Brocade Fabric OS v2.6.2d Release Notes_v1.0

May 23, 2005

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v2.6.2d Release Notes_v1.0	First release.	May 23, 2005

TABLE OF CONTENTS

Overview

Fabric OS v2.6.2 is planned to be the last maintenance release for the SilkWorm 2xxx product family. All future releases of v2.6.2 will be patches that will address only critical or high-severity customer issues.

Fabric OS v2.6.2d is a patch release that contains fixes to a small number of defects found since the release of Fabric OS v2.6.2. Aside from these changes, this patch is functionally identical to the Fabric OS v2.6.2 release. Fabric OS v2.6.2 provides the following enhancements and new features to Fabric OS v2.6.1x:

- Reduces fabric configuration downtime.

  Extended-edge PID for mixed fabrics eliminates host reboot for hosts that statically bind PIDS.

- Improves fabric diagnostics.

  pathInfo command displays information about the path between any two ports in a fabric.

- Improves manageability and ease of use.

  Advanced Web Tools is improved.

About This Release

This patch release includes:

- Fixes to defects as detailed in the section "Defects Closed in Fabric OS v2.6.2d"

Supported Switches

Brocade Fabric OS v2.6.2 supports Brocade SilkWorm 2000-series switches.

Technical Support

Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To assist your support representative and to expedite your call, have the following three sets of information immediately available when you call:

1. General Information

- Technical Support contract number, if applicable
- Switch model
- Switch operating system version
- Error messages received
- **supportShow** command output
- Detailed description of the problem and specific questions
- Description of any troubleshooting steps already performed and results

2. Switch Serial Number
The switch serial number and corresponding bar code are provided on the serial number label, as shown here.

The serial number label is located as follows:

- *SilkWorm 2000-series switches:* Bottom of chassis

3. World Wide Name (WWN)

- Use the **wwn** command to display the switch WWN.

Standards Compliance

Brocade Fabric OS v2.6.2d conforms to the following Fibre Channel Standards, in a manner consistent with accepted engineering practices and procedures. In certain cases, Brocade might add proprietary supplemental functions to those specified in the standards. Brocade verifies conformance with Fibre Channels Standards by subjecting its switches to SANmark Conformance Tests developed by the Fibre Channel Industry Association. Brocade switches have earned the SANmark logo, indicating such conformance. SANmark is a limited testing program and does not test all standards or all aspects of standards. For a list of standards conformance, visit the following Brocade web site:

http://www.brocade.com/sanstandards

Important Notes

This section lists important information that you should be aware of when running Fabric OS v2.6.2.

OS Requirements

The following table summarizes the versions of Brocade software that are supported in conjunction with this release. These are the minimum software versions that interoperate. Brocade recommends using the latest software release versions to get the most benefit out of the SAN.

Fabric OS v2.4.x or earlier, v3.0.0x or earlier, and v4.0.0 or earlier have reached their end-of-life and are no longer supported as of February 2004.

	SilkWorm 2xxx	**SilkWorm 3200 & 3800**	**SilkWorm 3250, 3850, 3900, 12000, & 24000** [1]	**Fabric Manager**
General compatibility	2.6.0c or later	3.0.2c or later	4.0.2 or later	3.0.2c or later
With Secure Fabric OS enabled	2.6.1 or later	3.1.0 or later	4.1.0 or later	3.0.2c or later
Recommended software versions	2.6.2d or later	3.2.0a or later	4.4.0d or later	4.4.0 or later

[1] SilkWorm 3900 is supported by Fabric OS v4.0.2 or later.
SilkWorm 3250, 3850, and 24000 are supported by Fabric OS v4.2.0 or later.

SilkWorm 2000-Series Scalability Support

Exhaustive testing has demonstrated that SilkWorm 2000-series switches should not be deployed in fabrics that exceed 728 SAN devices.

Mixed-Fabric Environment with Different SilkWorm Platforms

Fabric OS v2.6.2/v3.1.2/v4.2.0 introduced a new switch PID format: extended-edge PID (Format 2). Extended-edge PID might be useful if you introduce a Fabric OS v4.2.0 switch to a fabric consisting solely of Fabric OS v2.x/v3.x switches. Before adding a Fabric OS v4.2.0 switch to such a fabric, refer to *Brocade Fabric OS Procedures Guide,* publication number 53-0000518-03, for information on the extended-edge PID format. Note that in order to use the extended-edge PID format, Fabric OS v2.6.2, v3.1.2, and v4.2.0 must be deployed together, as applicable, to the switches.

If extended-edge PID format is set before downgrading from the current Fabric OS release to an older Fabric OS version that does not support extended-edge PID format, PID must be returned to supported formats, such as core PID (Format 1) or native PID (Format 0).

Advanced Web Tools Updates

- Fabric View is not supported beginning with Fabric OS v2.6.2.

  In Fabric OS v2.6.2, a new HTML-based home page replaces Fabric View. Switches are sorted by Fabric OS version, and the current launch switch and FCS switch are indicated (for Secure Fabric OS). Fabric Events are not available in Fabric OS v2.6.2.

- **Issue:** Entering invalid IP addresses causes certain areas of Advanced Web Tools to become inaccessible.

  Workaround: If configuring IP addresses over Ethernet connections, you should leave the FCIP address value blank.

  If configuring IP addresses over Fibre Channel connections, only the switch that functions as the IP/FC router needs to have both a valid IP and FCIP address. The rest of the switches need only have a valid FCIP address. Using invalid addresses or address combinations might make certain functions of Advanced Web Tools inaccessible. All FCIP addresses used should belong to the same subnet.

- This release of Advanced Web Tools recognizes existing Brocade switches properly, rather than as generic 16-port switches.

- Advanced Web Tools browser, operating system, and Java Plug-in support is updated for Fabric OS v2.6.2.

The following table identifies the supported browsers, operating systems, and Java Plug-ins for this release.

Operating System	Browser	Java Plug-in
Red Hat Linux 9.0	Mozilla 1.4	1.4.2
Solaris 2.8	Mozilla 1.4	1.4.2
Solaris 2.9	Mozilla 1.4	1.4.2
Windows 2000	Internet Explorer 6.0	1.3.1_04 1.4.1_02 (recommended)
Windows 2003	Internet Explorer 6.0	1.3.1_04 1.4.1_02 (recommended)
Windows XP	Internet Explorer 6.0	1.3.1_04 1.4.1_02 (recommended)

- When using a fabric containing v4.x, v3.x, and v2.x switches, Brocade recommends that you use the most advanced switches to control the fabric. For example, use the v4.x switches as the primary FCS, the location to perform zoning tasks, and the time server (CLI). Brocade also recommends that you use the most recently released firmware to control the fabric.

- Fabric OS v2.6.2 does not support loading of the Switch Admin page using Mozilla.

- For instructions on installing Mozilla 1.4 on Solaris 8 and Solaris 9, refer to the following Web site:

http://ftp.mozilla.org/pub/mozilla.org/mozilla/releases/mozilla1.4/mozilla-sparc-sun-solaris2.8_1.4.readme

- **Issue:** The Mozilla browser does not support the Switch Admin module properly in Fabric OS v2.6.x; a warning message is displayed. For other 2.6.x versions, no warning message is displayed.

  Workaround: Use Netscape 4.7.7 or later.

- The additionally supported browsers, operating systems, and Java Plug-ins introduce the following limitations when using mixed OS versions in Advanced Web Tools v2.6.2.

Launch Switch Environment	Problems
Firmware: Fabric OS v2.6.x **Operating System:** Solaris **Browser:** Mozilla	**Issue**: The Switch Admin does not launch correctly. If you try to launch the Switch Admin using Fabric OS v2.6.2 on a Solaris operating system with a Mozilla browser, a warning dialog displays, telling you to use the Netscape browser. If you try to launch the Switch Admin using Fabric OS v2.6.1 or earlier on a Solaris operating system with a Mozilla browser, the Switch Admin fails and no warning is displayed. **Workaround:** Although the Netscape browser is not supported by Web Tools for switches running Fabric OS v2.6.2, 3.1.2, or 4.2.0 or later, if you must access the Switch Admin on a switch running Fabric OS v2.6.x from a Solaris operating system, use the Netscape 4.77 browser.
Firmware: version *prior* to Fabric OS v2.6.2, v3.1.2, or v4.2.0 with secure mode enabled **Operating System:** Solaris **Browser:** Mozilla	**Issue**: If you try to launch the Switch Admin, Zoning, Fabric Watch, or High Availability Admin using firmware versions prior to v2.6.2, v3.1.2, or v4.2.0 on a Solaris operating system with a Mozilla browser, the browser might crash due to a buffer overflow problem with Mozilla. **Workaround**: Although the Netscape browser is not supported by Web Tools for switches running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later, if you must access the Switch Admin, Zoning, Fabric Watch, or High Availability Admin on a switch running firmware versions prior to v2.6.2, v3.1.2, or v4.2.0 from a Solaris operating system, use the Netscape 4.77 browser.
Firmware: version *prior* to Fabric OS v2.6.2, v3.1.2, or v4.2.0 **Operating System:** Any supported operating system (with supported browser) **Browser:** Any supported browser (on supported operating system)	**Issue**: When trying to access a switch running firmware versions prior to Fabric OS v2.6.2, v3.1.2, or v4.2.0 from the launch switch, Switch Explorer will display a null pointer exception, and the SwitchInfo applet will not display; Switch Explorer does not work properly with switches running the latest firmware. **Workaround**: Use a launch switch running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later to access the switch.

Launch Switch Environment	Problems
	Issue: When trying to perform end-to-end monitoring (Brocade Advanced Performance Monitoring) on a SilkWorm 24000 or SilkWorm 3250, the SilkWorm 24000 or SilkWorm 3250 is displayed as a 16-port switch. **Workaround:** For a SilkWorm 3250, ignore the extra ports. For a SilkWorm 24000, use a launch switch running Fabric OS v4.2.0 or later to perform end-to-end monitoring on the switch.
	Issue: When trying to perform zoning on a SilkWorm 24000 or SilkWorm 3250, the SilkWorm 24000 or SilkWorm 3250 is displayed as a 16-port switch. **Workaround:** If you are running Brocade Secure Fabric OS, select a switch running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later as the primary FCS switch. If you are not running Secure Fabric OS, use a launch switch running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later to perform zoning on the switch.
Firmware: Fabric OS v2.6.2, v3.1.2, or v4.2.0 **Operating System:** Any supported operating system (with supported browser) **Browser:** Any supported browser (on supported operating system)	**Issue:** The Name Server table does not display properly for a switch running firmware versions prior to Fabric OS v2.6.2, v3.1.2, or v4.2.0. **Workaround:** If secure mode is enabled, select a switch running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later as the primary FCS switch. If secure mode is not enabled, use a launch switch running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later to access the Name Server table on the switch.
Firmware: version *prior* to Fabric OS v2.6.2, v3.1.2, or v4.2.0 **Operating System:** Solaris **Browser:** Netscape	**Issue**: Any switches running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later are unsupported through Netscape. **Workaround**: The Netscape browser is not supported by Web Tools for switches running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later. Use the Mozilla browser to manage all of your switches from a Solaris operating system.
Firmware: version *prior* to Fabric OS v2.6.1, v3.0.x, or v4.0.x **Operating System:** Windows **Browser:** Internet Explorer	**Issue**: When you are trying to run Fabric View, the browser might crash. **Workaround**: Use a launch switch that runs Fabric OS versions v2.6.1, v3.0.x, or v4.0.x or later, so that you can use Switch Explorer (not Fabric View). For a fabric in which all switches are running firmware versions prior to v2.6.2 (in which Switch Explorer is not available), use a switch running Fabric OS v2.6.2 as the launch switch.

Other Notes

This table lists other important information you should be aware of regarding Fabric OS v2.6.2. These notes are applicable to Fabric OS v2.6.1 as well and have been disclosed in previous release notes.

Area	Description

Area	Description
Code download	Starting with Fabric OS v2.6.1c, a different compression algorithm is used to create a smaller image of the Fabric OS v2.6.x final code for downloading into flash memory. This compression algorithm does not change the functionality of the code after boot up in any way. There is a small incremental boot up time of approximately 10 seconds.
Compatability	Sometimes in a mixed fabric of v4.x/3.x/2.x operating systems, fabric reconfiguration is caused by link reset on v3.x/v2.x. This only happens in a fabric containing any Fabric OS v3.x versions released prior to v3.1.0 or Fabric OS v2.x versions releases prior to v2.6.1 under heavy traffic or CPU- intensive operations such as large (50K) zone database propagation. Use the latest revision code across all releases in a mixed fabric.
Fabric configuration	During fabric configuration, the countdown message that used to appear on the console no longer appears, starting with Fabric OS v2.6.2, v3.1.2, and v4.2.0. The fabric reconfiguration message is instead captured in the error log. For details, refer to the "New Error Messages" section of this document.
Fabric Watch, e-mail alert error message	When enabling e-mail alerts in Fabric Watch and an event occurs, the message "ErrLog: Error Level=3 [(null)]" is captured to the system error log. This message is from SMTP and can be ignored.
FARP requests	Fabric OS v2.x and v3.x do not support FARP requests, only ARP requests. When using IP over Fibre Channel, confirm that all host HBAs support ARP requests and issue ARP requests.
License removal	When a user removes a license from the switch, the licensed feature is not disabled until the switch is rebooted or a switch disable and enable is performed.
Mixed-fabric, zone database size limitations	In a mixed-version fabric, make sure that any zone database sent to that fabric is no larger than the maximum supported by the most restrictive version; otherwise, the fabric will segment.
Security, PKICERT utility	Before using the PKICERT utility to prepare a Certificate Signing Request (CSR), ensure that there are no spaces in the switch names of any switches in the fabric. The Web site that processes the CSRs and generates the digital certificates does not accept switch names containing spaces, and any CSRs that do not conform to this requirement are rejected.
Security	The **licenseAdd** command fails with certain proxy-target combinations if the license key already exists in the target switch.
Zoning	To use zoning in a non-RCS (Reliable Commit Service) mode fabric (that is, in a fabric containing switches with firmware versions other than v2.6.x, v3.1 or later, and v4.1 or later), install all appropriate zoning licenses on all the switches in the fabric before attempting to bring a switch into the fabric. Furthermore, if the zoning license is to be removed, the user must make sure it is reinstalled properly on the affected switch before attempting the **cfgEnable** zoning operation. Failure to follow these steps can cause inconsistency of zoning configuration on the affected switches should a zoning operation be attempted from a remote switch in the fabric. On the affected switches, an error message appears on the console or telnet session (this can also be seen by using **errShow**, **errDump**), indicating that the zoning license was missing.
Large fabric support	WAN_TOV and MAX_HOPS as configurable parameters for large fabric functionality is supported.

Documentation Updates

This section provides information on last-minute additions and corrections to the documentation.

Brocade Secure Fabric OS User's Guide, v2.6

(Publication number 53-0000195-02)

The *Brocade Secure Fabric OS User's Guide* was updated for releases v2.6.2, v3.1.2, and v4.2.0. The updated book is *Brocade Secure Fabric OS User's Guide,* publication number 53-0000526-03.

Brocade Zoning User's Guide, v2.6

(Publication number 53-0000202-02)

On page 3-4, after the existing Note, add the following new Note:

> "**Note**
>
> The maximum number of items that can be stored in the zoning configuration database depends on the switches in the fabric, whether or not interop mode is enabled, and the number of bytes required for each item. The number of bytes required for an item depends on the specifics of the fabric but cannot exceed 64 bytes per item. At 64 bytes per item, you can have:
>
> - 767 entries for a fabric with at least one v2.x or v3.x switch and interop mode disabled.
> - 383 entries for a fabric with at least one v2.x or v3.x switch and interop mode enabled.
> - 997 entries for a fabric consisting solely of v4.x switches and interop mode disabled.
> - 498 entries for a fabric consisting solely of v4.x switches and interop mode enabled.
>
> You can use the **cfgSize** command to check both the maximum available size and the currently saved size. If you believe you are approaching the maximum, you can save a partially completed zoning configuration and use the **cfgSize** command to determine the remaining space."

Brocade Secure Fabric OS QuickStart Guide, v2.6.1/3.1.0/4.1.0

(Publication number 53-0000352-02)

The *Brocade Secure Fabric OS QuickStart Guide* was updated for releases v2.6.2, v3.1.2, and v4.2.0. The updated book is *Brocade Secure Fabric OS QuickStart Guide,* publication number 53-0000352-03.

Brocade Secure Fabric OS User's Guide, v2.6.2/3.1.2/4.2.0

(Publication number 53-0000526-03)

On page 2-3, following this paragraph:

> "All switches that are shipped with Fabric OS v3.1.2 or v4.2.0 installed already have the required PKI objects and a digital certificate. If a switch no longer has the required PKI objects, refer to section 'Recreating PKI Objects if Required' on page 2-19 for information on recreating the PKI objects. If a switch no longer has the required digital certificate, refer to section 'Obtaining the Digital Certificate File' on page 2-14 for information on obtaining digital certificates."

Add the following paragraph:

> "Switch digital certificates are checked when a switch joins a fabric, either because the switch is added to the fabric or because the switch is booting. Changes to the certificate--for example, if the certificate is removed or corrupted--might not be noticed until the switch is rebooted."

On page 3-2, following the second paragraph of "Enabling Secure Mode":

"Secure Mode is enabled using the **secmodeenable** command. This command must be entered through a **sectelnet**, Secure Shell, or serial connection to the switch designated as the primary FCS switch. The command fails if any switch in the fabric is not capable of enforcing Secure Fabric OS policies. If the primary FCS switch fails to participate in the fabric, the role of the primary FCS switch moves to the next available switch listed in the FCS policy."

Add the following note:

"**Note:** To activate security, all switches in the fabric are automatically rebooted. All I/O should be stopped prior to running the **secmodeenable** command."

Brocade Fabric OS v2.6.1 and v2.6.1a Release Notes

In Fabric OS v2.6.1 and v2.6.1,a Release Notes section, "SilkWorm 2xxx Scalability Limit," specifies that fabrics containing Fabric OS v2.6.1 or later should not exceed 500 user (non-ISL) ports or devices. Brocade has increased to 728 the maximum number of devices supported in fabrics that include SilkWorm 2000-series switches running Fabric OS v2.6.1 or later. This is only a change to the documentation; there is no change to the Fabric OS.

A new command, **cfgSize**, was supported beginning in Fabric OS v2.6.1 but was not documented in the subsequent Release Notes. For details on this command, refer to the "New Commands Introduced in 2.6.1" section of this document.

Brocade Web Tools User's Guide, v2.6.0

(Publication number 53-0000197-02)

Fabric View is not supported for Fabric OS v2.6.x, beginning with Fabric OS v2.6.2.

All references to "Fabric View" should be removed.

The Fabric View section on page 3-1 through page 3-4 should be removed and replaced with the following text:

"Every switch in the fabric, including any unlicensed switches, is represented in the display when you first access the Web Tools interface; however, only switches with a Web Tools license can be managed from the Web Tools interface.

To launch Web Tools:

1. Launch the Web browser.
2. Type the switch name or IP address in the **Location/Address** field and press **Enter**:

```
http://switch name
```

Note: This switch is assumed to be the local domain. For information that is specific to a QuickLoop to be made available, the QuickLoop switch must be the host domain.

Web Tools launches."

The "Fabric Events View" section on page 3-4 to 3-5 should be removed.

The following text should be removed from page 1-3, "Views Available in Web Tools":

"Initial Display Upon Launching Web Tools:

Fabric View
Displays a control panel that provides access to fabric-wide options, a panel for each switch in the fabric, plus a legend that explains the meaning of the background colors on the **Switch** icons. Each panel contains an icon that represents the switch itself, in addition to icons for Switch Events and the Administrative and Telnet interfaces. The background color of the switch icon represents the status of that particular switch or Integrated Fabric (as defined by the legend provided in the window).

Note: Switch status is calculated approximately once per second; however the initial calculation does not occur until 30-60 seconds after the switch is booted. It is calculated from the state of data structures in the switch, and stored as the variable "switchStatus". For all statuses that are based on errors per time interval, any errors will cause the status to show faulty until the entire sample interval has passed.

Fabric Events View
Displays the error log for the fabric, which is the combination of the error logs of all the switches in the fabric. Accessed by clicking on the **Fabric Events** icon on the control panel."

Brocade Fabric OS Reference Manual, v2.6.0

(Publication number 53-0000194-02)

The following commands have been added or modified from what is stated in the *Brocade Fabric OS Reference Manual, v2.6.0*::

- **pathInfo**
- **cfgSize**
- **shellFlowControlDisable**
- **shellFlowControlEnable**

Refer to "New Commands Introduced in v2.6.2" and "New Commands Introduced in v2.6.1" for more information.

The following commands have been modified in the documentation:

- **configure**
- **quietMode**

Refer to "Commands Modified in v2.6.2" for more information.

SilkWorm 2800 Hardware Reference Manual

(Publication number 53-0001485-03)

Figure 1-1 on page 1-1 of the *SilkWorm 2800 Hardware Reference Manual* has mislabeled callouts. The power supplies 1 and 2 are reversed and should be labeled as follows:

New Commands Introduced in v2.6.2

pathInfo

Displays routing and statistics information along a path.

SYNOPSIS **pathInfo** [[[*domain*], *source port*], *destination port*] [,"**-r**"]

AVAILABILITY root, admin

DESCRIPTION

The command **pathInfo** displays detailed routing information from a source port (or area) on the local switch to a destination port (or area) on another switch. This routing information describes the exact path that a user datastream takes to go from the source to the destination. If the user specifies inactive ports or a path through a switch that does not have active routing tables to the destination, **pathInfo** describes the path that would be used if the ports were active. If the user specifies a destination port that is not active, **pathInfo** uses the embedded port as the destination.

For switches with blades, the ingress and egress points are specified as area numbers. For a non-bladed switch, ingress and egress points are specified as ports. This agrees with the representation shown in the **switchShow** command.

In addition, **pathInfo** can provide, upon request, statistics on every traversed ISL.

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

Other options allow the collection of information on the reverse path or on a user-selected path (source route).

For each hop, the routing information output includes the following:

Hop	The hop number, the local switch being hop 0.
In Port	The port (or area) from which the frames come; for hop 0, the source port. For a switch with blades, this is specified as the area number; otherwise, it is specified as the port number.
Domain ID	The domain ID of the switch.
Name	The name of the switch.
Out Port	The output port that the frames take to reach the next hop; for the last hop, the destination port or area. For a switch with blades, this is specified as the area number; otherwise, it is specified as the port number.
BW	The bandwidth of the output ISL, in Gbits/sec. BW does not apply to the embedded port.
Cost	The cost of the link used by FSPF routing protocol. Cost applies only to an E_Port.

For each hop, statistics are broken down into *basic* and *extended*. They are reported below the routing information, separated into *input port statistics* and *output port statistics*. For each port, they are further separated into *transmit* and *receive* statistics. Statistics are not reported for the embedded port.

Some values are measured over multiple time intervals. For example, the output line utilization in bytes per second is calculated over both a 1-second period and over a 64-second period. This gives an idea of both the current line utilization and the utilization over a longer period of time. The time interval is reported in parenthesis after the value's description.

Maximum Hop Count

pathInfo uses a special frame that is sent hop-by-hop from the source switch to the destination switch, collecting routing and statistics information at every hop. To prevent such a frame from looping forever if an error occurs, a maximum number of hops is enforced.

The hop count includes all hops in the direct path from source to destination, as well as all the hops in the reverse path, if tracing of the reverse path is requested. The default value for the maximum hop count is 25.

Basic Statistics

Basic statistics report variables that give an indication of ISL congestion along the path. They include the following:

B/s	Bytes per second.
Txcrdz	The length of time, in milliseconds, that the port has been prevented from transmitting frames due to lack of buffer-to-buffer credit. This is an indication of downstream congestion. Note that other commands—for example, **portStatsShow**—might express this value in units other than milliseconds.

Extended Statistics

Extended statistics report variables of general interest. They include the following:

F/s	Frames per second.
Words	Total number of 4-byte Fibre Channel words.
Frames	Total number of frames.
Errors	Total number of errors that might cause a frame to be received incorrectly. This includes CRC errors, bad-EOF errors, frame-truncated errors, frame-too-short errors, and encoding errors inside a frame.

Reverse Path

In general, the path from port A on switch X to port B on switch Y might be different from the path from port B to port A. The difference could be in the links traversed between the same sequence of switches, or the reverse path might even involve different switches. The trace reverse path option allows the user to determine both routing and statistics information for the reverse path, in addition to those for the direct path.

Source Route

The source route option allows the user to specify a sequence of switches or ports (or areas) that the **pathInfo** frame has to follow to reach the destination. Therefore, the path might be different from the one the actual traffic from source to destination takes.

The source route is expressed as a sequence of switches, a sequence of output ports (or areas), or a combination thereof. The next hop in the source route is described by either the output port (or area) to be used to reach the next hop or the domain ID of the next hop.

The source route can specify a partial route from source to destination as a full route, or as an arbitrary route across the fabric. If a partial route is specified, the remaining hops to the destination is the path from the input port (or area) on the first hop not listed in the source route. The maximum hop count is enforced.

If the source route does not specify all the switches along a section of the path, a further option allows specification of a *strict path* versus a *loose path*. A strict source route requires that only the specified switches be reported in the path description. If two switches are specified back-to-back in the source route descriptor but are not directly connected, the switches in between are ignored. In the case of a loose source route, the switches in between are reported. The concepts of strict and loose route apply to the portion(s) of the path described by domains, not to the part described by output ports/areas.

Operands

The following operands are allowed:

domain	The ID of the destination domain.
source port	The port (or area) whose path to the destination domain is sought. The embedded port (-1) is used by default. For a switch with blades, the destination is specified as the area; otherwise, it is specified as the port. If the source port is given as -1 with no additional arguments, then basic statistics are displayed for the route.
destination port	A port on the destination switch. **pathInfo** returns the state of the port (or area). The embedded port (-1) is used by default or if the user specifies a destination port that is not active. For a switch with blades, the destination is specified as the area; otherwise, it is specified as the port.
-r	Show reverse path in addition to forward path in display output.

Without operands, **pathInfo** displays a menu in which the following parameters can be provided:

max hops	The maximum number of hops that the **pathInfo** frame is allowed to traverse. Default: 25.
domain	The ID of the destination domain. Mandatory, no default.
source port	The port whose path to the destination domain is sought. It can be an F_Port or an E_Port. The embedded port (-1) is used by default. For a switch with blades, this is specified as the area, otherwise, it is specified as the port.
destination port	A port on the destination switch. **pathInfo** returns the state of the port and all requested statistics pertaining to the port. The embedded port (-1) is used by default or if the specified destination port is not an existing active port. For a switch with blades, this is specified as the area; otherwise, it is specified as the port.
basic stats	Requests the reporting of basic statistics on every link. Default: no.
extended stats	Requests the reporting of extended statistics on every link. Default: no.
trace reverse path	Provides path information from the destination port to the source port. Default: no.
source route	Specifies a sequence of switches or ports that the **pathInfo** frame should traverse. Note that if an output port (or area) to the next hop is specified, the user is not prompted for the domain of the next switch; that is determined by the port (or area) specified. Default: no.
strict source rte	Specifies that the source route must be followed strictly as indicated, skipping possible intermediate switches. When using this option, the source route must be specified using domain numbers (rather than the output port).
timeout	The maximum time allowed to wait for the response. Default: 10 seconds.

EXAMPLES

The following example shows the **pathInfo** command invoked with all operands on the command line:

```
web226:root> pathInfo 91


     Target port is Embedded

     Hop  In Port  Domain ID (Name)      Out Port    BW   Cost
     ------------------------------------------------------
      0       E         9 (web226)           2       1G   1000
      1       3        10 (web229)           8       1G   1000
      2       8         8 (web228)           9       1G   1000
      3       6        91 (web225)           E       -      -
```

This next example shows the **pathInfo** command invoked through the menu, including basic and extended statistics:

```
web226:root> pathInfo

         Max hops: (1..127) [25]
         Domain: (1..239) [-1] 8
         Source port: (0..15) [-1]
         Destination port: (0..255) [-1]
         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: (1..30) [5]
     Target port is Embedded

     Hop  In Port  Domain ID (Name)      Out Port    BW   Cost
     ------------------------------------------------------
      0       E         9 (web226)           2       1G   1000

     Port                              E                              2
                              Tx              Rx              Tx              Rx
                              ------------------------------------------------
     B/s (1s)                  -               -               0               0
     B/s (64s)                 -               -               1               1
     Txcrdz (1s)               -               -               0               -
     Txcrdz (64s)              -               -               0               -
     F/s (1s)                  -               -               0               0
     F/s (64s)                 -               -            2743               0
     Words                     -               -         2752748         2822763
     Frames                    -               -          219849           50881
     Errors                    -               -               -               0


     Hop  In Port  Domain ID (Name)      Out Port    BW   Cost
     ------------------------------------------------------
      1       3        10 (web229)          12       1G   1000

     Port                              3                             12
                              Tx              Rx              Tx              Rx
                              ------------------------------------------------
     B/s (1s)                 36              76               0               0
     B/s (64s)                 5               5               5               5
     Txcrdz (1s)               0               -               0               -
     Txcrdz (64s)              0               -               0               -
     F/s (1s)                  1               1               0               0
     F/s (64s)                 0               0               0               0
     Words             240434036         2294316         2119951         2121767
     Frames             20025929           54999          162338           56710
     Errors                    -               4               -               0


     Hop  In Port  Domain ID (Name)      Out Port    BW   Cost
     ------------------------------------------------------
      2      14         8 (web228)           E       -      -
```

```
Port                          14                              E
                        Tx            Rx            Tx            Rx
                        ----------------------------------------------
B/s (1s)                 0             0             -             -
B/s (64s)                5             5             -             -
Txcrdz (1s)              0             -             -             -
Txcrdz (64s)             0             -             -             -
F/s (1s)                 0             0             -             -
F/s (64s)                0             0             -             -
Words             20158695       1021842             -             -
Frames             1665662         56849             -             -
Errors                   -             4             -             -
```

New Commands Introduced Since v2.6.1

cfgSize

Displays size details of the zone database.

SYNOPSIS **cfgSize** [integer]

AVAILABILITY all users

DESCRIPTION

This command with no parameter (or parameter 0) displays the size of the zone database, including maximum size, committed size, and transaction size, all in bytes.

"Zone DB max size" is the upper limit for the defined configuration, determined by the amount of flash memory available for storing the defined configuration. This is smaller than the flash size because of additional information about the database that needs to be stored.

"Committed size" is the size of the defined configuration currently stored in flash.

"Transaction size" is the size of the uncommitted defined configuration. This value is nonzero if the defined configuration is being modified by telnet, API, and so on; otherwise, it is 0.

If a nonzero integer is specified as the parameter, the size of the flash memory allocated for the zone database is displayed. The zone database includes both the defined and effective configurations. This size is in kilobytes.

See **cfgShow** for a description of defined and effective configurations.

Note: When security is enabled, this command must be issued on all of the switches in the fabric, not just on one or some of the switches.

OPERANDS The following operand is optional:

integer

EXAMPLE

To display size details of the defined configuration:

```
Sw5:user> cfgsize

Zone DB max size - 98232 bytes
      committed - 2439
      transaction - 0
```

To display size details of the defined configuration:

```
Sw5:user> cfgsize 1
Zone DB flash size - 98304 bytes
```

SEE ALSO

cfgShow

shellFlowControlDisable

Disables XON/XOFF flow control to the shell task.

SYNOPSIS **shellFlowControlDisable**

AVAILABILITY admin

DESCRIPTION

This command allows an administrator to disable XON/XOFF flow control to the shell task, which is the recommended behavior for the switch. Flow control is disabled for both serial port and telnet access into the command shell.

Once disabled, even in the event of a power boundary, the switch boots up with XON/XOFF flow control disabled.

LIMITATIONS none

OPERANDS none

EXAMPLE

```
admin> shellFlowControlDisable
Committing configuration...done.
```

SEE ALSO

shellFlowControlEnable

shellFlowControlEnable

Enables XON/XOFF flow control to the shell task.

SYNOPSIS **shellFlowControlEnable**

AVAILABILITY admin

DESCRIPTION

This command allows an administrator to enable XON/XOFF flow control to the shell task. Disabling XON/XOFF flow control is the recommended behavior for the switch; however, if it becomes necessary to enable XON/XOFF flow control, you can do it with this command. Flow control is enabled for both serial port and telnet access into the command shell.

Once enabled, even in the event of a power boundary, the switch boots up with XON/XOFF flow control enabled.

LIMITATIONS none

OPERANDS none

EXAMPLE

```
admin> shellFlowControlEnable
Committing configuration...done.
```

SEE ALSO

shellFlowControlDisable

Commands Modified in v2.6.2

quietMode

Sets/clears shell quiet mode.

SYNOPSIS **quietMode** [*newMode*]

AVAILABILITY all users (display)
admin (set/clear)

DESCRIPTION

This command affects the output displayed on the switch's console (serial port or telnet session).

By default, quiet mode is turned off, and all switch tasks can send output to the console. Some output is caused by asynchronous events, such as the fabric reconfiguring, or by devices logging in.

When quiet mode is turned on, only output produced by shell commands is shown; all asynchronous output produced by other tasks is suppressed. This is useful when driving a telnet session using a script that might not expect any asynchronous output.

OPERAND

The following operand is optional:

newMode 0 to clear quiet mode (all tasks can print to the console)

1 to set quiet mode (only shell commands can print)

EXAMPLE

The following example first displays the current mode and then on turns quite mode:

```
sw5:admin> quietMode
Quiet Mode is OFF
sw5:admin> quietMode 1
Committing configuration...done.
Quiet Mode is now ON
```

Commands Modified in v2.6.2a

configure

Changes system configuration settings.

SYNOPSIS **configure**

AVAILABILITY admin

DESCRIPTION

This command changes some system configuration settings, including:

- Switch fabric settings
- Virtual channel settings
- Switch operating mode
- Zoning operation parameters
- RSCN transmission mode
- NS operation parameters
- Arbitrated loop settings
- System services settings

- Portlog events disable/enable settings

This command cannot execute on an enabled system; you must first disable the system, using the **switchDisable** command.

Navigate the **configure** command output by responding to a series of hierarchical menus. Each top-level menu and its associated submenus consists of a text prompt, a list of acceptable values (if appropriate), and a default value (shown in brackets). Press **Enter** to use the default value (refer to "Special Inputs," later in this command description).

Switch Fabric Settings

There are several settings that control the overall behavior and operation of the fabric. Some of these values, such as the domain, are normally assigned automatically by the fabric and can be different from one switch to another. However, other parameters, such as the buffer-to-buffer credit or the timeout values, can be changed to suit particular applications or operating environments, as long as there is agreement among all switches, to allow formation of the fabric.

The following table defines changeable settings affecting the fabric.

Field	Type	Default	Range
Domain	Number	1	Varies
BB Credit	Number	16	1 to 27
R_A_TOV	Number	10000	E_D_TOV * 2 to 120000
E_D_TOV	Number	2000	1000 to R_A_TOV / 2
WAN_TOV	Number	0	0 to R_A_TOV / 4
MAX_HOPS	Number	7	7 to 19
Data Field Size	Number	2112	256 to 2112
Sequence Level Switching	Boolean	0	0 to 1
Disable Device Probing	Boolean	0	0 to 1
Suppress Class F Traffic	Boolean	0	0 to 1
SYNC IO mode	Boolean	0	0 to 1
VC Encoded Address Mode	Boolean	0	0 to 1
Disable Translative Mode	Boolean	0	0 to 1
Switch PID Format	Number	1	0 to 2
Per-frame Route Priority	Boolean	0	0 to 1
Long Distance Fabric	Boolean	0	0 to 1

Domain — The domain number uniquely identifies the switch in a fabric. Normally, the fabric automatically assigns this value. The range of allowed values varies depending on the switch model and other system settings (refer to VC Encoded Address Mode).

BB Credit — The buffer-to-buffer (BB) credit represents the number of buffers available to attached devices for frame receipt. The range of allowed values varies depending on other system settings.

R_A_TOV — The resource allocation timeout value (R_A_TOV) displays in milliseconds. This variable works with the variable E_D_TOV to determine the switch's actions when presented with an error condition.

	Allocated circuit resources with detected errors are not released until the time value has expired. If the condition is resolved prior to the timeout, the internal timeout clock resets and waits for the next error condition.
E_D_TOV	Error detect time out value (E_D_TOV) displays in milliseconds. This timer flags a potential error condition when an expected response is not received (an acknowledgment or reply in response to packet receipt, for example) within the set time limit. If the time for an expected response exceeds the set value, then an error condition is met.
WAN_TOV	Wide Area Network Time Out Value (WAN_TOV) displays in milliseconds. This timer is the maximum frame timeout value for a WAN, if any, interconnecting the Fibre Channel islands
MAX_HOPS	Maximum Hops (MAX_HOPS) is an integer. It denotes the upper limit on the number of hops a frame might traverse to reach any destination port from any source port across the fabric. **Note:** The four configuration parameters R_A_TOV, E_D_TOV, WAN_TOV and MAX_HOPS, described above are inter-related. Assigning a specific value to one or more of these parameters can change the range of allowed values that are assigned to the other parameters. As a result, the user might not be able to set all the values with in the range displayed against each parameter. To make it easier, the configuration utility validates the modified values of these four parameters and prompts the user to re-enter them if the validation check fails.
Data Field Size	This specifies the largest possible value, in bytes, for the size of a type-1 (data) frame. The switch advertises this value to other switches in the fabric during construction of the fabric as well as to other devices when they connect to the fabric. Setting this to a value smaller than 2112 might result in decreased performance.
Sequence Level Switching	When set to 1, frames of the same sequence from a particular source are transmitted together as a group. When set to 0, frames are transmitted interleaved among multiple sequences. Under normal conditions, sequence-level switching should be disabled for better performance. However, some host adapters have performance issues when receiving interleaved frames from multiple sequences. When there are such devices attached to the fabric, sequence-level switching should be enabled.
Disable Device Probing	When this is set, devices that do not register themselves with the Name Server will not be present in the Name Server database. Set this mode only if the switch's N_Port discovery process (PLOGI, PRLI, INQUIRY) causes some attached device to fail.
Suppress Class F Traffic	By default, the switch can send Class-F frames. When this option is turned on, Class-F traffic is converted to Class-2 traffic before being transmitted.
SYNC IO mode	By default, SYNC IO is used for performance enhancement. When the option is set, SYNC IO is used.
VC Encoded Address Mode	When set, frame source and destination addresses utilize an address format compatible with some first-generation switches. Set this mode only if the fabric includes such switches. **Note:** VC-encoded address mode cannot be set in security mode. Also, when this mode is set, security mode cannot be enabled.
Disable Translative Mode	The setting is only relevant if VC-encoded address mode also is set. This feature, when set, disables translative addressing to achieve explicit address compatibility with some first-generation switches.

Set this feature only if hardware or software systems are attached to the fabric that explicitly relies on a specific frame address format.

Switch PID Format — The setting is only relevant if VC-encoded address mode is not set:

- 0 Native PID format (16 based, 16 port format), for fabrics with legacy low-count port switches.
- 1 Core PID format (0 based, 256 port format), preferred mode for mixed fabrics with legacy and new switches.
- 2 Extended Edge PID format (16 based, 256 port format), used in mixed fabrics with legacy and new switches to avoid rebooting host systems when static PID binded is used.

If VC-encoded address mode is not set, the default setting is 1. **Note: configDefault** does not change switch PID format.

Per-frame Route Priority — In addition to the eight virtual channels used in frame routing priority, support also is available for per-frame-based prioritization when this value it set. When pre-frame route priority set, the virtual channel ID is used in conjunction with a frame header to form the final virtual channel ID.

Long Distance Fabric — When this value is set, ISLs in a fabric can be up to 100 km long. The exact distance is determined by the per-port configuration on the E_Ports of each ISL. Configure both E_Ports in an ISL to run the same long-distance level; otherwise, the fabric segments.

The Brocade Extended Fabrics license is required to set this mode.

Virtual Channel Settings

You can tune the switch in a specific application by configuring the parameters for the switch's eight virtual channels. Note that the first two virtual channels are reserved for the switch's internal functions and are not user-configurable.

The default virtual channel settings are optimized for switch performance. Changing the default values can improve switch performance somewhat but also can severely degrade performance; you should not change these settings without fully understanding the effects.

Field	Type	Default	Range
VC Link Control	Number	0	0 to 1
VC Class 2	Number	2	2 to 5
VC Class 3	Number	3	2 to 5
VC Multicast	Number	7	6 to 7
VC Priority 2	Number	2	2 to 3
VC Priority 3	Number	2	2 to 3
VC Priority 4	Number	2	2 to 3
VC Priority 5	Number	2	2 to 3
VC Priority 6	Number	3	2 to 3
VC Priority 7	Number	3	2 to 3

VC Link Control — Specifies the virtual channel used for N_Port-generated, Class-2 link control frames (ACKs, P_BSYs, P_RJTs). Forces N_Port-generated link control frames to be sent using a Class-2 data virtual channel when set to 0. When this value is set to 1, the control frames are sent using a

virtual channel normally reserved for fabric-internal traffic. This setting is configurable only when VC-encoded Address Mode is set.

VC Class 2 — Specifies the virtual channel used for Class-2 frame traffic. This setting is configurable only when VC-encoded address mode is set.

VC Class 3 — Specifies the virtual channel used for Class-3 frame traffic. This setting is configurable only when VC-encoded address mode is set.

VC Multicast — Specifies the virtual channel used for multicast frame traffic. This setting is configurable only when VC-encoded address mode is set.

VC Priority — Specifies the class of frame traffic given priority for a virtual channel.

Switch Operating Mode

This configuration parameter is obsolete. Instead, use the **interopMode** command to control the switch interop mode.

Zoning Operation Parameter

The zoning operation parameters are shown in the following table.

Field	Type	Default	Range
Disable Nodename Zone Checking	Boolean	0	0 to 1
Default Access	Boolean	1	0 to 1

Disable Nodename Zone Checking — By default, zoning uses both port WWN and node WWN to perform zoning. However, when this value is set to 1, node WWN cannot be used in zoning.

Default access when zoning is not active — 0: No access
1: All access

RSCN Transmission Mode

The RSCN transmission mode parameter is shown in the following table.

Field	Type	Default	Range
End-device RSCN Transmission Mode	Number	1	0 to 2

Values range from 0 through 2, as follows:

0 RSCN only contains a single PID.

1 RSCN contains multiple PIDs.
2 Indicates fabric address RSCN.

NS Operation Parameter

The NS operation parameter is shown in the following table.

Field	Type	Default	Range
Pre-zoned response Mode	Boolean	0	0 to 1

Values range from 0 through 1, as follows:

0 Standard mode.

1 Pre-zoning mode.

Arbitrated Loop Settings

The following table defines changeable settings affecting Fibre Channel Arbitrated.

Field	Type	Default	Range
Send FAN frames?	Boolean	1	0 to 1
Always send RSCN?	Boolean	0	0 to 1
Enable CLOSE on OPEN Received?	Boolean	0	0 to 1
AL_PA 0x00?	Boolean	0	0 to 1
Initialize All Looplets?	Boolean	0	0 to 1

Send FAN frames? — Specifies whether fabric address notification (FAN) frames are sent to public loop devices to notify them of their node ID and address. Set to 1 to send, 0 to not send.

Always send RSCN? — After loop initialization, a remote state change notification (RSCN) is issued only when FL_Ports detect new devices or the absence of preexisting devices. When this feature is set, an RSCN will always be issued following the completion of loop initialization, regardless of the presence of new or absence of preexisting devices.

Enable CLOSE on OPEN Received? — There are compatibility issues between the Tachlite-based product and switches with Enable CLOSE on OPEN Received.

Value	Enable CLS on OPN
0	0 (Tachlite compatible)
1	1

AL_PA 0x00? — Some loop devices do not like AL_PA 0 on the same loop. This option provides a workaround for such devices. By default, the switch can use phantom AL_PA 0 for an embedded port in QuickLoop configuration. Set to 1 to have the switch not use AL_PA 0.

Initialize All Looplets? — By default, only looplets in the same zone reinitialize. Set to 1 to re-initialize all the looplets in QuickLoop.

System Services Settings

The following table defines changeable settings affecting Fibre Channel Arbitrated.

Field	Type	Default	Range
rstatd	Boolean	Off	On or Off
rusersd	Boolean	Off	On or Off
rapid	Boolean	On	On or Off
thad	Boolean	On	On or Off
Disable RLS	Boolean	On	On or Off

rstatd — Dynamically enables or disables a server that returns information through remote procedure calls (RPC) about system operation information. The protocol provides for a widerange of system statistics; however, only the Ethernet interface statistics (refer to **ifShow**) and system up time (refer to **uptime**) are supported.

	The retrieval of this information is supported by a number of operating systems that support RPC. On most UNIX-based systems (HP-UX, Irix, Linux, Solaris, and so on), the commands to retrieve the information are **rup** and **rsysinfo**. Refer to your local system documentation for the appropriate usage of **rup**, **rsysinfo**, or equivalent commands.
rusersd	Dynamically enables or disables a server that returns information through remote procedure calls (RPC) about the user logged in to the system. The information returned includes the user login name, the system name, the login protocol or type, login time, idle time, and remote login location (if applicable). The retrieval of this information is supported by a number of operating systems that support RPC. On most UNIX-based systems (HP-UX, Irix, Linux, Solaris, and so on), the command to retrieve the information is **rusers**. Refer to your local system documentation for the appropriate usage of **rusers** or equivalent command.
Rapid	Dynamically enables or disables API service.
Thad	Dynamically enables or disables Fabric Watch service.
Disable RLS	Enables or disables FCP RLS (read link state) information probing for F/FL_Port. It is disabled by default.

Portlog Events Disable/Enable Settings

Port events can be disabled from logging. The default is on, or enabled. When this setting is disabled, this event will not be logged by portlog.

Special Inputs

Carriage return	When entered alone at a prompt without any preceding input, accepts the default value (if applicable) and moves to the next prompt.
Interrupt	Aborts the command immediately and ignores all changes made.
End-of-file	When entered alone at the prompt without any preceding input, terminates the command, saving any changes made.

OPERANDS none

EXAMPLE

```
switch:admin> configure

     Configure...

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

    Domain: (1..239) [1]
    BB credit: (1..27) [16]
    R_A_TOV: (4000..120000) [10000]
    E_D_TOV: (1000..5000) [2000]
    WAN_TOV: (0..30000) [0]
    MAX_TOPS: (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]
```

```
    SYNC IO mode: (0..1) [0]
    VC Encoded Address Mode: (0..1) [0]
    Switch PID Format: (0..2) [21]
    Per-frame Route Priority: (0..1) [0]
    Long Distance Fabric: (0..1) [0]

  Virtual Channel parameters (yes, y, no, n): [no] y

    VC Priority 2: (2..3) [2]
    VC Priority 3: (2..3) [2]
    VC Priority 4: (2..3) [2]
    VC Priority 5: (2..3) [2]
    VC Priority 6: (2..3) [3]
    VC Priority 7: (2..3) [3]

  Zoning Operation parameters (yes, y, no, n): [no] y

    Disable NodeName Zone Checking: (0..1) [0]
    Default Access when zoning is not active (0 = NOACCESS 1 = ALLACCESS):
(0..1) [1]

  RSCN Transmission Mode (yes, y, no, n): [no] y

    End-device RSCN Transmission Mode
      0 = RSCN with single PID, 1 = RSCN with multiple PIDs, 2 = Fabric RSCN):
(0..2) [1]

  NS Operation Parameters (yes, y, no, n): [no] y

    Pre-zoned responses Mode
      (0 = Standard Mode, 1 = Pre-zoning On): (0..1) [0]

  Arbitrated Loop parameters (yes, y, no, n): [no] y

    Send FAN frames?: (0..1) [1]
    Always Send RSCN?: (0..1) [0]
    Enable CLOSE on OPEN received?: (0..1) [0]
    Do Not Allow AL_PA 0x00?: (0..1) [0]
    Initialize All Looplets?: (0..1) [0]

  System services (yes, y, no, n): [no] y

    rstatd (on, off): [off]
```

```
    rusersd (on, off): [off]
    rapid (on, off): [on]
    thad (on, off): [on]
    Disable RLS probing (on, off): [on]
  Portlog events enable (yes, y, no, n): [no]

     Committing configuration...done.
```

SEE ALSO

agtcfgDefault, agtcfgSet, agtcfgShow, configDefault, configShow, ifShow, ipAddrSet, portCfgLongDistance, switchDisable, switchEnable, uptime

New Error Messages

The following are new error messages in Fabric OS v2.6.2.

Fabric Reconfiguration Message

FABRIC-RECONFIG

Message

```
Switch: <number>, Info FABRIC-RECONFIG, 4, fabric: <reason>
```

Probable Cause

The fabric has reconfigured due to an offline port. The reason can be one of the following:

Fabric Merge
: Merging two fabrics.

Own ID Rcvd
: A subordinate switch receives an EFP or EFP ACC that has a payload error, listing this switch as being the principal switch.

Fabric Segment
: Principal port became segmented.

Offline
: Principal port went offline.

Unconfirmed domain
: Switch was not able to get a domain ID. RDI ACC was never received.

Rcv BF
: Received Build Fabric (BF) command.

HA: At F2 State
: According to the Fibre Channel specification, F2 is defined as the principal switch selection. If a failover occurs at this time, the switch is forced to restart principal switch selection.

HA: No Upstream
: After failover, the newly active fabric thinks it is subordinate, but there is no upstream.

HA: bad EFP resp
: Received an invalid EFP response.

HA: RJT EFP resp
: Received an EFP reject response in which this EFP was used for verifying the neighbor's domain list as part of fabric warm-start recovery. A reject occurs if the neighbor is reconfiguring or the neighbor's port is in a bad state.

HA: DLST EFP resp
: Received an EFP accept response with a different domain list.

HA: PPRI EFP resp
: Received an EFP accept response in which the response has a different principal switch priority number.

HA: PWWN EFP resp

Received an EFP accept response in which the response has a different principal switch World Wide Name.

HA: MAX EFP resp
: An EFP to a neighbor failed to respond, and the fabric reached its maximum retry count for this neighboring switch.

HA: Can't Snd EFP
: Was not able to send an EFP.

HA: Offline
: A principal port went offline during fabric daemon's warm-start recovery.

Principal Selection Mode
: User has run the **fabricprincipal** command, forcing a fabric rebuild.

D-list conflict
: The principal switch received a domain list with additional domains than what the principal switch has already assigned, and the payload has the Principal WWN and principal priority number as the principal switch.

Recommended Action
If the reconfiguration was unplanned, check for problems with the specified port. Some troubleshooting tasks include:

- Verify that the port was not disabled using the **portshow** command.
- Verify that the port is cabled correctly.
- Verify that the SFP has not deteriorated.

Refer to the Fibre Channel Standard FC-SW3, Chapters 6 and 7, for more information on fabric initialization.

Severity
Information

Security Messages

SEC-PIDCHGERR, PID Change failed: Change Area failed

Message

```
Switch: <number>, Error SEC-PIDCHGERR, 2, PID Change failed: Change Area failed.
<reason>
```

Probable Cause
Either the defined or active policy could not be updated. If the policy database is very large, it might not be able to change the area because the new policy database exceeds the maximum size. This message can also be caused when the switch is short of memory. The <reason> value can be defined or active, or both policy sets were failed by the daemon. A negative value means that a policy set was failed by the daemon.

Recommended Action
Reduce the size of the policy database.

Severity
Error

SEC-PIDCHGERR, PID Change failed: Size check failed

Message

```
Switch: <number>, Error SEC-PIDCHGERR, 2, PID Change failed: Size check failed.
<reason>
```

Probable Cause
Either the new defined or active policy was too large after modifying the area ID. The <reason> value can be defined or active, or both policy sets were failed by the daemon. A negative value means that a policy set was failed by the daemon.

Recommended Action
Reduce the size of the specified policy database.

Severity
Error

SEC-PIDCHGERR, PID Change failed: Switch is busy

Message

```
Switch: <number>, Error SEC-PIDCHGERR, 2, PID Change failed: Switch is busy.
<reason>
```

Probable Cause
The switch security daemon is busy updating something else. The <reason> value can be defined or active, or both policy sets were failed by the daemon. A negative value means that a policy set was failed by the daemon.

Recommended Action
For the first reject, wait a few minutes and then resend the transaction. Fabric-wide commands might take a few minutes to propagate throughout the fabric. Make sure to leave enough time so that your commands do not overlap in the fabric.

Severity
Error

SEC-PIDCHGINFO

Message

```
Switch: <number>, Info SEC-PIDCHGINFO, 4, PID Change: Success
```

Probable Cause
The PID format of the switch was changed either to or from extended-edge PID. If DCC policies existed, all area ID values either increased or decreased by 16. The values wrap around after a port value of 128. If a DCC policy contains an area of 127 before changing to displaced PID, then the new area is 15 because of the wraparound.

Recommended Action
No action is required.

Severity
Information

SEC-SECCHANGE

Message

```
Info SEC-SECCHANGE, 4, text message
```

Probable Cause

A major security event has occurred. This message is for information purposes only, but you should verify that the event was planned. The text messages for individual events are:

- secModeEnable: Secure mode has been enabled.
- secModeDisable: Secure mode has been disabled.
- secPolicyActivate: A, B, C policies have been changed. (A, B, C are names for changed policies.)
- secVersionReset: Secure fabric version stamp has been reset.
- secFCSFailover: The primary FCS has failed over to a new switch.
- All password changes: A, B, C account passwords have been changed. (A, B, C are account names for which passwords are changed.)
- configDownload: A configdownload process has been executed that changed the security policy database.
- secPolicySave: A change to the security policy database has been saved.
- SNMP community string change: The admin has made a change to the SNMP community strings.

Recommended Action

Verify that the security event was planned.

If the security event was planned, no action is required.

Severity

Information

PID Change Message

CONFIG-PIDCHANGE_EXTENDED_EDGE

Message

```
Switch: <number>, Warning CONFIG-PIDCHANGE_EXTENDED_EDGE, 3, Switch PID format
changed to Format 2 ('Extended Edge PID Format').
```

Probable Cause
The PID format for the fabric has been changed to Format 2, extended-edge PID. For more information on PID format, refer to the *Brocade Fabric OS Procedures Guide*.

Recommended Action
This message is for information purposes only. The entire fabric must be configured with the same PID format or the fabric will segment.

Severity
Warning

Defects Closed in Fabric OS v2.6.2d

Defects Closed In Fabric OS v2.6.2d		
Defect ID	**Severity**	**Description**
DEFECT000055489	High	Summary: In PID Format 2 (Extended Edge PID Format), extend the support beyond 127 ports. Solution: In PID Format 2 (Extend Edge PID FORMAT), change max port support to 256. Customer Impact: This change does not impact PID format 1 (the most common used Core PID Format). It only impacts PID format 2 (Extended Edge PID), usually used in statically PID binded hosts environment who wants to avoid host reboot during fabric migration to FOS 4.x. This does not impact current environment but is need for future bigger than 128 port count platforms. Reported in Release: V2.6.2
DEFECT000057465	High	Summary: Silkworm 2800 switch directly connected to a Silkworm48000 will segment when security is turned on. Symptom: The following scenarios have been tested: - Silkworm2800 - Silkworm48000 - fabrics will segment reported by switchShow - Silkworm2800 - Silkworm3800 - Silkworm48000 - No problem with a secure fabric - Silkworm2800 - Silkworm12000 - no problem with a secure fabric. Solution: Frame is received from Silkworm 48000 before SLAP_SEND_DONE flag is set on Silkworm2800, cause fabric segmentation. Workaround: Do not connect a Silkworm 2x00 switch directly to a Silkworm48000 or any newer platform switches. Use Silkworm3x00, Silkworm12000 (or any newer Bloom based switch) as in between switches. Customer Impact: Cannot connect a Silkworm2x00 switch directly to a Silkworm48000 switch when security and fabric segments are turned on. Probability: Medium Reported in Release: V2.6.2

Defects Closed In Fabric OS v2.6.2d		
Defect ID	**Severity**	**Description**
DEFECT000054750	Medium	Summary: Can not create DCC_POLICY by using * to include port numbers greater than 127 in the DCC_POLICY. Symptom: secpolicycreate "DCC_POLICY", "domainid(*)" on a platform with more than 128 port, fails with VERIFY - Failed expression: strlen(mbrBuf) > 0 Solution: Adjust security code constant definition to handle 256 ports. Customer Impact: This defect does not impact current install base. The fix is needed when new platform with greater than 128 ports is introduced in fabric with security feature on. Reported in Release: V2.6.2

Defects Closed in Fabric OS v2.6.2c

Defects Closed In Fabric OS v2.6.2c		
Defect ID	**Severity**	**Description**
DEFECT000048158	High	Summary: After switch reboot, device login fails unless port is reset Symptom: After the switch reboot some ports could not login into fabric without a disable/enable related to that switch port. Solution: ppen on a fully loaded switch. The solution is to move the clearing of the flags to before the flogi message is generated. Thus if the tzone or tfpsf task get preempted, there is no race condition to clearing the flags. Workaround: portdisable; portenable Customer Impact: This is a race condition and happens rarely on a fully loaded switches. Service Request# RQST00000031494 Reported in Release: V2.6.0

Defects Closed In Fabric OS v2.6.2c		
Defect ID	**Severity**	**Description**
DEFECT000048208	High	Summary: CRITICAL MQ-QWRITE on 2.6.2 with 40+ "phantom" fabrics Symptom: In a large fabric with Fabric Channel Router, CRITICAL MQ_QWRITE observed on multiple queues. Solution: FC response from remote may not have the LASTSEQ bit set in the FCTL field. In such case, if local switch is the originator of the request, simply free the exchange. so semaphore are released for other queues. Workaround: SwitchDisable; SwitchEnable Customer Impact: This defect was pre-existing since beginning of 2.x release. It's now exposed by stress testing with large fabric (FCR in fabric). Once it happens only switchdisable and switchenable can recover. Reported in Release: V2.6.2

Defects Closed in Fabric OS v2.6.2b

Defects Closed In Fabric OS v2.6.2b		
Defect ID	**Severity**	**Description**
DEFECT000040164	High	Summary: Fabric Manager failed to activate security policies via Policy Editor. Symptom: The attempt to activate security policies via Policy Editor fails with following error: Error code: 0 - Unknown error encountered. Solution: 1. In secFCSInformActivate add a delay of 2 ticks in semaTake to allow lower priority api task to run. 2. Increase RAPI stack size to 20000. Reported in Release: V2.6.2

Defects Closed In Fabric OS v2.6.2b		
Defect ID	**Severity**	**Description**
DEFECT000043870	High	Summary: Watchdog reset when different layer of codes access the same data structure corrupts mr_lock. Symptom: Switch panic with trace indicates problem with the routine INTERNAL (license_db_close). This does DB_LOCK (mrLock) followed by deletion of the structure that holds the lock, followed by a DB_UNLOCK (mrUnlock). Solution: Stop API and MS layer from using 'close' functions in layers below it. All API and MS access now goes through the same MR_LOCK library interface. Service Request# RQST00000029381 Reported in Release: V2.6.0
DEFECT000044775	High	Summary: Switch reboots in secured fabric upon running zoning tests through API. Symptom: Switch panic when running zoning stress through API to add multiple ZoneMembers to an Alias. Solution: Replace taskNameToId() call with one of the new routines that are task safe. Reported in Release: V2.6.2
DEFECT000045655	High	Summary: Extended Edge Format issue found when directly connect host/device to FOS 2.6.2 Symptom: Host does not see device when change pid format to Format 2 a.k.a Extended Edge Format, when zoning is enforced. Solution: Compare port area while programming hardware enforced zoning. Service Request# RQST00000030030 Reported in Release: V2.6.2
DEFECT000043324	Medium	Summary: Unable to received fabric watch email alert on SW2800 Symptom: Unable to configure Fabric Watch Email with certain gateway. Solution: Add extra newline as in mime mail format required by protocol. Service Request# RQST00000028512 Reported in Release: V2.6.1

Defects Closed In Fabric OS v2.6.2b		
Defect ID	**Severity**	**Description**
DEFECT000044325	Medium	Summary: Improper termination of scripted telnet sessions causes SW2800 to hang Symptom: Loss access to switch via telnet. Solution: Fix hangs when pipes are blocked both ways on telnet. Service Request# RQST00000028703 Reported in Release: V2.6.1
DEFECT000044603	Medium	Summary: Fabric Manager Call Home triggers multiple e-mails with single switch event. Symptom: On some switches, the Health Status changes before the Status Reason is populated. First e-mail is triggered because the switch health changes. Then when the Status Reason is populated on the switch back-end, another e-mail is triggered. Solution: Fixed a Fabric Watch locking issue so switch status is populated before Fabric Manager polls for data. Reported in Release: V2.6.2
DEFECT000046698	Medium	Summary: "malloc failed" panic on SilkWorm2800 when using webtool Symptom: memshow indicates on going memory leak when there are active web tool sessions. Solution: 1. When convert date format, Web tool fails to free allocated memory. 2. When private devices are connected to a switch and do not respond to the PDISC, memory allocated to store the translated frame is not freed. Memory was freed only upon receive a response. Both memory leaks described above are being corrected. Service Request# RQST00000030728 Reported in Release: V2.6.2
DEFECT000047345	Medium	Summary: Fabric Watch email message being rejected due to malform mime. Symptom: With certain gateway, fw mail alert can not go through with following observed during analysis: Requested action not taken: Nonstandard SMTP line terminator. Solution: Change all "/n" to "/r/n" according to protocol in mime header. Service Request# RQST00000030941 Reported in Release: V2.6.2

Defects Closed In Fabric OS v2.6.2b		
Defect ID	**Severity**	**Description**
DEFECT000048180	Low	Summary: Unrecognized character in empty syslog daemon ip box on webtools Symptom: Syslog Daemon IP of WebTools display unrecognized characters when No IP configure. Solution: Fixed uninitialized character array being displayed as junk data. Reported in Release: V2.6.2

Defects Closed in Fabric OS v2.6.2a

Defects Closed In Fabric OS v2.6.2a		
Defect ID	**Severity**	**Description**
DEFECT000038701	High	Summary: Switch fails to send swFabricWatchTrap Symptom: Remove and insert the ISL several times, observe that switch fails to send swFabricWatchTrap for events in the following areas: - eportSync - eportSignal - eportState - fopportLink - fopportSync - fopportSignal - fopportState Solution: Change the interface called to get thresholds on errors for a port, as the port may be offline by the time we decide to send a trap. Customer Impact: The fix will be coordinated across releases. Service Request# RQST00000026464 Reported in Release: V2.6.2
DEFECT000036739	Medium	Summary: The cfgszie command output is different from other FabOS releases in interopmode. Symptom: In the same interopmode fabric, cfgsize output on switch running FabOS 2.x is different from switches running FabOS 3.x and FabOS 4.x. Solution: Calculate the zone db size in interopmode correctly. Customer Impact: This is a display inconsistency issue across releases and the fix needs to be coordinated. Probability: High Reported in Release: V2.6.2

Defects Closed In Fabric OS v2.6.2a		
Defect ID	**Severity**	**Description**
DEFECT000038125	Medium	Summary: Help page for 'configure' command needs updating across all platforms Symptom: Configure help page does not accurately offer customer the necessary information to configure the switch. Solution: Modified configure help page to reflect latest code Customer Impact: The fix will be coordinated across future releases. Probability: High Reported in Release: V2.6.2
DEFECT000039505	Medium	Summary: Switch reboots when access FCP related data through CLI or SNMP. Symptom: Trace show has following frame on stack back trace: Address: _fcpRlsGet + 0x5c (0x104b231c) Solution: Check that the port given to access data structures is not an embedded port. Service Request# RQST00000027931 Reported in Release: V2.6.1
DEFECT000040846	Medium	Summary: Zoning transaction aborted logged at Error level causes Call Home. Symptom: End user uses API to intentionally abort zone transaction and saw following in errlog: Error ZONE-TRANS_ABORT, 2, Zone transaction aborted - Solution: Change log level from Error to Info when abort zone transaction Service Request# RQST00000028262 Reported in Release: V2.6.2