options.

CUP Diagnostics

The FICON CUP supports the IBM Health Checker for z/OS to diagnose problems. Refer to the IBM Redbooks website at www.redbooks.ibm.com for details on using the IBM Health Checker for z/OS.

You can also refer to a Brocade white paper that discusses CUP diagnostics and the IBM Health Checker for z/OS, found at https://docs.broadcom.com/doc/12380287

Troubleshooting FICON CUP

In addition to the information that you collect for your support provider mentioned in Troubleshooting FICON, also gather the following information specific to FICON CUP:

- Verify that the FICON CUP license is installed.
- Check the state of the CUP by running the `ficonCupShow fmsmode` command. If it is disabled, enter the `ficonCupSet fmsmode enable` command to enable it. If the CUP is on a director, enter the `haFailover` command to ensure that both CPs are set correctly.
- Verify that the switch is using Fabric OS v8.2.x or later.
- Verify with the systems programmer that the CUP ports are defined properly.
  FICON ports are defined as part of the sysgen process. The z/OS systems programmer can verify if the CUP ports are defined properly.

Troubleshooting NPIV

Gather all information as listed in General Information to Gather for All Cases and Gathering Additional Information for FICON.

Diagnostic Features

Fabric OS Diagnostics

The purpose of the diagnostic subsystem is to evaluate the integrity of the system hardware.

Diagnostics are invoked in one of the following ways:

- Automatically during the power-on self-test (POST).
- Automatically on an individual blade whenever it is installed into a director chassis.
- Manually using Fabric OS CLI commands.

The error messages generated during these test activities are sent to the serial console and system message logs (output formats may differ slightly).

Use the `diagHelp` command to receive a list of all available diagnostic commands.

Diagnostic Information

On the switch, you can enter the `supportShow` command to dump important diagnostic and status information to the session screen, where you can review it or capture its data. If you are using a Telnet client, you may have to set up the client to capture the data before opening the session.

Most information can be captured using the `supportSave` command and downloading it off the switch by FTP, but when you are collecting information from specialized commands, such as `supportShow` , this information must be captured using a Telnet client.

To save a set of files that customer support technicians can use to further diagnose the switch condition, enter the `supportSave` command. The command prompts for an FTP server, packages the following files, and sends them to the specified server:

- The output of the `supportShow` command.
- Any core files, panic dumps, or FFDC files that may have been generated.
- System message (RAS) logs.
- Other special feature logs.

See Automatic Trace Dump Transfers.

Power-On Self-Test

By default, when you power on the system, the boot loader automatically performs power-on self-tests and loads a Fabric OS kernel image. Likewise, if you issue the `slotPowerOn` command or insert a new blade, a power-on self-test is run on that blade.

The POST tests provide a quick indication of hardware readiness when hardware is powered up. These tests do not require user input to function. They typically operate within several minutes, and they support minimal validation because of the restriction on test duration. Their purpose is to give a basic health check before a new switch joins a fabric.

These tests are divided into two groups: POST1 and POST2. POST1 validates the hardware interconnect of the device, and POST2 validates the ability of the device to pass data frames between the ports. The specific set of diagnostic and test commands run during POST depends on the switch model.

NOTE
When POST2 is running portloopbacktest mode 8 or mode 11 and if the peer blades are powered off while the test is running, the POST is expected to fail in the core blades as mode 8 and mode 11 test the peer links and the peer end is no longer active.

NOTE
The POST2 will run the test for both Fibre Channel and Ethernet frames on the Brocade FC32-64 blade.

On Gen 6 and Gen 7 directors, POST2 will run mode 11 (backend link test) from the Core blades only.

You can use the `diagDisablePost` command to disable both POST1 and POST2, and you can re-enable POST1 and POST2 using the `diagEnablePost` command.

If you choose to bypass POST or after POST completes, various system services are started and the boot process displays additional console status and progress messages.

NOTE
POST must be enabled or disabled in advance (just before power-cycling or rebooting the chassis). Do not enable or disable the POST in the middle of the chassis power-on/reboot sequence, which results in unpredictable behavior. POST must not be disabled or enabled in the middle of the chassis or slot power-on/reboot sequence.

Disabling POST

A reboot is not required for `diagDisablePost` to take effect.

NOTE
Disabling POST is not recommended and should be done only on the advice of your customer support technician.

1. Connect to the switch and log in with a user account that has admin privileges with the chassis-role permission.
2. Enter the `diagDisablePost` command.

   This disables POST1 and POST2.

Enabling POST

A reboot is required for `diagEnablePost` to take effect.

1. Connect to the switch and log in with a user account that has admin privileges with the chassis-role permission.
2. Enter the `diagEnablePost` command to enable POST, and reboot the switch for POST tests to run.

```
switch:admin> diagenablepost
Config update Succeeded
Diagnostic POST is now enabled.
```

Switch Status

Use the `mapsdb--show` command to display the overall status of the switch, including the status of its power supplies, fans, and temperature. If the status of any one of these components is either marginal or down, the overall status of the switch is also displayed as marginal or down. If all components have a healthy status, the switch displays a healthy status.

To modify the rules used to classify the health of each component, use the `switchStatusPolicySet` command. To view the rules, use the `switchStatusPolicyShow` command.

NOTE
The `switchStatusShow` command does work when Flow Vision is enabled. See the *Brocade Fabric OS Command Reference Manual* and the *Brocade Fabric OS Flow Vision User Guide* for more information.

Viewing the Overall Status of the Switch

1. Connect to the switch and log in as admin.
2. Enter the `mapsdb --show` command.

```
switch:admin> mapsdb --show
1 Dashboard Information:
========================
DB start time: Wed Feb 12 02:17:13 2020
Active policy: dflt_base_policy
Configured Notifications: SW_CRITICAL,SW_MARGINAL,SFP_MARGINAL,FPIN
Fenced Ports         : None
Decommissioned Ports : None
Fenced circuits      : N/A
Quarantined Ports    : None
Top Zoned PIDs <pid(it-flows)>: 0x070500(1)
2 Switch Health Report:
=======================
Current Switch Policy Status: HEALTHY

3.1 Summary Report:
===================
Category |Today |Last 7 days |
-------------------------------------------------------------------------------
Port Health |No Errors |In operating range | BE Port Health |In operating range |In operating range | Fru
 Health |Out of operating range |Out of operating range | Security Violations |No Errors |In operating
 range | Fabric State Changes |In operating range |In operating range | Switch Resource |In operating
 range |In operating range | Fabric Performance Impact|In operating range |In operating range | IO Latency
 |In operating range |In operating range | IO SCSI Health |In operating range |In operating range |
3.2 Rules Affecting Health:
===========================
Category(Violation Count)|RepeatCount|Rule Name |Execution Time |Object |Triggered Value(Units)|
-------------------------------------------------------------------------------------
Fru Health(29) |5 |defALL_PORTSSFP_STATE_IN |02/13/20 01:01:13|U-Port 81 |IN
```

For more information on how the overall switch status is determined, refer to the `switchStatusPolicySet` command in the *Brocade Fabric OS Command Reference Manual*.

If Flow Vision is enabled, the following message appears:

```
ras225:FID128:admin> switchstatusshow
MAPS is enabled, Fabric Watch is disabled. Please use MAPS for monitoring and execute mapsHelp command for
 available MAPS commands.
```

Displaying Switch Information

To display the switch information, perform the following task:

1. Connect to the switch and log in as admin.
2. Enter the `switchShow` command.

   The following table lists the switch summary information.

Table 41: Switch Summary Information

Variable	Definition
switchType	Switch model and revision numbers.
switchName	Switch name.
switchState	Switch state: Online, Offline, Testing, or Faulty.
switchMode	Switch operation mode: Native, Interop, or Access Gateway.
switchRole	Principal, Subordinate, or Disabled.
switchDomain	ID: 0-31 or 1-23.
switchId	Switch embedded port D_ID.
switchWwn	Switch World Wide Name (WWN).
switchBeacon	Switch beaconing state: On or Off.
zoning	When Access Gateway mode is disabled, the name of the active zone displays in parentheses.
FC Router	FC router's state: On or Off.
FC Router BB Fabric ID	The backbone fabric ID for FC routing.

The following table lists the following additional properties displayed in the switch summary for Virtual Fabrics-enabled switches.

Table 42: VF Output Values

Variable	Definition
LS Attributes	Displays logical switch attributes, including the fabric ID (FID) associated with the logical switch and the switch role (default switch or base switch).
Allow XISL Use	Allows the switch to use extended inter-switch links (XISLs) in the base fabric to carry traffic to this logical switch. Values are ON or OFF.

The following table lists the `switchShow` command output information for ports on the specified switch.

Table 43: switchShow Command Output

Variable	Definition
Index	Index follows Area up to 255. Then it continues to the maximum port of the platform. Index identifies the port number relative to the switch. The Index column is displayed only on enterprise-class platforms.
Slot	Slot number 1-4 and 7-10.
Port	Port number 0-15, 0-31, or 0-47.
Address	The 24-bit address identifier. The Address column is displayed only on enterprise-class platforms.
Media	SFP types used.
Speed	The speed of the port (1G, 2G, 4G, 8G, 10G, 16G, 32G, 64G, N1, N2, N4, N8, N10, N16, N32, N64, AN, and UN). The speed can be fixed, negotiated, or auto-negotiated.
State	The port status.

Variable	Definition
Proto	Protocol support by GbE port.

The details displayed for each switch differ on different switch models. For more information, refer to the `switchShow` command in the *Brocade Fabric OS Command Reference Manual*.

Displaying the Uptime for a Switch

1. Connect to the switch and log in as admin.
2. Enter the `uptime` command.

```
ecp:admin> uptime
 10:50:19 up 11 days,  6:28,  1 user,  load average: 0.49, 0.53, 0.54
```

The `uptime` command displays the length of time for which the system has been in operation, the total cumulative amount of uptime since the system was first powered on, and the load average over the past one minute. The reason for the last switch reboot is also recorded in the system message log.

Switch Decommissioning

From the Fabric OS 9.1.1 release, a switch decommissioning process is provided for users who want to erase all the data on the switch before decommissioning.

Use the `switchdecommission` command to erase the firmware and all data installed on that switch. Switch decommissioning is a disruptive process, which makes the switch unusable.

Once the command is executed, you will see the warning message `This operation will erase the firmware on the switch and should be return to the service provider`. You are prompted to provide a decommission authorization code (DAC) from the service provider. If you provide an invalid DAC, the command execution fails.

```
switch:admin> switchdecommission
This operation will erase the firmware on the switch and after completion, the switch will not be operational.
Would like to continue[y/n]:y
**********************************************************************
Please contact your service provider for special authorization code.
License ID : (10:00:00:aa:bb:cc:dd:00)
**********************************************************************
Enter decommission authorization code (DAC):*****
Authorization successful. Switch decommission started....
/**********************************************************************
Switch decommission has started. Please do not power off the switch.
Switch Decommission is completed.
Please return the switch to the service provider.
/**********************************************************************
```

Consider the following limitations while using the command:

- The switch decommissioning command should be executed on individual CPs separately.
- The user should run the command from the console session. It is not recommended to use the Telnet or SSH utility because the connection will be lost and the user might not see the completion status.
- If the switch is powered off right after executing the switchdecommision command, the switch will boot up as usual. The user must execute the command again to perform the decommission.
- If the switch is powered off before the erase operation, the erase operation will be performed and the decommission operation will be completed only at the next boot.
- If the switch is powered off in the middle of the erase operation, the file system will still be corrupted and the switch will not boot properly. The user can contact the service provider for recovery or to complete the decommission.

Removing a Switch from the Fabric

Removing a switch from the fabric is a disruptive operation. You must execute the `chassisdisable` command, which disables all logical switches in VF mode or disable the switch in non-VF mode. For more details on removing a switch from the fabric, refer to the *Brocade Fabric OS Administration Guide*.

Using the spinFab and portTest Commands

The `spinFab` command is an online diagnostics command to verify the ISLs between switches at the maximum speed. The routing functionality in the hardware must be set up so that the test frames received by the E_Port are retransmitted on the same E_Port. Several frames are then sent to the port attached to each active E_Port specified. These frames are special frames that never occur during normal traffic, and the default action for such frames is to route them back to the sender. These frames are circulated between switches until the test stops them.

CAUTION
During the spinFab testing, the switch remains in normal operation. However, some performance degradation occurs due to the ISL links being saturated with the test frames. This test should be run with caution on a live fabric.

The following table lists the supported ports for the specified version of Fabric OS when using the `spinFab` command.

Table 44: Port Type Support

Port Type	Supported by FOS
Loopback	Yes
D_Ports	Yes
D_Ports to AG switch ports	Yes
E_Ports	Yes
Trunk master ports	Yes
Ports beyond index 255	Yes
Ports with swapped areas	Yes
Shared-area ports	Yes
Ports in logical switches	Yes
Ports in base switches	Yes
Trunk slave ports	Yes
Long-distance ports	Yes
F_Ports connected to Brocade HBAs	Yes
ICL ports	Yes

Port Type	Supported by FOS
F_Ports connected to Access Gateway	Yes
EX_Ports	No
Ports in an Access Gateway switch	No

NOTE

The `portTest` and `spinFab` commands are not supported on AE and AF ports for Brocade Analytics Monitoring Platform connections.

The `spinFab` and `portTest` commands on Ethernet ports are not supported for the FC32-64 blade and the Brocade G630 Switch.

The `spinFab` and `portTest` commands on VE ports are not supported for the Brocade 7810 Extension Switch and Brocade SX6 Extension Blade.

Debugging spinFab Errors

Link errors and transmit or receive errors are seen when the `spinFab` test fails.

Link Errors

Once the frame is sent out the port, the `spinFab` command monitors the link errors in the ASIC. If any of the error counters are nonzero, `spinFab` reports an error and the test fails on the port.

```
ERROR: DIAG ERRSTAT spinfab, pass 6,
Pt0/17(7) Ch0/7 CRC_err Error Counter is 109738997 sb 0,
```

```
ERROR: DIAG ERRSTAT spinfab, pass 1,
Pt0/3(33) Ch0/33 Enc_in Error Counter is 32 sb 0,
ERROR: DIAG ERRSTAT spinfab, pass 1,
Pt0/3(33) Ch0/33 Enc_out Error Counter is 187725412 sb 0,
ERROR: DIAG ERRSTAT spinfab, pass 1,
Pt0/3(33) Ch0/33 TruncFrm Error Counter is 32 sb 0,
ERROR: DIAG ERRSTAT spinfab, pass 1,
Pt0/3(33) Ch0/33 FrmTooLong Error Counter is 32 sb 0,
ERROR: DIAG ERRSTAT spinfab, pass 1,
Pt0/3(33) Ch0/33 BadOrdSet Error Counter is 32 sb 0,
ERROR: DIAG ERRSTAT spinfab, pass 1,
Pt0/3(33) Ch0/33 BadEOF Error Counter is 1 sb 0,
ERROR: DIAG ERRSTAT spinfab, pass 1,
Pt0/3(33) Ch0/33 DiscC3 Error Counter is 32 sb 0,
```

If you receive any link errors, follow the suggested debugging procedures:

- The `spinFab` command does not clear any existing error counters before running the test. You should first clear all error counters and rerun the `spinFab` command.
- Verify that the link comes up by enabling and disabling the local or remote ports.
- Verify that the source of the error is either the local port or the remote port. This can be done by monitoring the port statistics on both ends simultaneously. See Displaying Port Statistics for more information on how to display the statistics for a port.
- Verify that the cables and SFPs are inserted properly. Remove and insert them again on both ends.
- Verify that the failing local port is working when connected to another remote port. Similarly, check whether the failing remote port is working when connected to another local port.
- Once the fault is isolated on either the local port or the remote port, replace the cable and SFPs connected to the local port and the remote ports.
- In case of loopback ports, change the loopback plug. See Marginal links for more information on changing the loopback plug.
- Further isolation can be done by running the `portLoopbackTest` command (Offline test) on the failing port to check whether the blade internal ports are having problems.
  - The `-lb_mode 1` operand verifies that the SFP is working within normal operating parameters. The use of this operand requires that loopback cables are connected.
  - The `-lb_mode 2` verifies that the ASIC port is working within normal operating parameters. The use of this operand does not require any loopback cables.

Tx/Rx Errors

The following errors are seen when the port fails to transmit or receive frames.

```
ERROR: DIAG PORTSTOPPED spinfab:spinfab, 0 nMegs,
Pt7/2(2) Ch0/2 No Longer Transmitting, FTX Counter Stuck at 116295726,
ERROR: DIAG TIMEOUT spinfab:spinfab, pass 2,
Pt0/17(7) Ch0/7 Receive Error/Timeout
```

If you receive any Tx/Rx errors, follow the suggest debugging procedures:

- Check whether the same port is reporting link errors as discussed in Link Errors. If yes, follow the same set of debugging procedures as discussed there.
- Check whether the local port or the remote port is beyond port 255. If yes, try connecting to the lower numbered ports. This behavior is found in Fabric OS 6.2.0 and earlier versions only.
- Check whether the local port or the remote port port is part of a shared-area region. If yes, try connecting to the nonshared area ports. This behavior is found in Fabric OS 6.2.0 and earlier versions only.
- Check whether the local port or the remote port is having its area swapped. If yes, try connecting to the normal area ports. This behavior is found in Fabric OS 6.2.0 and earlier versions only.

Clearing Error Counters

This procedure clears the port hardware statistics, including AL_PA-based CRC monitor, end-to-end monitor, and filter-based performance monitor statistics.

1. Connect to the switch and log in as admin.
2. Enter the `portStatsClear` command.

Enabling a Port

1. Connect to the switch and log in using an account with admin permissions.
2. Enter the appropriate command based on the current state of the port and whether it is necessary to specify a slot number:
   - To enable a port that is disabled, enter the `portEnable` command.
   - To enable a port that is persistently disabled, enter the `portCfgPersistentEnable` command.

   If you change port configurations during a switch failover, the ports may become disabled. To bring the ports online, reissue the `portEnable` command after the failover is complete.

Disabling a Port

1. Connect to the switch and log in using an account with admin permissions.
2. Enter the appropriate command based on the current state of the port and whether it is necessary to specify a slot number:
   - To disable a port that is enabled, enter the `portDisable` command.
   - To disable a port that is persistently enabled, enter the `portCfgPersistentDisable` command.

Port Information

Use the following instructions to view information about ports and to help diagnose if your switch is experiencing port problems.

NOTE
For a detailed discussion of the diagnostic port (D_Port) feature, see Diagnostic Port.

Viewing the Status of a Port

1. Connect to the switch and log in as admin.
2. Enter the `portShow` command, specifying the number that corresponds to the port that you are troubleshooting. In this example, the status of port 10 is shown:

```
switch:admin> portshow 10
portName:
portHealth: HEALTHY
Authentication: None
portDisableReason: None
portCFlags: 0x1
portFlags: 0x20b03  PRESENT ACTIVE F_PORT G_PORT U_PORT LOGICAL_ONLINE LOGIN NOELP ACCEPT FLOGI
portType:  18.0
POD Port: Port is licensed
portState: 1 Online
portPhys:  6 In_Sync
portScn:   32 F_Port
```

```
port generation number:    14
portId:    020a00
portIfId:    4302000b
portWwn:   20:0a:00:05:1e:41:4a:a5
portWwn of device(s) connected:
 21:00:00:e0:8b:05:e0:b1
Distance:  normal
portSpeed: N2Gbps
LE domain: 0
FC Fastwrite: OFF
Interrupts:        0          Link_failure: 0          Frjt:         0
Unknown:           0          Loss_of_sync: 3          Fbsy:         0
Lli:               18         Loss_of_sig:  6
Proc_rqrd:         161        Protocol_err: 0
Timed_out:         0          Invalid_word: 563851
Rx_flushed:        0          Invalid_crc:  0
Tx_unavail:        0          Delim_err:    0
Free_buffer:       0          Address_err:  0
Overrun:           0          Lr_in:        3
Suspended:         0          Lr_out:       0
Parity_err:        0          Ols_in:       0
2_parity_err:      0          Ols_out:      3
CMI_bus_err:       0
Port part of other ADs: No
```

Refer to the *Brocade Fabric OS Command Reference Manual* for additional `portShow` command information, such as the syntax for slot or port numbering, displaying IP interfaces on a GbE port, or displaying FCIP tunnel connection or configuration information.

Displaying Port Statistics

1. Connect to the switch and log in as admin.
2. Enter the `portStatsShow` command.

   Port statistics include information such as the number of frames received, number of frames sent, number of encoding errors received, and number of class 2 and class 3 frames received.

   Refer to the *Brocade Fabric OS Command Reference Manaul* for additional `portStatsShow` command information, such as the syntax for slot or port numbering.

```
switch:admin> portstatsshow 68
stat_wtx             113535      4-byte words transmitted
stat_wrx             22813       4-byte words received
stat_ftx             9259        Frames transmitted
stat_frx             821         Frames received
stat_c2_frx          0           Class 2 frames received
stat_c3_frx          821         Class 3 frames received
stat_lc_rx           0           Link control frames received
stat_mc_rx           0           Multicast frames received
stat_mc_to           0           Multicast timeouts
stat_mc_tx           0           Multicast frames transmitted
tim_rdy_pri          0           Time R_RDY high priority
tim_txcrd_z          0           Time TX Credit Zero (2.5Us ticks)
time_txcrd_z_vc  0- 3:  0           0           0           0
```

```
time_txcrd_z_vc  4- 7:  0           0           0           0
time_txcrd_z_vc  8-11:  0           0           0           0
time_txcrd_z_vc 12-15:  0           0           0           0
er_enc_in             0           Encoding errors inside of frames
er_crc                0           Frames with CRC errors
er_trunc              0           Frames shorter than minimum
er_toolong            0           Frames longer than maximum
er_bad_eof            0           Frames with bad end-of-frame
er_enc_out            0           Encoding error outside of frames
er_bad_os             0           Invalid ordered set
er_c3_timeout         0           Class 3 frames discarded due to timeout
er_c3_dest_unreach    0           Class 3 frames discarded due to destination unreachable
er_other_discard      0           Other discards
er_type1_miss         0           frames with FTB type 1 miss
er_type2_miss         0           frames with FTB type 2 miss
er_type6_miss         0           frames with FTB type 6 miss
er_zone_miss          0           frames with hard zoning miss
er_lun_zone_miss      0           frames with LUN zoning miss
er_crc_good_eof       0           Crc error with good eof
er_inv_arb            0           Invalid ARB
open                  810         loop_open
transfer              0           loop_transfer
opened                409856      FL_Port opened
starve_stop           0           tenancies stopped due to starvation
fl_tenancy            1715        number of times FL has the tenancy
nl_tenancy            331135      number of times NL has the tenancy
zero_tenancy          4           zero tenancy
```

Displaying a Summary of Port Errors for a Switch

1. Connect to the switch and log in as admin.
2. Enter the `porterrshow` command.

```
switch:admin> porterrshow
        frames  enc  crc  crc   too  too  bad  enc disc link loss loss frjt fbsy
          tx   rx   in  err g_eof shrt long  eof  out   c3 fail sync  sig
      ========================================================================
  0:  665k 7.0k   0    0    0    0    0    0    6    0    0    1    2    0    0
  1:    0    0    0    0    0    0    0    0    0    0    0    0    2    0    0
  2:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
  3:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
  4:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
  5:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
  6:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
  7:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
  8:   78   60    0    0    0    0    0    0    7    0    0    3    6    0    0
  9:   12    4    0    0    0    0    0    0    3    0    0    1    2    0    0
 10:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
 11:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
 12:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
 13:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
 14:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
 15:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
 16:  665k 7.4k   0    0    0    0    0    0    6    0    0    1    2    0    0
```

```
17:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
18:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
19:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
20:  6.3k 6.6k   0    0    0    0    0    0    7    0    0    1    2    0    0
21:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
22:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
23:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
24:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
25:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
26:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
27:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
28:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
29:    0    0    0    0    0    0    0    0    0    0    0    0    1    0    0
30:  664k 6.7k   0    0    0    0    0    0    6    0    0    1    2    0    0
31:   12    4    0    0    0    0    0    0    3    0    0    1    2    0    0
    (output truncated)
```

The `porterrshow` command output provides one output line per port. See Table for a description of the error types.

Table 45: Error Summary Description

Error Type	Description
frames tx	Frames transmitted
frames rx	Frames received
enc in	Encoding errors inside frames
crc err	Frames with CRC errors
crc g_eof	CRC errors that occur on frames with good end-of-frame delimiters
too shrt	Frames shorter than the minimum
too long	Frames longer than the maximum
bad eof	Frames with bad end-of-frame delimiters
enc out	Encoding error outside of frames
disc c3	Class 3 frames discarded
link fail	Link failures (LF1 or LF2 states)
loss sync	Loss of synchronization
loss sig	Loss of signal
frjt	Frames rejected with F_RJT
fbsy	Frames busied with F_BSY

Equipment Status

You can display the status for fans, power supplies, and temperature.

NOTE
The number of fans, power supplies, and temperature sensors depends on the switch type. For detailed specifications on these components, refer to the switch hardware reference manual. The specific output from the status commands varies depending on the switch type.

Checking the Temperature, Fans, and Power Supplies

1. Log in to the switch as admin.
2. Enter the `sensorShow` command. Refer to the *Brocade Fabric OS Command Reference Manual* for details regarding the sensor numbers.
3. Check the temperature output.

   Look for indications of high or low temperatures.
4. Check the fan speed output.

   If any of the fan speeds display abnormal RPMs, replace the fan.
5. Check the power supply status.

   If any power supplies show a status other than OK, consider replacing the power supply as soon as possible.

Checking the Status of the Fans

1. Connect to the switch and log in as admin.
2. Enter the `fanShow` command.

```
switch:admin> fanshow
Fan 1 is Absent
Fan 2 is Ok, speed is 6553 RPM
Fan 3 is Ok, speed is 6367 RPM
```

The possible status values are:

- OK—Fan is functioning correctly.
- Absent—Fan is not present.
- Below minimum—Fan is present but rotating too slowly or stopped.
- Above minimum—Fan is rotating too quickly.
- Unknown—Unknown fan unit installed.
- FAULTY—Fan has exceeded the hardware tolerance or is not be seated properly.

The output from this command varies depending on the switch type and the number of fans present. Refer to the appropriate hardware reference manual for details regarding the fan status. You may first consider reseating the fan (unplug it and plug it back in).

Checking the Status of a Power Supply

1. Connect to the switch and log in as admin.
2. Enter the `psShow` command.

```
switch:admin> psshow
Power Supply #1 is OK
V10645,TQ2Z6452916     ,60-0300031-02, B, QCS ,DCJ3001-02P     , A,TQ2Z64529
Power Supply #2 is faulty
V10704,    TQ2J7040124     ,60-0300031-02, B,CHRKE,SP640-Y01A      ,C ,TQ2J7040
```

The possible status values are:

- OK—Power supply is functioning correctly.
- Absent—Power supply is not present.
- Unknown—Unknown power supply unit is installed.
- Predicting failure—Power supply is present but is predicting failure.
- FAULTY—Power supply is present but faulty (no power cable, power switch turned off, fuse blown, or other internal error).

If any of the power supplies shows a status other than OK, consider replacing the power supply as soon as possible. For certain switch models, the OEM serial ID data displays after each power supply status line.

Checking the Temperature Status

1. Connect to the switch and log in as admin.
2. Enter the `tempShow` command.

```
switch:admin> tempshow
Sensor  State           Centigrade     Fahrenheit
  ID
================================================
  1     Ok                  28             82
  2     Ok                  16             60
  3     Ok                  18             64
```

Information is displayed for each temperature sensor in the switch.

The possible temperature status values are:

- OK: Temperature is within the acceptable range.
- FAIL: Temperature is outside the acceptable range. Damage might occur.

Refer to the hardware reference manual for your switch to determine the normal temperature range.

System Message Log

The system message log (RASlog) feature enables messages to be saved across power cycles and reboots.

The Brocade X6 and X7 family of enterprise-class platforms maintains independent and separate RASlogs for each of the two CP blades. Because all RASlog messages are routed to the active CP, the message CPU ID is added as part of the RASlog message attribute. The RASlog message attribute SLOT is defined to identify the CPU that generated the message.

For example, in the following message, the identifier SLOT 2 means that the message was generated from the slot 2 blade main CPU:

```
2019/07/26-13:39:23, [SEC-1203], 134, SLOT 2 | FID 128, INFO, DS_128_Venator, Login information: Login
 successful via: HTTP. IP Addr: 10.155.163.83
```

In the following message, the identifier SLOT 2/1 means that the message was generated from the slot 2 blade co-CPU.

```
2019/07/26-13:39:23, [SEC-1203], 134, SLOT 2 | FID 128, INFO, DS_128_Venator, Login information: Login
 successful via: HTTP. IP Addr: 10.155.163.83
```

Because RASlog supports logical switches, the FID (fabric ID) displays on every RASlog message to identify the source of the logical switch that generates the message.

The FID can be a number from 0 to 128, and the identifier CHASSIS depends on the instance that generates the message and that it was generated by a chassis instance. The identifier FID 128 means that the message was generated by the default switch instance.

```
2020/02/21-01:30:32, [LOG-1003], 1, CHASSIS, INFO, sw0, The log has been cleared.
```

For details on error messages, refer to the *Brocade Fabric OS Message Reference*.

Displaying the System Message Log with No Page Breaks

1. Connect to the switch and log in as admin.
2. Enter the `errDump` command.

Displaying the System Message Log One Message at a Time

1. Connect to the switch and log in as admin.
2. Enter the `errShow` command.

Clearing the System Message Log

1. Connect to the switch and log in as admin.
2. Enter the `errClear` command.
3. Repeat Step 2 on the standby CP for a complete erasure of the message log.

   All switch and chassis events are removed from both CPs.

Port Log

Fabric OS maintains an internal log of all port activity. The port log stores entries for each port in a circular buffer. For all other switches, the number of lines range from 8192 to 16,384. These ranges are for all ports on the switch, not just for one port. When the log is full, the newest log entries overwrite the oldest log entries. The port log is not persistent and is lost over power-cycles and reboots. If the port log is disabled, an error message displays.

NOTE
Port log functionality is separate from the system message log. The port log is typically used to troubleshoot device connections.

Viewing the Port Log

1. Connect to the switch and log in as admin.
2. Enter the `portlogshow` command:

```
device:admin> portlogshow
time         task       event   port cmd  args
-----------------------------------------------
Fri Feb 22 16:48:45 2008
16:48:45.208 SPEE       sn       67   NM  00000009,00000000,00000000
16:48:46.783 PORT       Rx       64   40  02fffffd,00fffffd,02e2ffff,14000000
16:48:46.783 PORT       Tx       64    0  c0fffffd,00fffffd,02e201bf,00000001
16:48:46.783 FCPH       read     64   40  02fffffd,00fffffd,be000000,00000000,02e201bf
16:48:46.783 FCPH       seq      64   28  22380000,02e201bf,00000c1e,0000001c,00000000
16:48:46.828 SPEE       sn       67   NM  00000009,00000000,00000000
16:48:46.853 PORT       Rx       76   40  02fffffd,00fffffd,02e3ffff,14000000
16:48:46.853 PORT       Tx       76    0  c0fffffd,00fffffd,02e301c1,00000001
16:48:46.853 FCPH       read     76   40  02fffffd,00fffffd,bf000000,00000000,02e301c1
16:48:46.853 FCPH       seq      76   28  22380000,02e301c1,00000c1e,0000001c,00000000
16:48:47.263 PORT       Rx       79   40  02fffffd,00fffffd,02e4ffff,14000000
16:48:47.263 PORT       Tx       79    0  c0fffffd,00fffffd,02e401c2,00000001
     (output truncated)
```

Use the commands summarized in Table to view and manage port logs. Refer to the *Brocade Fabric OS Message Reference* for additional information about these commands.

Table 46: Commands for Port Log Management

Command	Description
`portlogclear`	Clears port logs for all or particular ports.
`portlogdisable`	Disables port logs for all or particular ports.
`portlogdump`	Displays port logs for all or particular ports, without page breaks.
`portlogenable`	Enables port logs for all or particular ports.
`portlogshow`	Displays port logs for all or particular ports, with page breaks.

The `portLogDump` command output (trace) is a powerful tool used to troubleshoot fabric issues. The `portLogDump` output provides detailed information about the actions and communications within a fabric. By understanding the processes that are taking place in the fabric, issues can be identified and located.

The `portLogDump` command displays the port log, showing a portion of the Fibre Channel payload and header (FC-PH). The header contains control and addressing information associated with the frame. The payload contains the information being transported by the frame and is determined by the higher-level service or FC_4 upper-level protocol. There are many different payload formats based on the protocol.

Because a `portLogDump` output is long, a truncated example is presented:

```
switch:admin> portlogdump
time         task       event    port cmd  args
-------------------------------------------------
Fri Feb 22 20:29:12 2008
20:29:12.638 FCPH       write       3   40  00ffffd,00ffffd,00000000,00000000,00000000
20:29:12.638 FCPH       seq         3   28  00300000,00000000,000005f4,00020182,0000000
20:29:12.638 PORT       Tx          3   40  02ffffd,00ffffd,09a5ffff,14000000
20:29:12.638 FCPH       write       9   40  00ffffd,00ffffd,00000000,00000000,00000000
20:29:12.638 FCPH       seq         9   28  00300000,00000000,000005f4,00020182,00000000
20:29:12.639 PORT       Tx          9   40  02ffffd,00ffffd,09a6ffff,14000000
20:29:12.639 PORT       Rx          3    0  c0ffffd,00ffffd,09a50304,00000001
20:29:12.640 PORT       Rx          9    0  c0ffffd,00ffffd,09a60305,00000001
20:29:20.804 PORT       Rx          9   40  02ffffd,00ffffd,0306ffff,14000000
20:29:20.805 PORT       Tx          9    0  c0ffffd,00ffffd,030609a7,00000001
20:29:20.805 FCPH       read        9   40  02ffffd,00ffffd,d1000000,00000000,030609a7
20:29:20.805 FCPH       seq         9   28  22380000,030609a7,00000608,0000001c,00000000
20:29:20.805 PORT       Rx          3   40  02ffffd,00ffffd,02eeffff,14000000
20:29:20.806 PORT       Tx          3    0  c0ffffd,00ffffd,02ee09a8,00000001
20:29:20.806 FCPH       read        3   40  02ffffd,00ffffd,d2000000,00000000,02ee09a8
20:29:20.806 FCPH       seq         3   28  22380000,02ee09a8,00000608,0000001c,00000000
20:29:32.638 FCPH       write       3   40  00ffffd,00ffffd,00000000,00000000,00000000
20:29:32.638 FCPH       seq         3   28  00300000,00000000,000005f4,00020182,00000000
20:29:32.638 PORT       Tx          3   40  02ffffd,00ffffd,09a9ffff,14000000
20:29:32.638 FCPH       write       9   40 00ffffd,00ffffd,00000000,00000000, 00000000
20:29:32.638 FCPH       seq         9   28  00300000,00000000,000005f4,00020182,00000000
20:29:32.639 PORT       Tx          9   40  02ffffd,00ffffd,09aaffff,14000000
<output truncated>
```

Syslogadmin Configuration

The system logging daemon (syslogadmin) is an IP-based service for logging system messages that is made available by default on UNIX and Linux operating systems. It is available as a third-party application for Windows operating systems.

Fabric OS can be configured to use a UNIX-style syslogadmin process to forward system events and error messages to log files on a remote host system. The host system can be running UNIX, Linux, or any other operating system that supports the standard syslogadmin functionality.

Fabric OS supports UNIX local7 facilities (the default facility level is 7). Syslogadmin configuration involves configuring the host, enabling syslogadmin on the switch, and, optionally, setting the facility level.

Configuring the Host

Fabric OS supports a subset of UNIX-style message severities that default to the UNIX local7 facility. To configure the host, edit the `/etc/syslog.conf` file to map Fabric OS message severities to UNIX severities, as shown in Table.

Table 47: Fabric OS to UNIX Message Severities

Fabric OS Message Severity	UNIX Message Severity
Critical (1)	Emergency (0)
Error (2)	Error (3)
Warning (3)	Warning (4)
Info (4)	Info (6)

In this example, Fabric OS messages map to local7 facility level 7 in the `/etc/syslog.conf` file:

```
local7.emerg          /var/adm/swcritical
local7.alert          /var/adm/alert7
local7.crit           /var/adm/crit7
local7.err            /var/adm/swerror
local7.warning        /var/adm/swwarning
local7.notice         /var/adm/notice7
local7.info           /var/adm/swinfo
local7.debug          /var/adm/debug7
```

If you prefer to map Fabric OS severities to a different UNIX local7 facility level, see Setting the Facility Level.

Configuring the Switch

Configuring the switch involves specifying syslogadmin hosts and, optionally, setting the facility level. You can also remove a host from the list of syslogadmin hosts.

Specifying syslogadmin Hosts

1. Connect to the switch and log in as admin.
2. Enter the `syslogadmin --set -ip` command and specify an IP address.
3. Verify that the IP address was entered correctly using the `syslogadmin --show -ip` command.

   The `syslogadmin --set -ip` command accepts IPv4, IPv6, and host name address. You can specify up to six host IP addresses for storing syslog messages, as shown in this example:

For IPv6 address:

```
syslogadmin --set -ip fc00:100:0:f101:111:f8ff:fef1:8fd1
```

For IPv4 address:

```
syslogadmin --set -ip 10.1.2.4
```

For Host Name address:

```
syslogadmin --set -ip WIN-I0ABCD5OF7B.abdcom.net
```

The following is a sample switch output:

```
switchoutput:
FID128:admin> syslogadmin --show -ip
syslog.1    10.1.2.4
syslog.2    fc00:100:0:f101::fa7e
syslog.3    win-i0abcd5of7b.sjs.abclab.abdcom.net
```

Securing syslog

When the syslog client sends data to a server, the connection is encrypted with TLS. The CA of the syslog server (the certificate used to start the process) is imported to allow the connection to succeed.

The `seccertmgmt` command is used to import the certificate for the syslog server.

The following is a sample switch output:

```
switch:admin> seccertmgmt import
-cert <fcap|commoncert|https|radius|ldap|syslog|extn>
-ca -client|-server <fcap|commoncert|https|radius|ldap|syslog|extn|asc>
-keypair_tag <keypair_name>
-protocol <scp|ftp>
-ipaddr <IP address>
-remotedir <remote directory>
-certname <certificate name>
-cacert <preimported_local_ca_cert>
-login <login name>
-password <password>
```

Setting the Facility Level

1. Connect to the switch and log in as admin.
2. Enter the `syslogadmin --set -facility` *n* command:

   The `n` variable is a number from 0 through 7 that indicates a UNIX local7 facility. The default is 7.

   You need to set the facility level only if you specified a facility other than local7 in the host `/etc/syslog.conf` file.

Removing a syslogadmin Host from the List

1. Connect to the switch and log in as admin.
2. Enter the `syslogadmin --remove -ip` command followed by the IP address of the host that you want to remove.

```
switch:admin> syslogadmin --remove -ip 10.1.2.1
```

3. Enter the `syslogadmin --show -ip` command to verify if the IP address was deleted.

Automatic Trace Dump Transfers

You can set up a switch so that diagnostic information is transferred automatically to a remote server. If a problem occurs, you can then provide your customer support representative with the most detailed information possible. To ensure the best service, you should set up automatic transfer as part of standard switch configuration, before a problem occurs.

Always check the cfgload attribute also while uploading the trace dump and use it as a protocol when it is configured as SCP. Otherwise we use FTP by default. Also do not allow the user to configure the supportftp protocol as FTP when the cfgload attribute is configured as secured.

Setting up automatic transfer of diagnostic files involves the following tasks:

- Specifying a remote server to store the files.
- Enabling the automatic transfer of trace dumps to the server.
  - In the case of Gen 6 devices, the trace dump files are stored on the switch by its type up to a limit and are transferred to an FTP server when the limit is exceeded. The files are deleted after they are transferred to an FTP server.
- Setting up periodic checking of the remote server so that you are alerted if the server becomes unavailable and you can correct the problem.

After the setup is complete, you can run the `supportSave -c` command to save RASlog, TRACE, supportShow, core file, FFDC data, and other diagnostic support information to the server without specifying server details.

The following procedures describe the tasks for setting up automatic transfer.

Specifying a Remote Server

1. Verify that the FTP service is running on the remote server.
2. Connect to the switch and log in as admin.
3. Enter the `supportFtp -s` command and respond to the prompts.

Enabling the Automatic Transfer of Trace Dumps

1. Connect to the switch and log in as admin.
2. Enter the `supportFtp -e` command.

Setting Up Periodic Checking of the Remote Server

1. Connect to the switch and log in as admin.
2. Enter the `supportFtp -t` command.

   Example of setting the interval in hours:

```
switch:admin> supportftp -t 4
supportftp: ftp check period changed
```

The minimum interval is 1 hour. Specify 0 to disable the checking feature.

Saving Comprehensive Diagnostic Files to the Server

1. Connect to the switch and log in as admin.
2. Enter the `supportSave -c` command and respond to the prompts.

```
switch:admin> supportsave -c
This command collects RASLOG, TRACE, supportShow, core file, FFDC data
and other support information from both active and standby CPs
and then transfer them to a FTP/SCP/SFTP server or a USB device.
Local CP, remote CP and BPs' information will be saved,
but supportShow information is available only on the Active CP.
This operation can take several minutes.
OK to proceed? (yes, y, no, n): [no]
```

NOTE
Use `supportSave -n -c` to run supportSave without confirmation on a chassis with AP blades included using supportFTP parameters

Support for Multiple Trace Dump Files

The following devices with warm memory support multiple trace dump files as described in this section.

- Brocade G610
- Brocade G620
- Brocade G630
- Brocade X6-4
- Brocade X6-8
- Brocade G720
- Brocade X7-4
- Brocade X7-8
- Brocade G730
- Brocade G648 Blade Server SAN I/O Module
- Brocade MXG610 Blade Server SAN I/O Module

Each of the following commands and scenarios triggers a separate trace dump from the warm memory to a file.

- `traceDump -n`
- `supportSave`
- When a software VERIFY error is detected
- When a panic dump is triggered
- When a RASLOG is generated with FFDC enabled as part of its execution

Auto FTP Support

You can automatically upload the trace dump that is triggered by FFDC and the `traceDump -n` command to a remote FTP server using the auto FTP feature.

- In case of `traceDump -n` , the tar file is automatically uploaded to the remote location. You can use the `supportDecode` command to decode.
- In case of FFDC, two tar files are generated. The `core_file.tar` file collects RASlog, and the `trace.tar` file collects FFDC trace logs.

Trace Dump Support

You can run the `traceDump` command to display the trace dump details. The following is an example from a Gen 6 device.

```
switch:admin> tracedump
Dump status for switch:
slot: 1
Type            Timestamp
---------------------------------
Reboot          2020/02/12 10:50
FFDC(EM-1100)   2020/02/13 02:13
Panicdump       2020/02/13 02:24
CLI             2020/02/13 02:47
```

You can use the `traceDump -r` command to remove the trace dump files generated by the CLI, panic dump, and FFDC messages. Fixed-port switches do not support the -s option.

NOTE
In the case of Gen 6 platforms, the trace dump files are automatically deleted from the switch when the auto FTP feature is enabled and you run the `supportSave` command.

Brocade ClearLink™ Diagnostic Port

Brocade ClearLink™ Diagnostic Port (D_Port) mode allows you to convert a Fibre Channel port into a diagnostic port for testing traffic. The test results can be very useful in diagnosing a variety of port and link problems.

NOTE
This feature uses Brocade ClearLink™ proprietary technology.

From Fabric OS v9.2.0, D-Port test supports only the link traffic test. Though the SFP supports Electrical and optical test, only link traffic test is performed.

The cable distance measurement is displayed only for the longer cables with more than 1 Km links. For shorter cables, the link distance is displayed as `unknown` .

Supported Platforms for D_Ports

The ports use Brocade-branded or certain Brocade-qualified SFP or QSFP transceivers. D_Port functionality is supported on the following Gen 6 and Gen 7 Fibre Channel (FC) platforms.

Table 48: Supported Transceivers for D_Ports with Fabric OS

Transceiver	SFP	QSFP
Gen 6	• 10/16/32G FC • 16/32G LWL FC • 8/16G ELWL FC	16G or 32G
Gen 7	• 64G/32G/16G LWL/ELWL FC • 10/16/32/64G FC	32G or Gen 7 ICL

NOTE
2-km 32G QSFPs only support the link traffic test.

The following table lists the Brocade devices and Fabric OS releases that support D_Ports.

Table 49: Supported platforms for D_Port with Fabric OS

Product	Fabric OS release and later
Brocade G620 Switch	8.0.0
Brocade X6-4 Director	8.0.1
Brocade X6-8 Director	8.0.1
Brocade G610 Switch	8.1.0
Brocade G630 Switch	8.2.0
Brocade 7810 Extension Switch	8.2.1
Brocade G720 Switch	9.0.0
Brocade X7-4 Director	9.0.0
Brocade X7-8 Director	9.0.0
Brocade G648 Blade Server SAN I/O Module	9.0.0
Brocade MXG610 Blade Server SAN I/O Module	9.0.0

Product	Fabric OS release and later
Brocade G730 Switch	9.1.0
Brocade 7850 Extension Switch	9.2.0

D_Port functionality is supported on the following HBAs:

- 16G HBAs: Emulex LPe16002B-M6, QLogic QLE-2672, QLogic 1860-2P
- 32G HBAs: Emulex LPe32000B, Emulex LPe35000, QLogic QLE2764, QLogic QLE2742
- 64G HBAs: Emulex LPe36002

HBA v3.1 provides limited support for D_Ports. HBA v3.2 provides extensive support for D_Ports, including dynamic D_Port mode.

- 16G HBAs (must have HBA D_Port support)

For applicable topologies, refer to the “Supported Topologies” section.

For D_Port functionality with 8G SFP transceivers, the switch must be running Fabric OS 9.0.0 or later.

To run D_Port tests on a link with 8G SFP transceivers, both ends of the link must have the same type of SFP. That is, both ends of the link must have LWL SFPs or both ends must have ELWL SFPs.

Licensing Requirements for D_Ports

The D_Port feature does not require a license if you are running tests between a pair of Brocade devices, whether the devices are switches, Access Gateways, or HBAs.

In Fabric OS 9.0.0 and later, If you want to run D_Port tests between a switch and a HBA, the Fabric Vision license for Gen 6 and Gen 7 is required. Also the HBA vendor must have implemented HBA D_Port support.

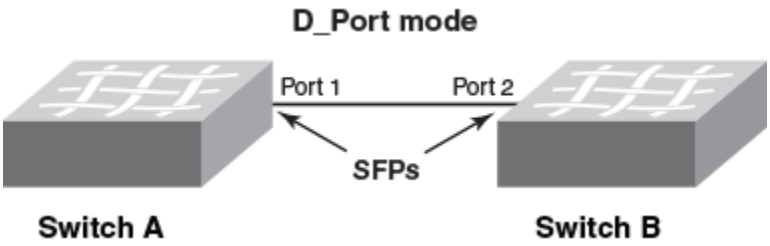
Understanding D_Ports

A port in D_Port mode does not carry any user traffic and is designed to run only specific diagnostics tests for identifying link-level faults or failures.

The following figure illustrates a D_Port connection between a pair of switches through SFP transceivers (port assignments will vary).

NOTE
D_Port functionality is supported only on 32G (Gen 6) platforms. However, the user can configure the link speed on a Gen 6 platform to come up at 8G, for example, because D_Port functionality remains available on links at lower speeds on those platforms.

Figure 4: Example of a Basic D_Port Connection between Switches



To bring up a port in D_Port mode, follow these basic steps:

1. Use the (`portdisable` *`port`*) to disable the ISL capability on the ports
2. Use the (`portcfgdport --enable` *`port`*) to enable D_Port functionality on both ends of the link.

3. Use the (`portenable` *`port`*) to enable the ISL capability on the ports.

   NOTE
   Detailed configuration examples are presented later in this chapter.

Once the ports are configured and enabled as D_Ports, the following basic test suite is executed in the following order, depending on the SFPs installed:

1. Link traffic
2. Link latency, distance, and power measurement (with 8G SFPs, 10G SFPs, 16/32/64G SFP+ and QSFP+, Gen 7 QSFP)

   NOTE
   32G QSFPs having a serial number beginning with ZTA11547 or newer to support only link traffic test.

The user configures the desired ports on either end, or both ends, of the connection. (The default D_Port mode of a port is dynamic mode. If the user configures one end as D_Port static mode, then the other end behaves as a D_Port. Alternatively, the user can configure both ends as D_Port static mode.) Once both sides are configured, a basic test suite is initiated automatically when the link comes online. After the automatic test is complete, the user can view results through the CLI or a GUI and rectify issues (if any) that are reported. The user can also start (and restart) the test manually to verify the link.

D_Port Configuration Modes and Testing

A D_Port can be configured in one of three modes:

- **Static** — This mode explicitly configures the port as a D_Port. In this mode, the port remains a D_Port until you explicitly remove the D_Port configuration.
- **Dynamic** — The port is automatically set to a D_Port based on an external request from a remote port on the other end of the connection. In this mode, the port remains a D_Port until all diagnostic tests are completed and the remote port reverts to normal mode. For the port to become a dynamic D_Port, the remote port on the other end of the connection must be either a static D_Port or an on-demand D_Port. Dynamic D_Port mode is supported on connections between a switch and a host bus adapter (HBA) or between an Access Gateway and an HBA/device, ISLs, and ICLs.

  By default, a switch has the capability to support dynamic D_Port mode. You can disable this capability by using the `configure` command, as shown in the following example.

```
switch:admin> configure
Configure...

  Fabric parameters (yes, y, no, n): [no]
  Virtual Channel parameters (yes, y, no, n): [no]
  F-Port login parameters (yes, y, no, n): [no]
  D-Port parameters (yes, y, no, n): [no] y

    Dynamic D-Port (on, off): [on] off
```

  NOTE
  Changes are reflected in the RASlog.
- **On-demand** — This mode is off by default and must be enabled. The port then becomes a D_Port as a result of an internal request or event within the local switch, such as the `slotpoweroff` , `slotpoweron` , `slot insert` , `portcfgPersistentDisable` , and `portcfgPersistentEnable` commands. In this mode, the port remains a D_Port until the diagnostic tests are completed successfully. If any of the tests fail, the port remains a D_Port. For a switch port to work as an on-demand D_Port, the other end of the connection must support dynamic D_Port capability. On-demand D_Port mode can be configured by means of a switch-wide command, and it is supported by default on switches and chassis (ISLs and ICLs). The following internal events within a switch or chassis can trigger a port to become a D_Port:

- `slotpoweroff` and `slotpoweron`
- `slot insert` (slot or blade insert)
- `portcfgPersistentDisable` and `portcfgPersistentEnable` commands

Once on-demand D_Port configuration is enabled on the switch and any of the on-demand triggers have been issued (such as `slotpoweroff` , `slotpoweron` , `slot insert`), the port comes up in on-demand D_Port mode.

If dynamic D_Port is supported, the on-demand D_Port forces the remote port to dynamic D_Port mode, triggers the diagnostic tests automatically, and then changes back to normal port mode after successful completion of the tests.

By default, a switch does not support on-demand D_Port mode. You can turn this capability on by using the `configure` command, as shown in the following example.

```
switch:admin> configure
Configure...

  Fabric parameters (yes, y, no, n): [no]
  Virtual Channel parameters (yes, y, no, n): [no]
  F-Port login parameters (yes, y, no, n): [no]
  D-Port parameters (yes, y, no, n): [no] y

    Dynamic D-Port (on, off): [on]
    On Demand D-Port (on, off): [off] on
```

NOTE
Even if the on-demand D_Port option is enabled, if any static D_Port configuration is enabled on a port, then that static configuration takes precedence.

The following table summarizes D_Port test initiation modes and test start behavior.

Table 50: D_Port Configuration Mode and Nature of Test

D_Port Mode/Nature of Test		Description
Mode	Static	You must configure the port explicitly. The port remains a D_Port until you remove the configuration.
	Dynamic	No user configuration is required. D_Port mode is initiated by an external request/event from the remote port. The remote port can be either a static or on-demand D_Port.
	On-demand	No user configuration is required. D_Port mode is initiated by an internal request within the local switch. The remote port should be a dynamic D_Port.
Nature of Test	Automatic	The test automatically starts when the port comes online.
	Manual	The user starts the test from the switch or Access Gateway side (using the `portdporttest` command with either the `--start` or `--restart` keyword) or from the HBA side. See BCU D_Port Commands for more information on BCU commands for HBAs.

When the tests complete, the port behavior depends on the mode:

- For static D_Ports, you must remove the D_Port configuration at either or both ends of the link to bring up the port as a regular E_Port or F_Port.
- For a switch port in dynamic D_Port mode, the port automatically reverts back to an E_Port or an F_Port if the port at the other end reverts to a regular port.
- For a switch port in on-demand D_Port mode, the port automatically reverts back to an E_Port after the tests are completed successfully.
- The following test options are available for link traffic: `-framesize` , `-nframes` , `-pattern` , `-payload` , `-time` . Both ends must be running the same release or the test reverts to legacy behavior.
- By default, forward error correction (FEC) is enabled on 32G and 64G ports, and the D_Port test is always run with FEC enabled.

General Limitations and Considerations for D_Port Tests

Consider the following issues when running D_Port tests:

- The link to be tested must be marginally functional and able to carry a minimal number of frames before it can become a D_Port link.
- D_Port testing is useful for diagnosing marginal faults only. A complete failure of any component cannot be detected.
- D_Port configuration is not supported on mezzanine cards.
- D_Port testing is not supported on adapter ports that are configured in CNA mode.
- Toggling the port on either side of the link during testing may result in a test failure.
- When a large number of D_Ports are configured, the test is run on one port per blade at a time, and other ports wait until the test is completed. No test begins until the fabric is stable.
- Before running on-demand D_Port tests on links that have the Dense Wavelength Division Multiplexing (DWDM) or Course Wavelength Division Multiplexing (CWDM), you must provision the port by using the `portcfgdport` command with the `dwdm` option.
- D_Port DWDM provisioning is applicable to static D_Ports, on-demand D_Ports, and dynamic D_Ports. During the configuration of a static D_Port using `portcfgdport --enable` , DWDM is automatically configured if the port was previously provisioned for DWDM.
- You can run a D_Port test on a maximum of eight links at a time. If you run the test on more than eight links simultaneously, false alarms may be raised.
- D-Port test may fail if it runs on multiple ports connected to HBA due to time constraints on the HBA firmware.
- In case of switch-to-HBA or Access Gateway-to-HBA connections with HBA v3.2.3 or later, limit D_Port tests to a maximum of eight D_Ports at once. Otherwise, there is a possibility of false alarms.
- If a remote SFP is not capable of running an optical loopback test or if a QSFP is connected by means of a breakout cable to an SFP, the test is skipped with the reason `No remote SFP or chip support`.
- During dynamic D_Port configuration, the switch is rebooted or there is a failover, it is possible for the ports to end up in an unsynchronized state. To clear this condition, enter the `portDportTest --clear all` command on a D_Port, an E_Port, or both, as appropriate.
- A D_Port test will fail if each switch in the test has the same domain ID. When you run the D_Port test on ISLs and spinfab, each switch should have unique domain IDs.

  NOTE

  A D_Port is not supported on an Ethernet port.
- There is no HA support for D_Port test options and results. Any information from a previous test is lost following a failover or reboot.
- During an HA failover or HA reboot or switch reboot or port toggle on one side of the link, the link is reinitialized and may restart the test. However, the test cannot proceed if the remote port is not ready to proceed further (the remote port may already be done with the D_Port test and in the final state). In such a case, the test will eventually fail with a `Remote port not ready` message. Restarting the test from either side will recover the port.
- Refer to the following topics in this guide for additional information:

Access Gateway Limitations and Considerations for D_Ports

The following are the limitations and considerations when using D_Ports with Access Gateways:

- Static D_Ports on an Access Gateway are supported only when there is no mapping between F_Ports and N_Ports; this includes static mapping and preferred port mapping. In addition, device (WWN) mapping is also not retained when a D_Port is used. If an Access Gateway port to be tested is mapped, the port mapping (including static and preferred port mapping) must be removed before the D_Port can be used. See Saving Port Mappings on an Access Gateway.
- With Dynamic D_Port mode on AG, when the user configures a static D_Port on the switch, the trunk configuration is backed up internally on the switch. Similarly, N_Port mappings, preferred mappings, and static mappings are saved on the AG. When the user removes the static D_Port configuration, the trunk configuration and AG mappings are restored.
- Dynamic D_Port on HBA: Enabling D_Port on the HBA automatically changes the AG port to dynamic D_Port mode, and the HBA-port-to-N_Port mapping is saved. Disabling the D_Port configuration on the HBA clears the dynamic D_Port configuration in the AG, and AG mappings are restored. For more details on D_Port support, refer to the *Brocade Fabric OS Access Gateway Administration Guide*.

8G LWL and ELWL SFP Transceiver Limitations for D_Ports

The following are the 8G LWL and ELWL SFP transceiver limitations when using D_Ports:

- On these transceivers, only the link traffic test is supported.
- On these transceivers, the cable length is displayed only for links that are greater than 1KM and for short cables, the length is displayed as `unknown` .

Support for Audit Logs

In previous releases, log messages were not generated when a port was configured or unconfigured as a D_Port.

The `switchShow` command was the only option available to verify whether a port was configured as a D_Port with Fabric OS 8.1.0, the following log messages are provided.

NOTE
The following messages are supported only for static D_Port configurations.

This example log message is generated when a port is configured as a D_Port.

```
4 AUDIT, 2020/02/16-22:12:16 (UTC), [PORT-1014], INFO, CONFIGURATION, NONE/admin/NONE/CLI, NA/Tyr1_DS/FID
 128, , Port (ID: 1) is not configured as D_Port.
```

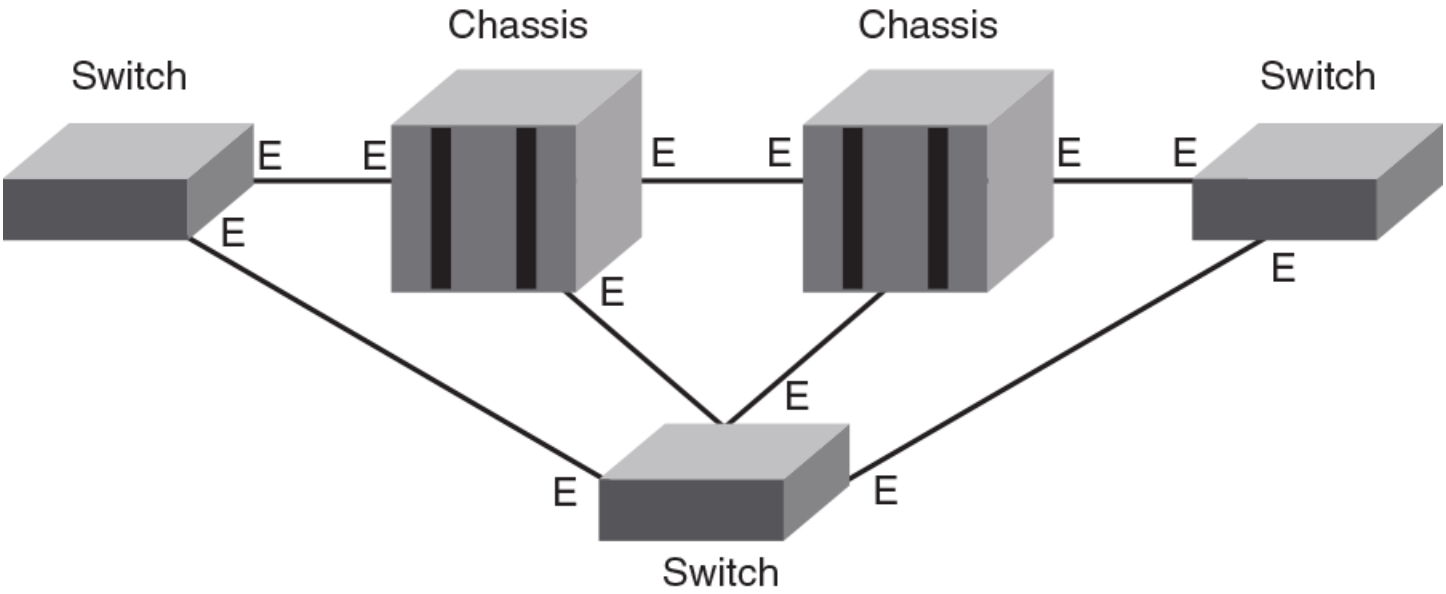
This example log message is generated when a port is unconfigured as a D_Port.

```
3 AUDIT, 2020/02/16-22:13:05 (UTC), [PORT-1013], INFO, CONFIGURATION, NONE/admin/NONE/CLI, NA/Tyr1_DS/FID
 128, , Port (ID: 1) is configured as Static D_Port.
```

Topology 1: ISLs

The following figure illustrates inter-switch links (ISLs) that connect multiple switches through a pair of chassis. The letter E represents E_Ports to be configured as D_Ports.

Figure 5: ISLs Connecting Multiple Switches and Chassis

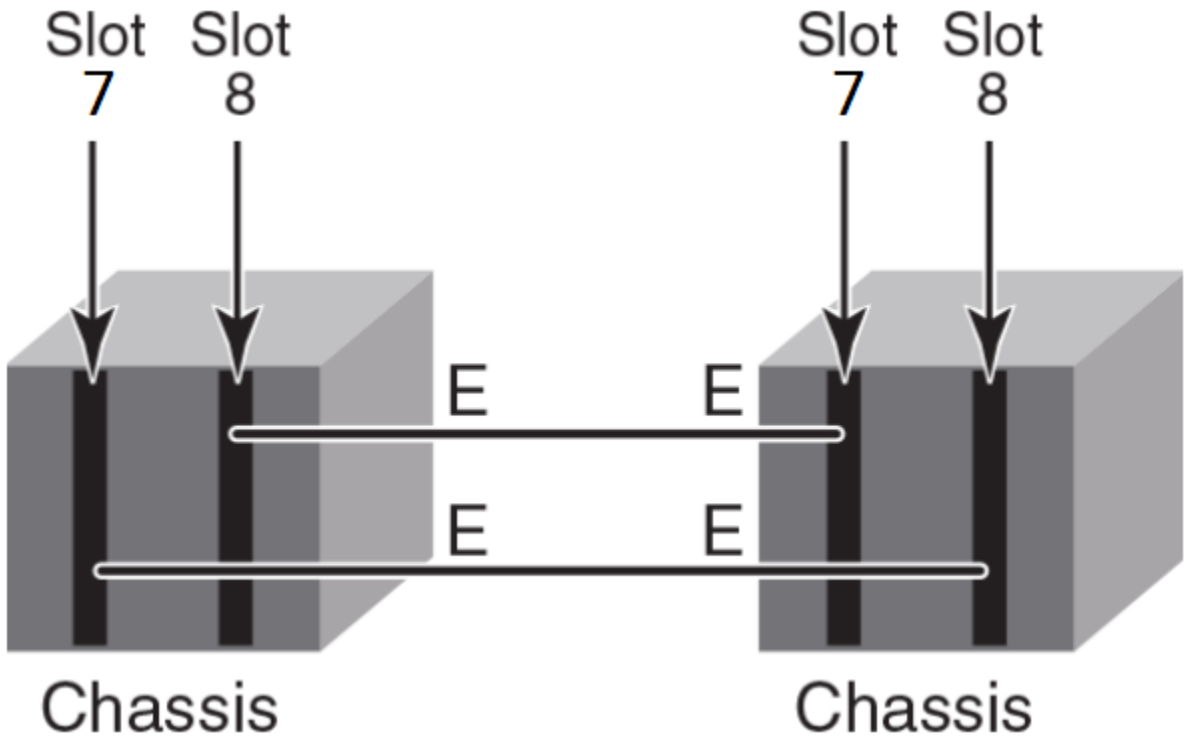


Only static-static and static-dynamic D_Port modes are supported on ISLs.

Topology 2: ICLs

The following figure illustrates inter-chassis links (ICLs) between slots 7 and 8 in corresponding chassis. The letter E represents E_Ports to be configured as D_Ports.

Figure 6: ICLs Connecting Chassis Blades



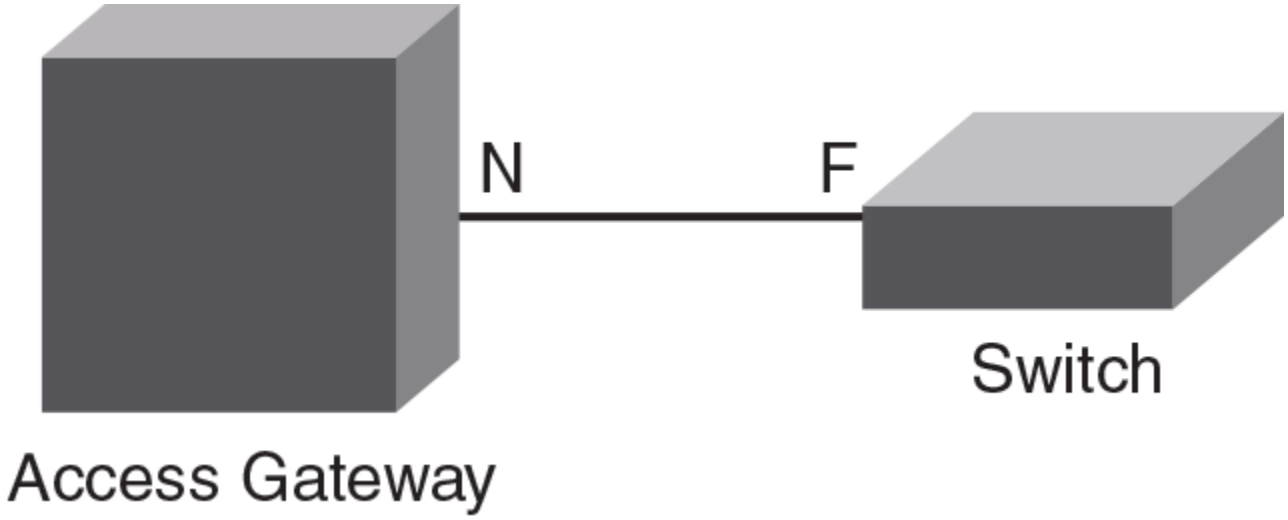
Static-static, static-dynamic, and on-demand-dynamic D_Port modes are also supported on ICLs.

Topology 3: Access Gateways

The following figure illustrates a switch configured as a single Access Gateway connected to a fabric switch. The letters N and F represent, an N_Port and an F_Port to be configured as D_Ports.

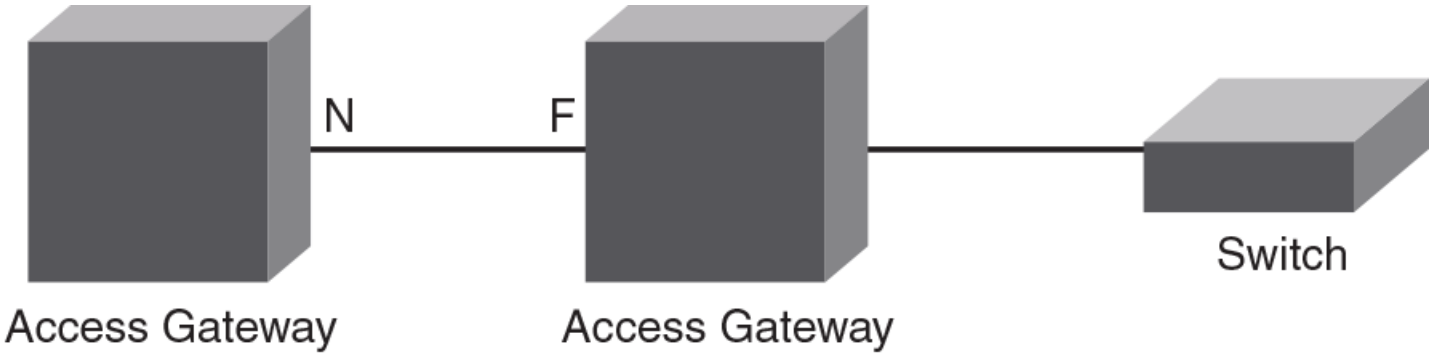
The Access Gateway mode is supported only on the Brocade G610, Brocade G620, Brocade G648, Brocade MXG610, and Brocade G720.

Figure 7: Single Access Gateway Connected to a Switch



The following figure illustrates multiple Access Gateways connected to a switch in a cascaded topology. The letters N and F represent, an N_Port and an F_Port to be configured as D_Ports.

Figure 8: Multiple Access Gateways Cascaded to a Switch

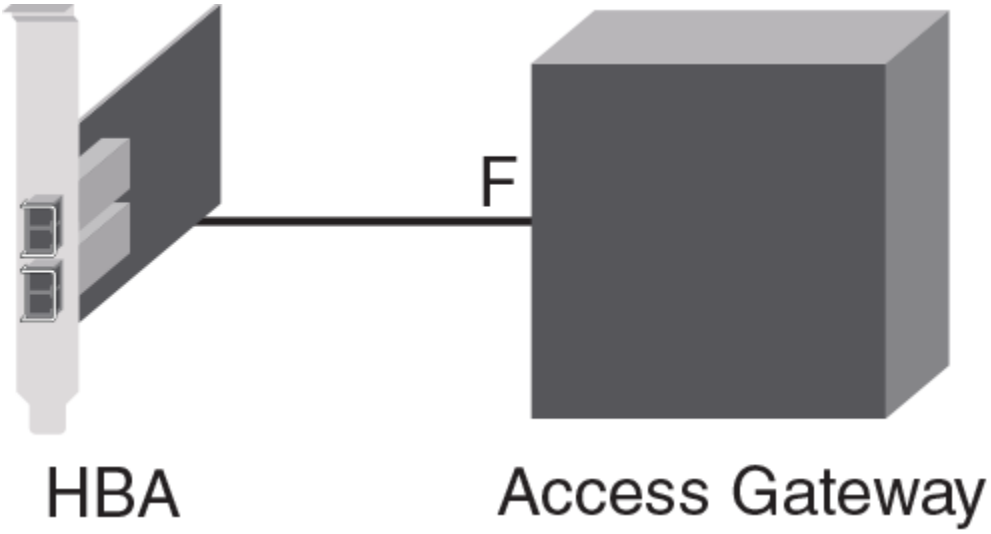


The above topology is supported only with static-static D_Port modes.

> **NOTE**
> N_Port-to-F_Port and device (WWN) mappings must be removed from an Access Gateway port before configuring the Access Gateway port as a D_Port. See Saving Port Mappings on an Access Gateway.

The following figure illustrates connectivity between an HBA and an Access Gateway. The letter F represents an F_Port to be configured as a D_Port.

Figure 9: HBA Connected to an Access Gateway



Static-static and static (HBA) - dynamic (AG) D_Port modes are supported.

Saving Port Mappings on an Access Gateway

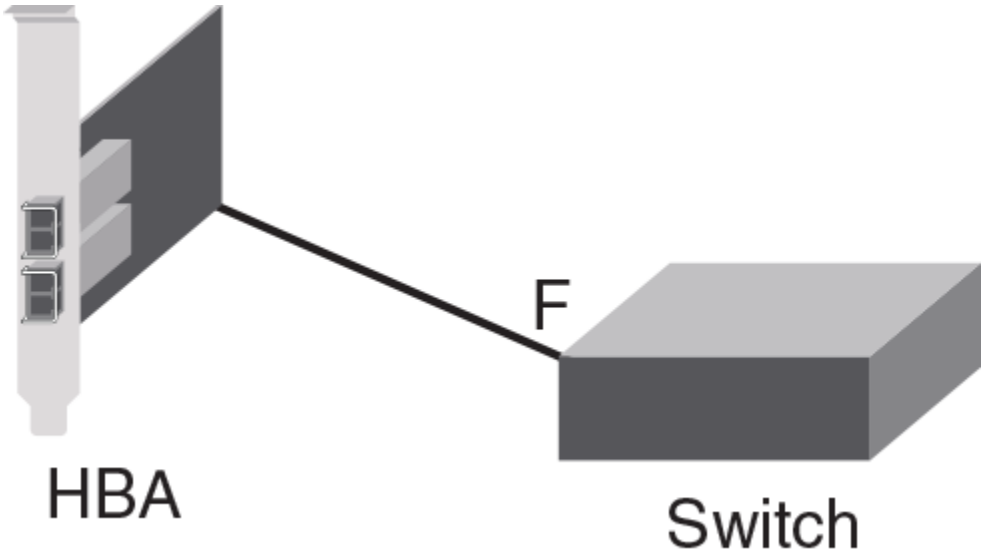
Before configuring ports as D_Ports on a switch configured as an Access Gateway, you must remove N_Port-to-F_Port and device (WWN) mappings. Fabric OS commands are available to save N_Port mappings. Once you save them, you can display the saved N_Port mappings to reconfigure them after the D_Port is disabled. A command is also available to delete saved N_Port mappings.

For more details, refer to Chapter 2, "Configuring Ports in Access Gateway Mode," in the *Brocade Fabric OS Access Gateway Administration Guide*.

Topology 4: HBA to Switch

The following figure illustrates connectivity between an HBA and a switch. The letter "F" represents an F_Port to be configured as a D_Port. This topology supports static-static and dynamic (switch) - static (HBA) D_Port mode. In dynamic mode, the switch port does not need to be configured explicitly as a D_Port. It comes up in D_Port mode when it receives a request from the remote port.

Figure 10: HBA Connected to Switch



For configuration details, refer to "Using D_Port with HBAs" in this chapter.

D_Port Loopback Plug Configurations

D_Port is supported on the following loopback topologies:

- Loopback plug directly connected to the SFP or QSFP module
- Loopback plug connected to the remote end of the cable connected to an SFP or QSFP module
- Cable loopback connected between two ports of the same switch

Using a D_Port in Static-Static Mode between Switches

You can configure D_Ports in static-static modes between switches (ISLs), chassis (ICLs), Access Gateways, and switch-Access Gateway links.

The sections "Enabling D_Port" and "Disabling D_Port" apply to topologies 1, 2, 3, and 4:

Enabling a D_Port in Static Mode

Use this procedure to configure a basic, automatic D_Port diagnostics session in static mode between two switches. The summary steps are as follows:

1. Disable ISL functionality on the ports.
2. Configure D_Port static mode on both ends of the link.
3. Enable ISL functionality on the ports.

ATTENTION
The automatic test might fail if you do not follow the sequence of steps exactly.

NOTE
"Port 1" and "Port 2" simply represent corresponding peer ports at opposite ends of the link to be tested. Switch A and Switch B can be in the same platform or different platforms supporting an end-to-end D_Port connection.

The detailed steps are as follows:

1. Disable Port 1 on Switch A.

```
switchA:admin> portdisable 1
```

2. Configure Port 1 on Switch A as a D_Port in static mode.

```
switchA:admin> portcfgdport --enable 1
```

3. Repeat Step 1 and Step 2 for the corresponding port (in this example, Port 2) on Switch B.

```
switchB:admin> portdisable 2
switchB:admin> portcfgdport --enable 2
```

4. Re-enable Port 1 on Switch A.

```
switchA:admin> portenable 1
```

5. Re-enable Port 2 on Switch B.

```
switchB:admin> portenable 2
```

   The basic test suite starts as soon as both ports are enabled and ready to perform the test.

6. While the test is running, you can enter a variety of `show` commands to confirm the D_Port configuration and view test results on an interface. See "Using D_Port show commands" at the end of this chapter.

   To view D_Port status and test results for an interface:

```
switch:admin> portdporttest --show 10/0/39

D-Port Information:
===================
Port:                           7
Remote WWNN:                    10:00:00:05:33:81:43:00
Remote port index:              71
Mode:                           Automatic
No. of test frames:             1 Million
Test frame size:                1024 Bytes
FEC (enabled/option/active):    Yes/No/No
CR (enabled/option/active):     Yes/No/No
Start time:                     Fri Feb 17 10:57:41 2023
End time:                       Fri Feb 17 10:57:47 2023
Status:                         PASSED
==============================================================================
Test                    Start time      Result          EST(HH:MM:SS)   Comments
==============================================================================

Link traffic test       22:49:26        PASSED          --------        ----------
==============================================================================
Roundtrip link latency:         49422 nano-seconds
Estimated cable distance:       4985 meters (4.985 Km)
Buffers required:               47 (for 2112 byte frames at 16Gbps speed)
Egress power:                   Tx: -2.6 dBm, Rx: -3.3 dBm, Diff: 0.7 dBm (Loss is within tolerable limit)
Ingress power:                  Rx: -2.5 dBm, Tx: -2.7 dBm, Diff: 0.0 dBm (No Loss)
```

7. To confirm D_Port test results for all ports, use the following command.

```
switch:admin> portdporttest --show all

Port State   SFP Capabilities Test Result
=============================================
24   ONLINE  ---              PASSED
26   ONLINE  ---              PASSED
33   OFFLINE ---              FAILED
```

8. *Optional* : To stop the test on both ends, use the `portDportTest --stop` command on both the ends. After stopping the test, verify manually that the test has stopped on both ends. You can restart the test on both ends using the `portDportTest --start/restart` command on any one of the ends. You do not need to run the same command on both ends of a single connection

Disabling a D_Port in Static Mode

Use this procedure to disable a D_Port diagnostics session in static mode.

NOTE
"Port 1" and "Port 2" simply represent corresponding peer ports at opposite ends of the link to be tested.

1. Disable Port 1 on Switch A.

```
switchA:admin> portdisable 1
```

2. Disable the D_Port functionality in static mode on Port 1 on Switch A.

```
switchA:admin> portcfgdport --disable 1
```

3. Repeat Steps 1 and Step 2 for Port 2 on Switch B.

```
switchB:admin> portdisable 2
switchB:admin> portcfgdport --disable 2
```

4. Reenable Port 1 on Switch A.

```
switchA:admin> portenable 1
```

5. Reenable Port 2 on Switch B.

```
switchB:admin> portenable 2
```

Using D_Ports in Dynamic Mode

Enabling dynamic D_Port switch-wide configuration forces the ports on that switch or chassis to respond to D_Port requests from the other end of the connection. It basically responds to a remote port request to change its mode to D_Port mode, and run diagnostic tests automatically. For more information on enabling dynamic D_Port mode for all ports in a switch or chassis, refer to "D_Port configuration mode and testing" in this chapter.

Preprovisioning D_Ports

In a normal scenario, you must disable a port before configuring it as a static D_Port. This is a disruptive operation and any command or procedure error could cause the wrong port to go down. To avoid such errors, you can preprovision a

port that needs to be configured as a D_Port. A preprovisioned port does not need to be disabled before being configured as a D_Port.

1. To add one or more ports to the D_Port provision list, use the `portcfgdport --provision -add` [slot/] *port_list* command. If the `-dwdm` option is specified, the ports in the provision list are provisioned for D_Ports over links with DWDM or CWDM.

   With the preprovisioning of D_Ports, links with DWDM or CWDM can support dynamic D_Port testing and on-demand D_Port testing.

   The following example shows how to provision a port with the DWDM option.

   ```
   Switch:admin> portcfgdport --provision -add -dwdm 7/16
   ```

   The following example shows how to provision a port without the DWDM option.

   ```
   Switch:admin> portcfgdport --provision -add 7/20
   ```

2. (Optional). To remove one or more ports from the provision list, use the `portcfgdport --provision -delete` [*slot/*] *port_list* command. Specifying the `-dwdm` is optional. When a port is removed from the provision list, the D_Port DWDM provisioning is automatically cleared.

   The following example shows how to delete a port with the DWDM option.

   ```
   Switch:admin> portcfgdport --provision -delete -dwdm 4/12
   ```

   The following example shows how to delete a port without the DWDM option.

   ```
   Switch:admin> portcfgdport --provision -delete 4/16
   ```

3. To list the ports in the provision list, use the `portcfgdport --provision -show` command, as in the following example.

   ```
   Switch:admin> portcfgdport --provision -show
    Slot Port D-Port provision DWDM
   ================================
      3    4      ON           OFF
      3    5      ON           OFF

   Switch:admin> portcfgdport --provision -show 3/2-5
    Slot Port D-Port provision DWDM
   ================================
      3    2      OFF          OFF
      3    3      OFF          OFF
      3    4      ON           OFF
      3    5      ON           OFF
   ```

   The following example shows a port that is not preprovisioned.

   ```
   Switch:admin>  portcfgdport --provision -show 3/2
    Slot Port D-Port provision DWDM
   ================================
      3    2      OFF          OFF
   ```

4. To enable D_Port mode on a preprovisioned port, use the `portcfgdport --enable` command. You do not need to disable the port before running this command. However, this command will display an error message if the particular port is not preprovisioned using the previous steps.

   Specifying `-dwdm` is optional. If the port is preprovisioned as DWDM, the port is automatically configured as DWDM.

   The following example enables the port as D_Port.

   ```
   Switch:admin> portcfgdport --enable 4/10
   ```

   The following example enables the port as DWDM.

   ```
   Switch:admin> portcfgdport --enable -dwdm 5
   ```

5. To disable D_Port mode on a preprovisioned port, use the `portcfgdport --disable` command.

   The following example disables the port as D_Port.

   ```
   Switch:admin> portcfgdport --disable 4/10
   ```

   The following example disables the port as DWDM.

   ```
   Switch:admin> portcfgdport --disable -dwdm 5
   ```

Using D_Port Mode between Switches and HBAs

When HBAs are used, D_Port mode initiates link-traffic diagnostic tests on the link between the HBA and the connected switch port. Results can be viewed from the switch by means of Fabric OS commands and from the HBA by way of the Brocade Command Line Utility (BCU) and Brocade Host Connectivity Manager (HCM) during or after the test. Once in D_Port mode, the adapter port does not participate in fabric operations, log in to a remote device, or run data traffic.

> **NOTE**
> The syntax in this section applies to HBAs only. Where HBAs are supplied by other vendors, view the appropriate GUI or CLI interface to see the results on the HBA side, and use the commands as provided by the vendor.

In dynamic D_Port mode, you can disable the physical port by using the `bcu port --disable` command. However, that command will not exit dynamic D_Port mode. When you enable the port again, the switch will again force the adapter port into D_Port mode if the switch port is still enabled as a D_Port.

The following sections apply to "Topology 4: HBA to switch":

- **Automatic mode configuration**
- **Dynamic mode configuration**
- **BCU D_Port commands**

Enabling a D_Port in Static Mode between a Switch and an HBA

This procedure enables a D_Port diagnostic session from the connected switch to an HBA. After the default test suite is run automatically, you can run specific tests manually to obtain additional detail.

1. Disable the switch port by using the `portDisable` command.
2. Configure the switch port that you want to enable as a D_Port by using the `portCfgDport --enable` command.
3. Disable the adapter port by using the adapter `bcu port --disable` command.
4. Enable the switch port by using the `portEnable` command.
5. Enable the adapter port as a D_Port by using the adapter `bcu diag --dportenable` command and configure test parameters.
6. Enable the switch port.

Using HBAs for D_Port Testing

This section illustrates how to enable Emulex or QLogic HBA cards for D_Port testing.

Cards must be installed in a server according to the manufacturer's instructions and must be connected to a Brocade switch.

NOTE
You should configure and enable dynamic D_Port Configuration on the HBA port, if the D_Port tests do not start after the switch port is configured as a static D_Port.

Enabling D_Port Testing with an Emulex HBA

This task illustrates how to enable D_Port testing with an Emulex HBA.

D_Port testing is supported on Emulex 16G, 32G and 64G cards. For the latest firmware and product-specific details, go to www.broadcom.com.

NOTE
D_Port implementations for different HBAs vary in FOS 9.0. Refer to the HBA vendor for the latest Emulex firmware/driver while executing the D_Port test. You can also check from the OneCommand™ Manager under the **Firmware Parameters** tab for each port.

NOTE
When the Emulex devices are connected to ZUA QSFP ports via a breakout cable, it is recommended to configure D_Ports on F_Ports from the switch side as well.

1. Configure the Brocade switch into dynamic D_Port mode as follows.
   a) Disable the switch by entering the `switchDisable` command.

      NOTE
      Dynamic D_Port is enabled by default.

```
switch:admn> switchdisable
```

   b) Enter the `configure` command, and then select `D-Port Parameters` and ensure that dynamic D_Port testing is enabled and on-demand port testing is disabled.

```
Configure...

  Fabric parameters (yes, y, no, n): [no]
  Virtual Channel parameters (yes, y, no, n): [no]
  F-Port login parameters (yes, y, no, n): [no]
  D-Port Parameters (yes, y, no, n): [no]  y
```

```
Dynamic D-Port (on, off):  on
On Demand D-Port (on, off):  off
```

2. Re-enable the switch by using the `switchEnable` command.

```
switch:admin> switchenable
```

3. From the host server, start D_Port testing by selecting the Emulex OneCommand Manager.
4. For each port under test, click **Firmware parameters**, and then enable by selecting **Dynamic D_Port**.

NOTE
You must disable the Dynamic D_Port mode/feature from the HBA side using the OneCommand Manager (OCM) before starting the D_Port testing using OCM.

5. Reboot the host and wait for two to three minutes before you start the test.
6. Reset the port on the HBA end by selecting the Reset FC port.
7. Click the **Diagnostics** tab, and then click **D_Port Tests** under the OCM.

Enabling D_Port Testing with a QLogic HBA

This task illustrates how to enable D_Port testing with a QLogic HBA.

D_Port testing is supported on QLogic 16G, 32G and 64G cards. For the latest firmware/driver and product-specific details, go to www.qlogic.com. If the latest firmware/driver supporting D_Port testing is installed in the server, nothing further needs to be done on the server side.

NOTE
Please refer to the HBA vendor while executing the D_Port test. For QLogic Dynamic D_Port testing, you can use the QConvergeConsole user interface to execute the "Run Diagnostics Test".

Before you configure and start the D_Port test automatically, you must check the following on the QLogic HBA:

- Verify if the QLogic HBA has "Enabled Diagnostics Port Status" under the "QConvergeConsole" -> Diagnostics tab -> Diagnostics Port Test tab.
- You can also use the `fdmiShow` command to display Fabric-Device Management Interface (FDMI) information for all host bus adapters (HBAs) and ports.

1. On the Brocade switch, convert the port from an F_Port to a D_Port, disabling the specified F_Port by entering the `portDisable` *`port_ID`* command.

```
switch:admin> portdisable 1/1
```

2. Enter the `portCfgDport --enable` *`port_ID`* command.

```
switch:admin> portcfgdpdort --enable 1/1
```

3. Enable the port by using the `portEnable` *`port_ID`* command.

```
switch:admin> portenable 1/1
```

The D_Port test begins automatically.

BCU D_Port Commands

The following BCU commands can be used for D_Port configuration and control:

NOTE
Refer to the HBA user guide to verify the usage of the D_Port feature on HBAs that support the D_Port functionality.

- `bcu diag --dportenable` – Enables D_Port on a specific port, sets the test pattern, and sets the frame count for testing.
- `bcu diag --dportdisable` – Disables D_Port on a specific port and sets the port back to an N_Port or NL_Port.
- `bcu diag --dportshow` – Displays test results for a test in progress on a specific port.
- `bcu diag --dportstart` – Restarts a test on a specific port when the test has completed.
- `bcu port --list` – Displays the D_Port enabled or disabled state on the adapter and connected switch.

Host Bus Adapter Limitations and Considerations for D_Ports

In addition to the items listed in General Limitations and Considerations for D_Port Tests, keep in mind the following limitations and considerations when using a D_Port with a host bus adapter (HBA):

- D_Port is supported on Gen 6 platforms if you have a Fabric Vision license present on the switch.
- D_Ports are not supported in a configuration of an HBA to another HBA (in target mode).
- D_Ports on the HBA do not support forward error correction (FEC) and credit recovery (CR). If these features are enabled on the switch side, the HBA ignores them.
- Because of SFP electrical wrap (EWRAP) bleed-through, the HBA will receive some broken frames. This causes the port statistic error counter to increase. Examples are “CRC err”, “bad EOF”, and “invalid order set”. You should ignore these port statistics on the HBA.
- The following commands from the switch are not supported by the HBA, and the HBA will drop them:
  - `portdporttest --restart`
  - `portdporttest --setarg`
- The Qlogic HBA does not support manual D_Port tests that are started from the switch side by means of the `portdporttest` command with suboptions (`--start` , `--setargs` , `--restart` , and so on). It supports only automatic tests when the port is configured as a D_Port by means of the `portcfgdport --enable` command from the switch side.
- When Emulex HBAs are used, a D_Port test can be triggered from both the switch and Emulex HBA side. The supported D_Port configurations are “Switch (Dynamic D_Port) /Emulex HBA (On-Demand D-port)” and "Switch(Static) /HBA(Dynamic)".
- The maximum number of D_Ports on which the tests can run simultaneously depends on the HBA firmware version.

Table 51: Limitation on Number of D_Ports for Simultaneous Tests

HBA Firmware Version	Maximum Number of D_Ports on Which Tests Can Be Run Simultaneously
HBA v3.2.0	4
HBA v3.2.6	8

- You must configure D_Port using the `portcfgdport` command from the switch side and then start the test from the HBA side for a 32G QSFP.
- As soon as the HBA is configured as the static D_Port, the switch changes to dynamic D_Port mode. After the test is completed and the switch is rebooted, the switch port changes back to G_Port mode. To resolve this issue, remove the static D_Port configuration on the HBA.
- Powering off and on or plugging in and out slots containing ports in D_Port mode results in those ports losing the dynamic D_Port state when the slot or port is back up. If this happens, you must reconfigure the static D_Port mode on the HBA.
- D_Port is supported on Qlogic HBAs only at link speeds of 32G and 16G.

The following considerations apply to 32G SFPs and QSFPs.

With the introduction of the new SFPs and QSFPs, FEC and FEC with Transmitter Training Signal (TTS) mode are enabled by default for 32G. FEC cannot be disabled in this case. The following table summarizes the state of the FEC fields and the resulting behavior.

Table 52: FEC Field State and Behavior for 32G Tests

Field	State/Behavior
Enabled	The state is “Yes” if the port is FEC capable and FEC is configured by means of the `portcfgfec` command. For 32G SFPs/QSFPs at a link speed of 32G, FEC is enabled by default and cannot be disabled.
Option	The state is “Yes” if the `portdporttest` command is used with the `-fec` option. For a link speed of 32G, FEC is auto-enabled, irrespective of this option.
Active	The state is always “Yes” for 32G alone. This depends on the capability of local and remote ports and does not depend on the `-fec` option alone.

The output of the `portdporttest --show` command displays “FEC = Yes” for both Enabled and Active for 32G only. The output is not changed for port speeds of 10G or 16G.

Confirming SFP and Link Status with an HBA

The steps in the following example illustrate how the `bcu diag --dportenable` command will fail with an SFP installed but without a connection to the switch.

1. Confirm the initial port status.

```
# bcu port --list
-------------------------------------------------------------------------
Port#  FN  Type  PWWN/MAC                FC Addr/  Media  State       Spd
                                         Eth dev
-------------------------------------------------------------------------
1/0    -   fc    10:00:8c:7c:ff:1c:e9:00  160000    sw     Linkup      16G*
       0   fc    10:00:8c:7c:ff:1c:e9:00  160000    sw     Linkup      16G*
1/1    -   fc    10:00:8c:7c:ff:1c:e9:01  --        sw     Linkdown    ---
       1   fc    10:00:8c:7c:ff:1c:e9:01  --        sw     Linkdown    ---
-------------------------------------------------------------------------
```

2. Disable the port.

```
# bcu port --disable 1/0
port disabled
```

3. Remove the connection to the switch and attempt to enable the D_Port.

```
# bcu diag --dportenable 1/0
ERROR: Timer expired - Retry if persists contact support
```

4. Install an SFP and attempt to enable the D_Port.

```
# bcu diag --dportenable 1/0
ERROR: Switch port is not D_Port capable or D_Port is disabled
```

5. Connect to the HBA without the SFP and disable the native port.

```
# bcu port --disable 1/0
port disabled
```

6. Attempt to enable the D_Port.

```
# bcu diag --dportenable 1/0
ERROR: SFP is not present.
D-port will be enabled but it will be operational only after inserting a valid SFP.
```

Using a D_Port in On-demand Mode

Enabling on-demand D_Port switch-wide configuration forces the ports on that switch or chassis to respond to an internal requests within the switch as a result of certain events. The switch basically responds to internal request to change a port mode to D_Port mode, and run diagnostic tests automatically. For more information on enabling on-demand D_Port mode for all ports in a switch or chassis, refer to "D_Port configuration modes and nature of test," above.

When an on-demand D_Port-capable switch or chassis comes online, the switch checks if the other end of the connection supports dynamic D_Port mode. If dynamic D_Port is supported on the other end, the switch changes the remote port to D_Port mode, and then triggers diagnostic tests automatically. The D_Ports change to normal port mode after successful completion of the tests.

Using the fabriclog Command

This command can be enabled or disabled on either a fabric log or a D_Port log.

During D_Port testing that involves a large number of ports, the logs for specific ports can become “wrapped around.” Log file wrapping overwrites existing data with incoming data when the maximum log file size is exceeded. This creates a problem for logging on ports of interest, particularly if a test fails and logging continues unnecessarily.

To remedy this, a new failstop option has been added to the `fabriclog` command (`fabriclog` -f). When this option is enabled, The D_Port fabric is stopped and disabled when a test fails, making the log available for debugging purposes. To resume logging, the user must reenable logging explicitly.

The complete syntax is as follows. Adding the optional `dport` keyword applies the command only to D_Port logs.

To display fabric logs: `fabriclog -s | --show dport`

To clear fabric logs: `fabriclog -d | --clear dport`

To disable fabric logging: `fabriclog -c | --disable dport`

> **NOTE**
> If the `dport` keyboard is specified, only D_Port fabric logs are disabled. if it is not specified, only fabric logs are disabled.

To enable fabric logging: `fabriclog -e | --enable dport`

> **NOTE**
> If the `dport` keyword is specified, only D_Port fabric logs are disabled. if it is not specified, only fabric logs are disabled.

To stop and disable D_Port fabric logging upon failure of the first D_Port test. `fabriclog -f | --failstop dport`

> **NOTE**
> The `failstop` option is applicable only when the `dport` keyword is applied. If the `failstop` option is set, the D_Port fabric log is stopped and disabled when the first D_Port test fails. This option is cleared automatically when the fabric log for D_Port is reenabled.

The following example shows the effect of this operand.

```
switch:admin> fabriclog -failstop dport
fabriclog failstopset successfully
sw0:FID128:admin> fabriclog -s dport
```

```
Time Stamp Input and *Action S, P Sn,PnPort Xid
================================================================================
Switch 0; Thu Feb 6 03:27:13 2020 GMT (GMT+0:00)
03:27:13.301915 DP:D_PORT_FINAL(TEST_START)->D_PORT_INIT A2,P3 A2,P30 NA
03:27:13.302013 MSG_FAB_DIAG_CMD, stage (cold done) A2,P3 A2,P30 NA
03:27:13.302034 DiagCmdSend:Cnt=1,Cmd=136 A2,P3 A2,P30 NA
:
Number of entries: 119
Max number of entries: 2048
fabriclog is disabled
failstopis set
```

To display the help for the command: `fabriclog -h | --help`

Note the following considerations and limitations for this option:

- This option is not synchronized to a standby control processor and must be specified again following a high-availability (HA) failover.
- This option is not persistent and must be specified again on the device following a manual or HA reboot.
- This option stops the D_Port fabric log when the first D_Port test fails. Consequently, the debugging of multiple test failures may not be possible simultaneously, as the fabric log may not be available for subsequent failures. To remedy this, the user must resolve the first test failure before addressing subsequent failures.

Calculating Buffers for Long-Distance Cables

Consider the following when making D_Port measurements over long-distance cables.

When D_Port testing is done over long-distance cables, the values returned by the `portbuffershow` command are calculated according to the buffers required, the frame size, and the cable length provided by the user. For D_Ports the "Buffers required" value displayed by the `portdporttest --show` command is calculated according to link latency, link speed, and a fixed frame size of 2112 (the default). If the user-provided values are the same, then the buffer values displayed by both the `portbuffershow` and `portdporttest --show` commands will be the same. If the user-provided values are different, then the displayed values will be different.

With the `portbuffershow` command, the buffers are calculated according to user-provided values as well as those provided by the `portcfglongdistance` command. The buffers required, frame size, and cable length are provided by the user. The default frame size used in this case is 2048.

With the `portdporttest` command, the "Buffers required" value is calculated according to link latency, link speed, and frame size (2112, the default). The link latency is calculated according to the actual cable distance, and not the user-specified value.

Support for Audit Logs

In previous releases, log messages were not generated when a port was configured or unconfigured as a D_Port.

The `switchShow` command was the only option available to verify whether a port was configured as a D_Port with Fabric OS 8.1.0, the following log messages are provided.

NOTE
The following messages are supported only for static D_Port configurations.

This example log message is generated when a port is configured as a D_Port.

```
4 AUDIT, 2020/02/16-22:12:16 (UTC), [PORT-1014], INFO, CONFIGURATION, NONE/admin/NONE/CLI, NA/Tyr1_DS/FID
 128, , Port (ID: 1) is not configured as D_Port.
```

This example log message is generated when a port is unconfigured as a D_Port.

```
3 AUDIT, 2020/02/16-22:13:05 (UTC), [PORT-1013], INFO, CONFIGURATION, NONE/admin/NONE/CLI, NA/Tyr1_DS/FID
 128, , Port (ID: 1) is configured as Static D_Port.
```

Using D_Port Show Commands

This section presents a variety of options for viewing the results of D_Port testing.

In addition to using the `portdporttest` command to start or stop D_Port tests, you can also use it to show a variety of detailed test results.

You can display the complete results from either the responder or the initiator switch. If the initiator switch is running Fabric OS v7.1.x or earlier, the responder displays only the local D_Port results, and you must query the initiator to see the complete results.

The following example shows basic D_Port results for a specified port:

```
device:admin> portdporttest --show 26
D-Port Information:
===================
Port:           26
Remote WWNN:    10:00:00:05:33:13:2f:b5
Remote port index:    42
Mode:           Automatic
FEC (enabled/option/active):    Yes/No/No
CR (enabled/option/active):    Yes/No/No
Start time:            Fri Feb 17 10:57:41 2023
End time:            Fri Feb 17 10:57:47 2023
Status:              PASSED
================================================================================
Test                  Start time   Result          EST(secs)  Comments
================================================================================

Link traffic test     01:43:15     PASSED           --        ----------
================================================================================
Roundtrip link latency:        49422 nano-seconds
Approximate cable distance:    4985 meters (4.985 Km)
Buffers required:        47 (for 2112 byte frames at 16Gbps speed)
Egress power:            Tx: -2.2 dBm, Rx: -4.2 dBm, Diff: 2.0 dB (Cable power loss is within tolerable limit)
Ingress power:            Rx: -6.2 dBm, Tx: -1.6 dBm, Diff: 4.6 dB (Cable power loss is within tolerable
 limit)
```

The following example shows the `portdporttest --show` output for port 26 where the link traffic test fails:

```
device:admin> portdporttest --show 26
D-Port Information:
===================
Port:           26
Remote WWNN:    10:00:00:05:33:13:2f:b5
Remote port index:    42
Mode:           Automatic
Start time:     Wed Feb  2 01:41:43 2023
End time:       Wed Feb  2 01:43:23 2023
Status:         PASSED
================================================================================
Test                  Start time   Result          EST(secs)  Comments
```

```
================================================================================

Link traffic test     01:43:15     FAILED           --        ----------
================================================================================
Roundtrip link latency:        49422 nano-seconds
Approximate cable distance:    4985 meters (4.985 Km)
Buffers required:               1 (for 1024 byte frames at 16Gbps speed)
Egress power:                   Tx:-3.3 dBm, Rx: Not Avail
Ingress power:                  Rx:-3.5 dBm, Tx: Not Avail
```

Enter `portdporttest --show all` to display the capabilities and test results of all the D_Ports in a switch, as shown in the example below:

```
switch:admin> portdporttest --show all
Port  State     SFP Capabilities  Test Result
============================================
24    ONLINE    --                PASSED
26    ONLINE    --                FAILED
33    ONLINE    --                PASSED
```

Enter `switchshow` to see detailed switch and D_Port information, as shown in the example below:

```
device:admin> switchshow
switchName:     switch_10
switchType:     109.1
switchState:    Online
switchMode:     Native
switchRole:     Principal
switchDomain:   1
switchId:       fffc01
switchWwn:      10:00:00:05:33:13:2f:b4
zoning:         OFF
switchBeacon:   OFF
FC Router:      OFF
Allow XISL Use: ON
LS Attributes:  [FID: 10, Base Switch: No, Default Switch: No, Address Mode 0]
Index Port Address Media Speed State     Proto
============================================
  24  24   010000   id    N16   Online      FC  D-Port Loopback->Port 24
  26  26   010200   id    N16   Online      FC  D-Port segmented,(D-Port mode mismatch)
  33  33   010300   id     N8   Online      FC  D-Port 10:00:00:05:33:13:2f:b5
```

The following example illustrates D_Port test output at 32G:

```
device:admin>  portdporttest --show 2
D-Port Information:
===================
Port:                            2
Remote WWNN:                10:00:00:27:f8:f0:26:40
Remote port index:                0
Mode:                         Manual
No. of test frames:                1 Million
Test frame size:                1024 Bytes
FEC (enabled/option/active):        Yes/No/Yes
```

```
CR (enabled/option/active):        No/No/No
Start time:                        Tue Jun 23 07:27:43 2023
End time:                        Tue Jun 23 07:28:15 2023
Status:                         PASSED
================================================================================
Test                 Start time            Result        EST(HH:MM:SS)    Comments
================================================================================

Link traffic test      07:28:10            PASSED         --------        ----------
================================================================================
Roundtrip link latency:        27422 nano-seconds
Approximate cable distance:    2785 meters (2.785 Km)
Buffers required: 1 (for 2112 byte frames at 32gbps speed)
Egress power:     Tx: 0.3  dBm, Rx: -3.6 dBm, Diff: 3.9 dBm (Loss is within tolerable limit)
Ingress power:    Rx: -4.1 dBm, Tx: 0.3  dBm, Diff: 4.4 dBm (Loss is within tolerable limit)
```

The following example illustrates D_Port test output for a longer test duration:

```
device:admin> portdporttest --show 31
D-Port Information:
===================
Port:                31
Remote WWNN:            10:00:50:eb:1a:0d:be:08
Remote port index:        31 (External loopback)
Mode:                Manual
Test Duration (HH:MM):        00:01
Test frame size:        1024 Bytes
FEC (enabled/option/active):    Yes/No/No
CR (enabled/option/active):    Yes/No/No
Start time:            Fri Apr 15 05:14:20 2023
End time:            -------------------
Status:                IN PROGRESS
================================================================================
Test             Start time    Result        EST(HH:MM:SS)    Comments
================================================================================

Link traffic test      --------    NOT STARTED    --------    ----------
================================================================================
Roundtrip link latency:        21422 nano-seconds
Approximate cable distance:    2185 meters (2.185 Km)
Egress power:                   Tx: -2.9 dBm, Rx: Not Avail.
Ingress power:                  Rx: -2.8 dBm, Tx: Not Avail.
```

Entere `portcfgshow` to see which ports are D_Port-enabled, as shown in the example below:

```
device:admin> portcfgshow
Ports of Slot 0        24  26  27
----------------------+---+---+---
Octet Speed Combo      1   1   1
Speed                  AN  AN  AN
AL_PA Offset 13        ..  ..  ..
Trunk Port             ON  ON  ON
Long Distance          ..  ..  ..
.....
```

```
.....
Port Auto Disable      ..  ..  ..
CSCTL mode             ..  ..  ..
D-Port mode            ON  ON  ON
D-Port over DWDM       ..  ..  ..
Compression            ..  ..  ..
Encryption             ..  ..  ..
FEC                    ON  ON  ON
Fault Delay             0   0   0
    where AE:QoSAutoEnable, AN:AutoNegotiate, ..:OFF, -:NotApplicable, ??:INVALID
```

Enhanced Support for QSFPs

From Fabric OS v9.2.0, the electric and optical loopback test on QSFP is not supported. The ISL-to-ISL connections are supported, but the ICL-to-ICL connections are not supported. Below are the supported connections:

- 32G QSFP ISL < -- > 32G QSFP ISL
- 32G QSFP ISL < -- > 32G SFP ISL
- 32G QSFP ICL < -- > 32G QSFP ICL
- Gen 7 QSFP ICL < -- > Gen 7 QSFP ICL

Limitations and Considerations

If one end of the link has older 16G or 32G QSFPs or QSFPs that do not support electrical wrap or optical wrap, and the other end supports this feature, the electrical loopback test will run on the end that supports the feature. The optical loopback test is not supported.

From Fabric OS v9.2.0, If the initiator has Fabric OS v9.2.0 firmware version, then both the electrical and optical loopback tests will not run, and if the responder has any previous firmware version, then the electrical test will be performed and optical test will be skipped. If the initiator has any previous firmware version, then the electrical test will be performed and the optical test will be skipped as the remote end does not support the O_WRAP. If the responder has Fabric OS v9.2.0, then both the electrical and optical will be skipped.

Beginning with Fabric OS 9.0.0, when a port is configured as a static D_Port, the D_Port test will automatically start on the configured D_Ports when the static D_Port end switch is rebooted. However, reboot on the dynamic D_Port switch will not run the D_Port test on dynamically configured D_Ports and the test status will be marked as STOPPED.

Before Fabric OS 8.2.0, when the D_Port test was started on multiple QSFP channels, the test would run simultaneously on multiple channels. For example, the electrical loopback test ran on channel 1, then the electrical loopback started the test on channel 2, followed by an optical loopback test on channel 1, and so on. With Fabric OS 8.2.0, the tests are sequenced within a QSFP. This means that the entire test now runs on one channel, and then the test starts on the next channel in the QSFP. For example, the electrical loopback test runs on channel 1, then the optical loopback test runs on channel 1, then the link traffic test runs on channel 1, followed by the electrical loopback test on channel 2, and so on. The sequencing is within the quad only.

NOTE
From Fabric v9.2.0, this sequence is not supported.

In Fabric OS 8.2.0, support is provided for the D_Port test if the channels within the QSFP are configured in different LSs. Channels within the QSFP must still be configured as static a D_Port to run the D_Port test.

For the D_Port test on SmartOptics SFPs, the user must follow the cable length requirements as per the SFP specification of the modules.

ATTENTION

The following restrictions apply to both 32G and 16G breakout QSFPs and 32G fixed-speed QSFPs. These restrictions are not applicable if these QSFPs are in ICL ports.

- Fabric OS enforces the same static D_Port configuration for all channels in the QSFP ports, for 32G and 16G breakout QSFPs and 32G fixed-speed QSFPs.
- Fabric OS blocks and skips on-demand D_Port tests for 32G and 16G breakout QSFPs and 32G fixed-speed QSFPs.
- Fabric OS enforces either static or dynamic D_Port configuration for all channels of the Gen 7 ICL QSFP starting with serial no. "BAR".
- A warning message appears when the static D_Port configuration for QSFPs is changed.

With these restrictions, an Emulex HBA cannot run on-demand D_Port tests. For an Emulex HBA, you must configure a static D_Port on the switch side and initiate D_Port tests from the Emulex HBA side.

Example Output

Below is the example output for a SmartOptics SFP on ISL ports:

```
switch> portdporttest --show 55
D-Port Information:
===================
Port:                55
Remote WWNN:            10:00:00:27:f8:f0:26:38
Remote port index:         55
Mode:                Manual
No. of test frames:         1 Million
Test frame size:         1024 Bytes
FEC (enabled/option/active):    Yes/No/Yes
CR (enabled/option/active):    Yes/No/No
Start time:            Mon Apr 18 09:57:43 2016
End time:            Mon Apr 18 09:57:50 2016
Status:                PASSED
=============================================================================
Test                      Start time    Result        EST(HH:MM:SS)    Comments
=============================================================================

Link traffic test      09:57:46    PASSED         --------    ----------
=============================================================================
Roundtrip link latency:        1116 nano-seconds
Approximate cable distance:    unknown
Buffers required:            1 (for 2112 byte frames at 32Gbps speed)
Egress power:                             Tx: Not Avail, Rx: -1.6 dBm.
Ingress power:                         Rx: -0.5 dBm, Tx: -23.6dBm, Diff: 0.0 dBm (No Loss)62:admin>
```

Switch Types and Blade IDs

The switchType is a field displayed in the `switchshow` command output. When you gather information to give to your switch support provider, you may be asked for the switch model. If you do not know the model, use the "switchType to B-Series Model Conversions" table in this section to convert the switchType to a B-Series model number.

```
device:admin> switchshow
switchName:     4thfloor_A
switchType:     162.0  <=== Convert this number using the following table.
switchState:     Online
switchMode:     Native
switchRole:     Principal
switchDomain:     1
switchId:    fffc00
switchWwn:     10:00:00:00:00:00:00:00
zoning:         OFF
switchBeacon:     OFF
FC Router:     OFF
FC Router BB Fabric ID:     128
```

In the preceding example, the number 162 is the switchType and .0 is the revision of the switch motherboard. The revision number is not necessary when converting the number. Convert the value using the following table.

Table 53: switchType to B-Series Model Conversions

switchType	B-Series Switch Model	Base Switch Speed
162 or 183	G620	32G, 64-port switch which includes 4 4x32G QSFP ports
165	X6-4	32G, 256-port core fabric backbone plus 16 4xGen 6 ICLs, total 64-port ICLs
166	X6-8	32G, 512-port core fabric backbone plus 32 4xGen 6 ICLs, total 128-port ICLs
170	G610	32G, 24-port switch
173 or 184	G630	32G, 128-port switch, which includes 8 4x32G QSFP-ports
178	7810 Extension Switch	32G, 12-port extension switch
179	X6-4+ upgraded to X7-4	64G, 192-port core fabric backbone plus 16 4xGen 7 ICLs, total 64-port ICLs
180	X6-8+ upgraded to X7-8	64G, 384-port core fabric backbone plus 32 4xGen 7 ICLs, total 128-port ICLs
181	G720	64G, 56-port switch
189	G730	64G, 128-port switch
190	7850 Extension Switch	64G, 24-port extension switch
179	X7-4	64G, 192-port core fabric backbone plus 16 4xGen 7 ICLs, total 64-port ICLs
180	X7-8	64G, 384-port core fabric backbone plus 32 4xGen 7 ICLs, total 128-port ICLs

NOTE
For more information about the B-Series switch models, refer to the relevant hardware installation guide.

Use the following table to find the description of the blade model that is displayed in the output from the `slotshow` command.

```
device:admin> slotshow
Slot   Blade Type     ID    Model Name     Status
```

```
-------------------------------------------------
 1     CP BLADE    220     CPX7           ENABLED
 2     CP BLADE    220     CPX7           ENABLED
 3     SW BLADE    216     FC64-48        ENABLED
 4     SW BLADE    216     FC64-48        ENABLED
 5     SW BLADE    216     FC64-48        ENABLED
 6     SW BLADE    216     FC64-48        ENABLED
 7     CORE BLADE  215     CR64-8         ENABLED
 8     CORE BLADE  215     CR64-8         ENABLED
 9     AP BLADE    186     SX6            ENABLED
 10    SW BLADE    204     FC32-64        ENABLED
 11    SW BLADE    204     FC32-64        ENABLED
 12    AP BLADE    186     SX6            ENABLED
```

Table 54: B-Series Blade Model Descriptions

Blade ID	B-Series Blade Model	Description
175	CPX6+	X6 Director control processor blade upgraded to support Gen 7
175	CPX6	X6 Director control processor blade
176	CR32-4	4x32G, 8-FC ports core routing blade
177	CR32-8	4x32G, 16-FC ports core routing blade
178	FC32-48	32G, 48-FC ports blade
204	FC32-64	32G, 64-FC ports blade
186	SX6	32G, 16-FC port FCIP extension blade
216	FC64-48	64G, 48-FC port blade
232	FC64-64	64G, 64-FC port blade
218	FC32-G7-48	32G, 48-FC port blade
214	CR64-4	4x64G, 4-FC ports core routing blade
215	CR64-8	4x64G, 8-FC ports core routing blade
220	CPX7	X7 Director control processor blade
220	CPX[a]	X6 Director control processor blade with switch ID 165.5 or 166.5.

a. In the Fabric OS 9.1.0b release, the CPX blade is displayed as CPX7 for X6 Directors with switch type 165.5/166.5.

Hexadecimal Conversion

Hexadecimal Overview

Hexadecimal, also known as hex, is a numeral system with a base of 16, usually written by means of symbols 0-9 and A-F (or a-f). Its primary purpose is to represent the binary code that computers interpret in a format easier for humans to remember. It acts as a form of shorthand, in which one hexadecimal digit takes the place of four binary bits. For example, the decimal numeral 79, with the binary representation of 01001111, is 4F (or 4f) in hexadecimal, where 4 = 0100 and F = 1111.

Hexadecimal numbers can have either an *0x* prefix or an *h* suffix. The address 0xFFFFFA is the same address as FFFFFA*h*. This type of address with 6 digits representing 3 bytes, is called a hex triplet. Fibre Channel uses hexadecimal notation in hex triplets to specify well-known addresses and port IDs.

Example Conversion of the Hexadecimal Triplet Ox616000

Notice that the PID (610600 - in bold) in the `nsShow` output is in hexadecimal.

```
switch:admin> nsshow
{
 Type Pid    COS     PortName                NodeName                 TTL(sec)
 N    610600;    2,3;10:00:00:00:c9:29:b3:84;20:00:00:00:c9:29:b3:84; na
    FC4s: FCP
    NodeSymb: [36] "Emulex LP9002 FV3.90A7  DV5-5.10A10 "
    Fabric Port Name: 20:08:00:05:1e:01:23:e0
    Permanent Port Name: 10:00:00:00:c9:29:b3:84
    Port Index: 6
    Share Area: No
    Device Shared in Other AD: No
    Redirect: No
    LSAN: Yes
The Local Name Server has 1 entry }
```

1. Separate the 6 digits into triplets by inserting a space after every 2 digits: 61 06 00.
2. Convert each hexadecimal value to a decimal representation:

   61 = Domain ID = 97

   06 = Area (port number) = 06

   00 = Port (AL_PA) = 0 (not used in this instance, but is used in loop, shared areas in PID assignments on blades, NPIV, and Access Gateway devices)

   Result: hexadecimal triplet 610600 = decimal triplet 97,06,00

   See Decimal-to-Hexadecimal Conversion Table when converting hexadecimal values to a decimal representation.

Decimal-to-Hexadecimal Conversion Table

Table 55: Decimal-to-Hexadecimal Conversion Table

Decimal	01	02	03	04	05	06	07	08	09	10
Hex	01	02	03	04	05	06	07	08	09	0a
Decimal	11	12	13	14	15	16	17	18	19	20
Hex	0b	0c	0d	0e	0f	10	11	12	13	14
Decimal	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**
Hex	15	16	17	18	19	1a	1b	1c	1d	1e
Decimal	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**
Hex	1f	20	21	22	23	24	25	26	27	28
Decimal	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**50**
Hex	29	2a	2b	2c	2d	2e	2f	30	31	32
Decimal	**51**	**52**	**53**	**54**	**55**	**56**	**57**	**58**	**59**	**60**
Hex	33	34	35	36	37	38	39	3a	3b	3c
Decimal	**61**	**62**	**63**	**64**	**65**	**66**	**67**	**68**	**69**	**70**
Hex	3d	3e	3f	40	41	42	43	44	45	46
Decimal	**71**	**72**	**73**	**74**	**75**	**76**	**77**	**78**	**79**	**80**
Hex	47	48	49	4a	4b	4c	4d	4e	4f	50
Decimal	**81**	**82**	**83**	**84**	**85**	**86**	**87**	**88**	**89**	**90**
Hex	51	52	53	54	55	56	57	58	59	5a
Decimal	**91**	**92**	**93**	**94**	**95**	**96**	**97**	**98**	**99**	**100**
Hex	5b	5c	5d	5e	5f	60	61	62	63	64
Decimal	**101**	**102**	**103**	**104**	**105**	**106**	**107**	**108**	**109**	**110**
Hex	65	66	67	68	69	6a	6b	6c	6d	6e
Decimal	**111**	**112**	**113**	**114**	**115**	**116**	**117**	**118**	**119**	**120**
Hex	6f	70	71	72	73	74	75	76	77	78
Decimal	**121**	**122**	**123**	**124**	**125**	**126**	**127**	**128**	**129**	**130**
Hex	79	7a	7b	7c	7d	7e	7f	80	81	82
Decimal	**131**	**132**	**133**	**134**	**135**	**136**	**137**	**138**	**139**	**140**
Hex	83	84	85	86	87	88	89	8a	8b	8c
Decimal	**141**	**142**	**143**	**144**	**145**	**146**	**147**	**148**	**149**	**150**
Hex	8d	8e	8f	90	91	92	93	94	95	96
Decimal	**151**	**152**	**153**	**154**	**155**	**156**	**157**	**158**	**159**	**160**
Hex	97	98	99	9a	9b	9c	9d	9e	9f	a0
Decimal	**161**	**162**	**163**	**164**	**165**	**166**	**167**	**168**	**169**	**170**
Hex	a1	a2	a3	a4	a5	a6	a7	a8	a9	aa
Decimal	**171**	**172**	**173**	**174**	**175**	**176**	**177**	**178**	**179**	**180**
Hex	ab	ac	ad	ae	af	b0	b1	b2	b3	b4
Decimal	**181**	**182**	**183**	**184**	**185**	**186**	**187**	**188**	**189**	**190**

Hex	b5	b6	b7	b8	b9	ba	bb	bc	bd	be
Decimal	**191**	**192**	**193**	**194**	**195**	**196**	**197**	**198**	**199**	**200**
Hex	bf	c0	c1	c2	c3	c4	c5	c6	c7	c8
Decimal	**201**	**202**	**203**	**204**	**205**	**206**	**207**	**208**	**209**	**210**
Hex	c9	ca	cb	cc	cd	ce	cf	d0	d1	d2
Decimal	**211**	**212**	**213**	**214**	**215**	**216**	**217**	**218**	**219**	**220**
Hex	d3	d4	d5	d6	d7	d8	d9	da	db	dc
Decimal	**221**	**222**	**223**	**224**	**225**	**226**	**227**	**228**	**229**	**230**
Hex	dd	de	df	e0	e1	e2	e3	e4	e5	e6
Decimal	**231**	**232**	**233**	**234**	**235**	**236**	**237**	**238**	**239**	**240**
Hex	e7	e8	e9	ea	eb	ec	ed	ef	ee	f0
Decimal	**241**	**242**	**243**	**244**	**245**	**246**	**247**	**248**	**249**	**250**
Hex	f1	f2	f3	f4	f5	f6	f7	f8	f9	fa
Decimal	**251**	**252**	**253**	**254**	**255**					
Hex	fb	fc	fd	fe	ff					

Revision History

FOS-92x-Troubleshooting-RM100; April 28, 2023

Initial document version.

Documentation Legal Notice


BROADCOM®