



# Brocade Fabric OS v5.0.3 GA Release Notes v1.0

December 23, 2005

## ***Document History***

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v5.0.3 Release Notes v1.0	First release.	December 23, 2005

Copyright © 2005, Brocade Communications Systems, Incorporated.

ALL RIGHTS RESERVED.

BROCADE, the Brocade B weave logo, Brocade: the Intelligent Platform for Networking Storage, SilkWorm, and SilkWorm Express, are trademarks or registered trademarks of Brocade Communications Systems, Inc. or its subsidiaries in the United States and/or in other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

FICON® is a registered trademark of IBM Corporation in the US and other countries.

Notice: The information in this document is provided “AS IS,” without warranty of any kind, including, without limitation, any implied warranty of merchantability, noninfringement or fitness for a particular purpose. Disclosure of information in this material in no way grants a recipient any rights under Brocade's patents, copyrights, trade secrets or other intellectual property rights. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

Notice: The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find-out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

Export of technical data contained in this document may require an export license from the United States Government.

## TABLE OF CONTENTS

Document History.....	1
About This Release.....	5
Overview .....	5
SilkWorm 48000.....	5
SilkWorm 200E .....	6
Supported Switches .....	6
Firmware Upgrades .....	6
Technical Support.....	7
Standards Compliance .....	7
OS Requirements .....	8
Important Notes .....	8
Upgrading and Installing FC4-16 and FC4-32 Blades.....	8
General .....	8
Merging Zones.....	12
Web Tools .....	12
Other Notes.....	16
Documentation Updates.....	19
Fabric OS Administrator's Guide .....	19
Fabric OS Command Reference Manual .....	30
Fabric OS MIB Reference Manual .....	34
Fabric OS System Error Message Reference Manual.....	36
Fabric Watch User's Guide .....	39
Secure Fabric OS Administrator's Guide .....	39
SilkWorm 200E Hardware Reference Manual .....	40
SilkWorm 3250/3850 Hardware Reference Manual.....	41
SilkWorm 4020 Hardware Reference Manual.....	41
SilkWorm 4100 Hardware Reference Manual.....	41
SilkWorm 12000 Hardware Reference Manual.....	42
SilkWorm 24000 Hardware Reference Manual.....	43
SilkWorm 48000 Hardware Reference Manual.....	46
SilkWorm Director Blade Support Notes .....	46
Web Tools Administrator's Guide.....	46
Closed Defects in Fabric OS v5.0.3 GA .....	50
Closed Defects in Fabric OS v5.0.1d.....	68
Closed Defects in Fabric OS v5.0.1c.....	69

Closed Defects in Fabric OS v5.0.1b.....70

Closed Defects in Fabric OS v5.0.1a.....79

## About This Release

Fabric OS v5.0.3 is a Maintenance Release containing fixes to address a list of new/pending issues since the release of 5.0.2, which supports an OEM unique hardware platform. FOS v5.0.3 includes a number of defect fixes not deemed to be required in a patch release, but necessary to get to our customers before the next scheduled feature release. Aside from these changes, Fabric OS v5.0.3 is functionally identical to earlier releases of Fabric OS v5.0.x.

## Overview

Brocade Fabric OS v5.0.2 supports one additional platform: the SilkWorm 4020.

Brocade Fabric OS v5.0.1 supports two additional platforms: the SilkWorm 48000 256-port director and the SilkWorm 200E standalone switch.

## SilkWorm 48000

The SilkWorm 48000 director is based on the proven technology and innovation that has earned Brocade clear market share leadership in the SAN market. Brocade is the only vendor that offers the full spectrum of products from entry to enterprise, for multi-protocol routing and SAN solutions for bladed servers. Brocade leads in every category in the industry with the first 4 Gbit/sec products. Brocade's Advanced Fabric Services, which are delivered across the product family, are also extended with the introduction of the SilkWorm 48000.

- **High-end performance:** The SilkWorm 48000 is the industry's first Fibre Channel director that supports 4 Gbit/sec port speeds. It delivers exceptional performance and scalability with up to 256 ports in a single domain. The high-performance architecture provides auto speed negotiation to support legacy 1 and 2 Gbit/sec server and storage devices as well as new and forthcoming 4 Gbit/sec devices. The new 4 Gbit/sec technology also provides the ability to aggregate up to eight 4 Gbit/sec ports to create an Inter-Switch Link (ISL) trunk at up to an unprecedented 32 Gbit/sec of bandwidth between directors. High-end performance also applies to the extension of Fibre Channel over distance, supporting distances up to 500 kilometers. Trunking in the SilkWorm 48000 can also be extended over distance, enabling new levels of performance between data centers.
- **Investment protection:** Fully compatible with existing Brocade storage network offerings, the highly flexible blade format of the SilkWorm 48000 provides "pay-as-you-grow" scalability and support for multiple protocols and transports. Routing with Logical Private SAN (LSAN) enables secure selective sharing of resources between isolated SANs. FICON and CUP support enables an intermix of mainframe and open systems in a consolidated SAN.
- **Mission-critical availability, scalability, and flexibility:** The SilkWorm 48000 is designed for continuous operation. It supports "five-nines" availability with built-in redundancy; FRUs capable of hot-swap install/uninstall, and hardware and software upgrades concurrent with operation. The SilkWorm 48000 provides 256 ports per system and 768 ports per rack to help maximize valuable data center real estate. The leading network scalability of the Brocade SilkWorm family of products is extended with the SilkWorm 48000, which provides the largest building block for creating the largest storage networks.
- **Lower Total Cost of Ownership (TCO):** The SilkWorm 48000 lowers the overall costs of deploying and operating SAN infrastructures. With twice the port density of previous directors, the SilkWorm 48000 delivers more efficient use of expensive data center floor space. Lower power consumption per port represents significant cost savings in electricity and cooling expenses for the data center, as much as \$10,000 per year per system. More ports per director also means fewer devices to manage in large fabrics, improving administrative efficiencies for IT departments.

Fabric OS v5.0.1 includes all basic switch and fabric support software, as well as optionally licensed software enabled via license keys. It comprises two major software components: firmware, which initializes and manages the switch hardware, and diagnostics.

Optionally licensed products include:

- Brocade Extended Fabrics—Provides up to 500 km of switched fabric connectivity at full bandwidth over long distances.
- Brocade ISL Trunking Over Extended Fabrics—ISL Trunking has been enhanced to enable trunking over long-distance links of up to 250 km via a new command.
- Brocade Web Tools—Enables administration, configuration, and maintenance of fabric switches and SANs.
- Brocade Fabric Manager—Enables administration, configuration, and maintenance of fabric switches and SANs with host-based software.
- Brocade Advanced Performance Monitoring—Enables performance monitoring of networked storage resources.
- Brocade Fabric Watch—Monitors mission-critical switch operations.

Included in every switch:

- Brocade Advanced Zoning—Segments a fabric into virtual private SANs.

**NOTE:** Brocade software release policy is to carry forward all fixes in patches to subsequent maintenance and feature releases of Fabric OS.

## SilkWorm 200E

As the latest addition to the SilkWorm family of fabric switches and directors, the SilkWorm 200E provides small-to medium-size businesses deploying their first SAN or expanding their current SAN with low-cost access to easy-to-manage SAN technology. The SilkWorm 200E provides the lowest-cost 8- to 16-port SAN switch available for those who want the benefits of SAN solutions with the option to scale to larger fabrics on a “pay-as-you-grow” basis.

Brocade further simplifies the process of implementing SAN solutions with the SilkWorm 200E. The simplicity and ease-of-use features of the SilkWorm 200E help increase administrator productivity and lower the cost of management, which can benefit organizations with limited IT expertise. In addition, the SilkWorm 200E leverages industry-leading 4 Gbit/sec Fibre Channel technology to provide extremely high performance.

Delivering 8, 12, or 16 ports in a 1U form factor, the SilkWorm 200E enables substantial cost savings—from capital and operating expenses to overall management. It extends the Brocade modular building block approach to the development of storage networks. This approach has been widely adopted by storage networking vendors and is the de facto standard in the storage networking industry. The SilkWorm 200E stands up to any mission-critical test and offers significant business and performance advantages to small- to medium-size businesses as they develop and grow.

## Supported Switches

Fabric OS v.5.03 supports the SilkWorm 200E, 4020, 48000, 200E, 3014, 3016, 4012, 3250, 3850, 3900, 4100, 12000, and 24000, 48000.

## Firmware Upgrades

The recommended procedure for upgrading Fabric OS firmware levels is to limit the release levels to two or fewer releases. For example, upgrading a switch from v4.1.0 to v5.0.1 requires a two-step process: first upgrading to v4.4.0 and then upgrading to v5.0.1.

## Technical Support

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

### 1. General Information

- Technical Support contract number, if applicable
- Switch model
- Switch operating system version
- Error numbers and messages received
- **supportSave** 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 3016 and 4012—Side of switch module
- SilkWorm 200E—Nonport side of the chassis
- SilkWorm 3250, 3850, and 3900—Bottom of the chassis
- SilkWorm 4100—On the switch ID pull-out tab located on the port side and on the inside of the chassis, near power supply 1 (on the right when looking at the nonport side)
- SilkWorm 12000, 24000, and 48000 directors—Inside front of the chassis, on the wall to the left of the ports
- SilkWorm Multiprotocol Router Model AP7420—On the bottom of the chassis and on the back of the chassis

### 3. World Wide Name (WWN)

- SilkWorm 200E, 3016, 3250, 3850, 3900, 4012, and 4100 switches and SilkWorm 12000, 24000, and 48000 directors—Provide the license ID. Use the **licenseIDShow** command to display the license ID.
- SilkWorm Multiprotocol Router Model AP7420—Provide the switch WWN. Use the **switchShow** command to display the switch WWN.
- All other SilkWorm switches—Provide the switch WWN. Use the **wwn** command to display the switch WWN.

## Standards Compliance

Brocade Fabric OS v5.0.3 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 this Brocade Web site:

<http://www.brocade.com/sanstandards>

## OS Requirements

The following table summarizes the versions of Brocade software supported in this release. These are the *earliest* software versions that interoperate. Brocade recommends using the *latest* software release versions to get the most benefit from the SAN.

For a list of the effective end-of-life dates for all versions of Fabric OS, visit the following Brocade Web site:

[http://www.brocade.com/support/end\\_of\\_life.jsp](http://www.brocade.com/support/end_of_life.jsp)

	General Compatibility
SilkWorm 4012	v5.0.0 or later
SilkWorm 2000 series	v2.6.2 or later
SilkWorm 3200 and 3800	v3.1.3 or later
SilkWorm 3016, 3250, 3850, 3900, 12000, and 24000	v4.2.2 or later
SilkWorm 200E and 48000	v5.0.1 or later
SilkWorm 4100	v4.4.0c or later
SilkWorm AP7420	V7.3.0 or later
Fabric Manager	4.1.1c or later

## Important Notes

This section lists information that you should consider when running Fabric OS v5.0.1.

As of May 15, 2005, Brocade no longer includes a PKI Certificate as part of the installed Secure Fabric OS. If you wish to activate Secure Fabric OS on a supported director or switch, you must contact Brocade to obtain a PKI certificate.

Refer to the *Secure Fabric OS Administrator's Guide*, Chapter 2, “Adding Secure Fabric OS to the Fabric,” for a description of how to obtain certificates from the Brocade Certificate Authority.

## Upgrading and Installing FC4-16 and FC4-32 Blades

If you are planning to install FC4-16 or FC4-32 blades, you must upgrade firmware to Fabric OS v5.0.1 on both CPs *before* you install the blades.

### General

The major new features incorporated in Fabric OS v5.0.1 are summarized in the following sections.

### SilkWorm 48000 Platform Support

The SilkWorm 48000 places Condor-ASIC-based port and CP blades into the same core-edge infrastructure that was provided by the SilkWorm 24000 product. When a system is fully populated, it supports 256 ports in a single domain.

#### System/Blade Identification

Two CP blades that have different processors and slightly different hardware characteristics can co-exist in an active/standby relationship in the same SilkWorm 48000 chassis.

The platform identifiers for the two blades differ – largely to support the proper selection of platform-specific RPMs for the two different blades. When **switchShow** is issued from an active SilkWorm 24000 CP blade, and the same

command is issued when the SilkWorm 48000 CP blade is the active CP blade, **switchShow** shows two different switchType values. The switch type, however, tracks with the active CP blade – just as it does for the SilkWorm 24000 and 12000.

The condition of heterogeneous CP blades in a single chassis is designed to be transient. It should exist only until you have upgraded the system to homogeneous blades. However, Fabric OS does not distinguish between the cases in which the mixed configuration exists for a short period of time or a longer period of time.

### Chassis Configuration Options

With the Fabric OS v4.4.0 release, a new command, **aptPolicy**, allowed you to configure which egress port is selected for a frame, based on a particular policy:

- Port-based path selection (paths are chosen based on ingress port and destination only). This also includes user-configured paths. (Required for FICON see below)
- Device-based path selection (paths are chosen based on SID and DID). Note: Device based routing is currently not used and should not be activated at any time.
- Exchange-based path selection (paths are chosen based on SID, DID, and OXID). This is the default routing policy for Open Systems environments.
- For the SilkWorm 48000, the **aptPolicy** command is not available unless the chassis has been configured to run using option 5 described in the table below.

With the introduction of Fabric OS v5.0.1b and FICON support for the SilkWorm 4100 and 48000, the **aptPolicy** routing policy for FICON must be configured for port-based path selection on any director or switch with FICON devices attached. Other switches that reside in the fabric with Open Systems devices exclusively can remain configured as exchange-based routing. Any Brocade-supported FICON platforms can be cascaded without issue with FICON devices attached for backwards compatibility (that is, you can connect any of the SilkWorm 3900, 4100, 12000, 24000, and 48000 together).

For all other chassis configurations modes (1-4), the default routing policy is port-based path selection (paths are chosen based on ingress port and destination only). This cannot be changed. This also includes user-configured paths.

**NOTE:** Chassis configuration mode 1 is supported for FICON. Chassis configuration modes 2-4 are not supported for FICON configurations.

**Table 1 SilkWorm Chassis Option Descriptions**

Option	Number of Domains: Domains	Routing Module	Supported CPs	Supported Port Blades	Implications/Notes
1	1: 128	CER	CP2 or CP4	FC2-16, FC4-16	CP4 will be faulted if inserted into a D2 chassis
2	2: 64/64	CER/CER	CP2 only	FC2-16 only	
3	2: 64/64	CER/XYR	CP2 only	Left side: FC2-16 Right side: 12K	Same support as Fabric OS v4.4
4	2: 64/64	XYR/CER	CP2 only	Left side: 12K Right side: FC2-16	Same support as Fabric OS v4.4
5	1: 256	RTE	CP4 only	FC4-16, FC4-32	CP4 will be faulted if inserted into a D2 chassis

**Key**

CER = Core Edge Routing. Port-based routing scheme, same as routing option supported in v4.2 and v4.4

XYR = X-Y Linear Routing. Routing scheme used on SW12000 switches

RTE = Advanced Routing. Exchange-based (default) or device-based routing scheme

CP2 = SilkWorm 24000 CP blade

CP4 = SilkWorm 48000 CP blade

FC2-16 = 2G, 16-port blade

FC4-16 = 4G, 16-port blade

FC4-32 = 4G, 32-port blade

12K = SilkWorm 12000-port blade (2G, 16-port)

**SilkWorm 200E Platform Support**

The SilkWorm 200E is a 16-port pizza-box Fibre Channel switch using the Brocade Goldeneye ASIC. The Goldeneye ASIC implements a large subset of Brocade Condor ASIC functionality. Fabric OS v5.0.1 supports this platform including the SilkWorm 200E ports-on-demand (POD) features, which delivers 8, 12, or 16 ports in a 1U form factor.

**Reliability**

This release of Fabric OS features RSCN suppression: the ability to control RSCNs originating from hosts on a port-by-port basis.

## Enhanced RAS Log Messages

New with Fabric OS v5.0.1 are Zoning Audit messages. These messages record information about the type of zoning change made (including such tasks as **cfgenable** and **cfgdisable**) and the role level and user name making the changes. The messages are recorded in the RASlog whether change was made through the CLI or Web Tools. Note that occasional redundant entries are possible due to an extra HTTP entry when zoning changes are performed through the CLI.

## Scalability

Scaling the SAN is addressed under two topics:

- Single switch scalability, that is, the ability to handle up to 256 switch ports with some number of directly attached Nx\_Port types or the ability to effectively operate in a multiple-switch environment
- Fabric scalability, that is, the maximum number of ports and domains available fabric-wide

### Single Switch Scalability

The parameters specified here describe the number and types of ports that can be directly attached to a single-switch SW48000 domain:

- Maximum 256 user ports active on a single domain
- Maximum 252 initiators attached to a SilkWorm 48000 (with the balance of the ports connected to target ports, or ISLs)
- Maximum 14 switch ports connected to loops (for example, JBODs) of up to 24 devices (with the balance of the switch ports connected to N-Ports)

The rate of N-port connections is metered to ensure that devices sensitive to timeouts (such as in FICON environments) are not adversely affected. This mechanism delays N-port connections until all members of the fabric become reachable (allows routing and fabric formation to proceed without competition for CPU from N-port related service loads). When all these conditions are met, all ports that have been disabled for this reason are re-enabled.

## Fabric Scalability

Fabric OS v5.0.1 supports the same fabric scalability as Fabric OS v4.4.0, that is, 2,650 ports with 50 domains.

## FICON

FICON is now supported for the SilkWorm 48000 and 4100 platforms.

The FICON protocol is now supported on the following SilkWorm models and Fabric OS releases:

- SilkWorm 48000 and Fabric OS v5.0.1b  
A single-domain configuration is supported with a mix of 16-port and 32-port SilkWorm 48000 port blades in a SilkWorm 48000 director. Dual-domain configurations are not supported on the SilkWorm 48000 director. Mixed port blade configurations with SilkWorm 24000 and SilkWorm 48000 port blades in the same director are not supported in a FICON environment.
- SilkWorm 4100 and Fabric OS v5.0.1b

Both the SilkWorm 48000 and 4100 require the port-based routing policy either in a single-switch configuration or a cascaded-switch configuration only on those switches in the fabric that contain FICON devices (option 1 of the **aptPolicy** command). Other switches in the fabric may exist with the default exchange-based routing option (option 3 of the **aptPolicy** command) if only Open Systems devices are attached to those switches.

CUP is supported on SilkWorm 4100 and 48000 running Fabric OS 5.0.1b.

Fabric OS provides standard support for FICON single-switch operation. Multiple-switch cascaded FICON operation (double-byte addressing) requires a Brocade Secure Fabric OS license.

Control Unit Port (CUP) operation requires a Brocade FICON CUP license.

Although there are no specific zoning rules related to FICON environments, it is recommended that you follow standard FCP zoning practices. For management purposes, put FCP devices in one zone and FICON devices in another zone when operating in a mixed environment.

Any Brocade-supported FICON platforms can be cascaded without issue with FICON devices attached for backwards compatibility (that is, you can connect any of the SilkWorm 3900, 4100, 12000, 24000, and 48000 together).

For further information on FICON, refer to the latest Brocade technical documentation for the Fabric OS v 5.0.1 and Fabric Manager 5.0.0.

## Problem Determination

Fabric OS v5.0.1 features the **FcPing** command, which provides the ability to check Fibre Channel connectivity between any two nodes in a fabric.

## Security-Related Enhancement

A new role-based access control role, switch administrator, allows an administrator to control a switch but not modify any fabric-wide configuration, that is, security, zoning, or user configuration (see the **userConfig** command).

## Merging Zones

Before linking two switches together, it is important to know the zone database limit of adjacent switches. For details, refer to the section “Merging Zones,” in the *Fabric OS Administrator’s Guide* documentation update on [page 19](#) of this document.

## Web Tools

For instructions on installing Mozilla 1.6 on Solaris 2.8 and Solaris 2.9, refer to the following Web site:

<http://www.mozilla.org/releases/mozilla1.6/installation.html>

**Issue:** The Mozilla browser does not support the Switch Admin module properly in Fabric OS v2.6.x. In Fabric OS v2.6.2, a warning message is displayed. For other v2.6.x versions, no warning message is displayed.

**Workaround:** Use Netscape 4.7.7 or later.

The added supported browsers, operating systems, and Java Plug-ins introduce the following limitations when using mixed OS versions in Web Tools v5.0.1, as identified in the following table.

### Web Tools Compatibility Limitations

Launch Switch Environment	Problems
<b>Firmware:</b> Fabric OS v3.1.0+, v4.1.0+, or v5.0.1+ <b>Operating System:</b> Any supported operating system (with supported browser) <b>Browser:</b> Any supported browser (on supported operating system)	<b>Issue:</b> When viewing the topology from Web Tools, if your initial login was a v3.1.0+, v4.1.0+, or v5.0.1+ switch and you view the topology from a switch with a previous version of the Fabric OS, there is no print function available in the Fabric Topology window.  Web Tools v3.1.0+, v4.1.0+, and v5.0.1+ include a Print button in the Fabric Topology window; earlier versions do not.  <b>Workaround:</b> If the Fabric Topology window does not include a Print button, right-click anywhere inside the window and select <b>Print</b> from the popup menu.

Launch Switch Environment	Problems
<b>Firmware:</b> Fabric OS v2.6.x <b>Operating System:</b> Solaris <b>Browser:</b> Mozilla	<p><b>Issue:</b> The Switch Admin does not launch correctly.</p> <ul style="list-style-type: none"> <li>• If you try to launch Switch Admin using Fabric OS v2.6.2 on a Solaris operating system with a Mozilla browser, a warning message is displayed, telling you to use the Netscape browser.</li> <li>• If you try to launch 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.</li> </ul> <p><b>Workaround:</b> 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 on a switch running Fabric OS v2.6.x from a Solaris operating system, use the Netscape 4.77 browser.</p>
<b>Firmware:</b> Version <i>prior</i> to Fabric OS v2.6.2, v3.1.2, or v4.2.0 with secure mode enabled <b>Operating System:</b> Solaris <b>Browser:</b> Mozilla	<p><b>Issue:</b> If you try to launch 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.</p> <p><b>Workaround:</b> 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 or later from a Solaris operating system, use the Netscape 4.77 browser.</p>
<b>Firmware:</b> Version <i>prior</i> to Fabric OS v2.6.2, v3.1.2, or v4.2.0a <b>Operating System:</b> Any supported operating system (with supported browser) <b>Browser:</b> Any supported browser (on supported operating system)	<p><b>Issue:</b> 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.</p> <p><b>Workaround:</b> Use a launch switch running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later to access the switch.</p>
<b>Firmware:</b> Version <i>prior</i> to Fabric OS v4.4.0 <b>Operating System:</b> Any supported operating system (with supported browser) <b>Browser:</b> Any supported browser (on supported operating system)	<p><b>Issue:</b> When trying to perform end-to-end monitoring (Brocade Advanced Performance Monitoring) on a local switch with a Fabric OS prior to v4.4.0, the SilkWorm 4100 is displayed as a 16-port switch.</p> <p><b>Workaround:</b> For a SilkWorm 4100, use a launch switch running Fabric OS v4.4.0 or later to perform end-to-end monitoring on the switch.</p>

Launch Switch Environment	Problems
<b>Firmware:</b> Version <i>prior</i> to Fabric OS v4.4.0 <b>Operating System:</b> Any supported operating system (with supported browser) <b>Browser:</b> Any supported browser (on supported operating system)	<b>Issue:</b> When trying to perform zoning on a local switch with a Fabric OS version prior to v4.4.0, the SilkWorm 4100 is displayed as a 16-port switch. <b>Workaround:</b> If you are running Brocade Secure Fabric OS, select a switch running Fabric OS v4.4.0 or later as the primary FCS switch. If you are not running Brocade Secure Fabric OS, use a launch switch running Fabric OS v4.4.0 or later to perform zoning on the switch.
<b>Firmware:</b> Version <i>prior</i> to Fabric OS v2.6.2, v3.1.2, or v4.2.0 <b>Operating System:</b> Solaris <b>Browser:</b> Netscape	<b>Issue:</b> Any switches running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later are unsupported through Netscape. <b>Workaround:</b> 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 v1.6 to manage all of your switches from a Solaris operating system.
<b>Firmware:</b> Version <i>prior</i> to Fabric OS v2.6.1, v3.0.x, or v4.0.x <b>Operating System:</b> Windows <b>Browser:</b> Internet Explorer	<b>Issue:</b> When you are trying to run Fabric View with a large fabric, the browser might crash. <b>Workaround:</b> Use a launch switch that runs Fabric OS v2.6.1, v3.0.x, or v4.0.x or later so that you can use Switch Explorer (not Fabric View).  Use a launch switch with v.2.6.2, v3.1.x, or v4.1.x or later.
<b>Firmware:</b> Fabric OS v5.0.1+ <b>Operating System:</b> Any supported operating system (with supported browser) <b>Browser:</b> Internet Explorer and Mozilla	<b>Issue:</b> If you upgrade from Fabric OS v4.x to v5.x, you must upgrade your Java plug-in version to v1.4.2_06 from any prior version installed on your system. <b>Workaround:</b> For Internet Explorer, before launching Web Tools, check your Java plug-in version. If you have a version lower than 1.4.2_06, then you must uninstall it. When you launch Web Tools and you see a warning about a missing plug-in, follow the prompts. This procedure will make sure that the correct plug-in version is actually installed.  For Mozilla, follow the Mozilla Java plug-in installation instructions to install Java v1.4.2_06.

## Requests For Enhancement

The 5.0.3 Maintenance Release includes the following Requests for Enhancement (RFEs):

RFE #	Description
3545	Log the history of firmware versions whenever there is a firmware downgrade or upgrade performed on the switch
2365	Change the message when issuing the HAFailover command so it queries the user about to "fail the control processor."

<b>3273</b>	<b>Change the message for a successful login message in the event log so it shows the IP address of the station logging in.</b>
<b>3073</b>	<b>Change portlog event settings to be persistent across reboots.</b>
<b>2887</b>	<b>Allow the Switch Names to support the '-' character.</b>
<b>3474</b>	<b>Allow general users to determine the MAC address of an ethernet port.</b>

## Other Notes

The tables below list other important information you should consider about the SilkWorm 4012, SilkWorm 48000, and Fabric OS v5.0.1.

<b>SilkWorm 4012</b>	<b>Description</b>
Chassis	Early versions of the SilkWorm 4012 (including units used for beta) have the potential to interfere with a Cisco GbE3 switch being removed or installed into the adjacent slot when the SilkWorm 4012 is present.

<b>SilkWorm 48000</b>	<b>Description</b>
Fan insertion for the SilkWorm 4100	<p>If a fan is marked as faulty (amber flashing LED on fan assembly) within a few seconds after insertion, it may be a false failure indication due to a momentary disconnection caused by uneven insertion (contact bounce). Restore the fan to an operational status as follows:</p> <ol style="list-style-type: none"><li>1) Pull the fan assembly out half way.</li><li>2) Reinsert the fan at a moderate pace with a steady application of moderate force until the fan assembly is seated securely.</li></ol> <p>At this point, the fan should power up and the fan LED should indicate a functioning fan (green light). If the fan continues to indicate a fault (amber LED), then remove fan assembly and repeat procedure with a replacement fan assembly.</p>
FDMI host name support	If you have HBAs that support FDMI exposure of host names in a fabric you will need Fabric OS v3.2.0a and v4.4.0d to ensure that the host names are properly propagated to v5.0.1 switches
PID 2 support for the SilkWorm 48000	<p>The additional ports (128-258) on a SilkWorm 48000 require updates to certain Fabric OS releases in a special circumstance, that is, running PID-2 Format with a SilkWorm 48000 in the fabric.</p> <p>Minimum Fabric OS version required: 2.6.2d, 3.2.0a, 4.4.0d</p>
Power cycling	A minimum of 15 seconds between power cycles is required.
Proxy switches	If you are using a Fabric OS v4.x switch as an API or SMI-S proxy to manage a v5.0.1 switch, you will need Fabric OS v4.4.0d.
Secure Fabric OS support for the SilkWorm 48000	<p>The additional ports (128-258) on a 48000 require updates to certain Fabric OS releases in special circumstances; that is, Secure Fabric OS fabric with a SilkWorm 48000 in the fabric and port numbers higher than 127 specified in DCC policies.</p> <p>Minimum Fabric OS version required: 2.6.2d, 3.2.0a, 4.4.0d</p>

SilkWorm 48000	Description
SilkWorm 48000 hardware updates	The cable management comb, located on the lower portion of the port side of the SilkWorm 48000 director, has been updated with a slightly modified design prior to final release. The new design includes a reduced length of comb lower deck by 25mm. Replacement of the cable comb is a simple process, requiring the removal and replacement of two screws. The lower deck is now at a 4.5-degree angle. These changes are required to support improved part manufacturability.

Fabric OS Area	Description
Advanced Performance Monitor	<p>Adding Advanced Performance Monitor (<b>perfAddUserMonitor</b>) without zoning enabled at the same time will stop all frame traffic. The only frames that can go through are those that match the definitions in the <b>perfAddUserMonitor</b> command, in most cases, a very narrow definition. The result is that almost all traffic is blocked.</p> <p>Add Advanced Performance Monitor only when zoning is also enabled.</p>
Diagnostics	<p>Both backport and spinsilk tests are not supported for the Saturn platform, including any "mixed-bladed" platforms that include a Saturn blade type (FC4-16, FC4-32 or CP4).</p> <p>Instead, the user can run minicycle test. If minicycle is run from the burnin script and both lb_mode 1 and lb_mode 7 are selected, the user will get the same port frame passing coverage as spinsilk and backporttest.</p>
Nondefault operands	<b>IMPORTANT:</b> The use of nondefault operands for diagnostic commands is recommended for advanced users and technical support only.
SNMP	Starting with the FOS 4.4.0 release, Brocade added the ability to enable traps on a more granular level. After an upgrade, the <b>snmpMibCapSet</b> command should be run from the CLI to update the settings. This allows additional flexibility in controlling SNMP traps. The default setting is for all traps to be disabled.
Upgrade	Fabric OS v5.0.0 is superceded by version v5.0.1, and you are strongly encouraged to upgrade to v5.0.1.
Upgrading / downgrading	When considering an upgrade to a later Fabric OS release the user should save the zone database configuration immediately following the upgrade. Changes to the zoning database can then be conducted. If you are considering downgrading to the prior Fabric OS release, remember to clear the zoning database then restore the saved zoning database configuration prior to the downgrade.

Fabric OS Area	Description
Upgrading to Fabric OS v4.2.0 to v5.0.1	<p>The SilkWorm and FA traps in pre-Fabric OS v4.4.0 code were turned on and off as a group; and it wasn't possible to set individual SilkWorm or FA traps. In v4.4.0 the ability to turn traps on and off individually was added. That means, that individual traps need to be turned on explicitly after the corresponding trap group is turned on.</p> <p>After the upgrade from Fabric OS v4.2.0 firmware, individual traps are turned off by default even if the corresponding trap group was turned on before the upgrade. Therefore if you have been previously monitoring these traps, you need to use either <b>snmpMibCapSet</b> or the newer <b>snmpconfig</b> command to turn the desired traps on individually.</p>
FM Firmware Download	<p>For an embedded switch running Fabric OS 5.0.2 and 5.0.3 and using the small firmware file format, Fabric Manager (FM) version 5.0 supports firmware download using the external ftp server to download the firmware to the switch. In FM's options dialog, set the FTP server setting to the external option. In the firmware download dialog, select the external ftp server to download. FM does not support importing the image into the FM firmware repository.</p>
Zoning	<p>With AUDIT logging enabled, while performing zoning changes via CLI, an additional audit log from HTTP may also appear along with the audit logs from zoning. This message does not always appear, and when it does, it represents redundant reporting by the CAL layer.</p>
Loss of sync between Emulex HBA and Brocade 4Gb/sec switch	<p><b>Issue:</b> If there is a loss of sync forcing a link to be re-established, it is possible that links between Emulex HBAs and 4Gb Brocade switches may not automatically be re-established. This issue could occur after an error that has forced the switch and HBA to re-establish link initialization such as a cold switch reboot.</p> <p><b>Workaround:</b> Use the command <b>portCfgGPort</b> to configure the switch port in point-to-point only mode, also known as G port mode. To configure the HBA to point-to-point mode, please refer to Emulex HBAnyware™ documentation. To re-establish the link on the affected port without traffic disruption on other ports, issue the commands <b>portDisable</b> and <b>portEnable</b> commands on the affected port.</p>

## Documentation Updates

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

Fabric OS version 5.0.3 is supported by the Fabric OS version 5.0.1 documentation suite. The most recent Fabric OS version 5.0.1 documentation is available on Brocade Connect:

<http://www.brocadeconnect.com/>

### Fabric OS Administrator's Guide

(Publication number 53-0000518-07)

On page B-2, in the section “Supported Brocade Features,” add the following text to the bullet statement:

- Brocade translatable mode

Registers private storage target devices into the fabric, it can be used in a heterogeneous fabric if the devices are connected directly to Brocade switches. The devices will be accessible from any port on the fabric.

#### Note

Switches with a Condor ASIC do not support translatable mode.

On page 3-17, in the section “To enable or disable RADIUS service,” add the following:

#### Warning

When you issue **aaaConfig --radius on**, all sessions in which you are logged on are logged off immediately, and local authentication is disabled.

On page 4-8, in the section “Considerations for Downgrading Firmware,” add the following:

- Do not attempt to perform a firmware downgrade from v5.0.1 to v4.2.2 when you have a zone configuration larger than 128K.

On page 4-11, at the end of the section “Upgrading SilkWorm Directors,” add the following:

#### Caution

To successfully download firmware to a director you must have an active Ethernet connection on *both* CPs.

On page 5-5, in Table 5-1: SilkWorm Director Terminology and Abbreviations, remove the following rows:

Term	Abbreviation	Blade ID	Description
D1 Chassis	n/a	n/a	The first generation chassis. These chassis have a manufacture date prior to January 1, 2004. In Fabric OS 5.0.1, use the chassisShow command to view the backplane revision number for this chassis, 0x1F.
D2 Chassis	n/a	n/a	The second generation chassis. These chassis have a manufacture date from to January 1, 2004 to May 1, 2005. In Fabric OS 5.0, use the chassisShow command to view the backplane revision number for this chassis, 0x1D.
D3 Chassis	n/a	n/a	The third generation chassis. These chassis have a manufacture date from to May 1, 2005 to the present. In Fabric OS 5.0, use the chassisShow command to view the backplane revision number for this chassis, 0x1B.

On page 6-2, in the section “Specifying the Routing Policy,” add the following text to the bullet statement on port-based path selection:

- Port-based path selection

Default on SilkWorm 3016, 3250, 3850, 3900, 12000, 24000, and 48000 (using configuration option 1). These switches support the port-based policy only; you cannot change the routing policy for these switches. SilkWorm 200E, 4012, and 4100 switches can also use port-based routing. The default (and only) routing policy used in FICON environments is port-based routing.

In Chapter 7, “Administering FICON Fabrics,” add the following:

## N-Port ID Virtualization

N-Port ID Virtualization (NPIV) requires an N\_Port ID Virtualization license on the switch. The NPIV license must be installed before NPIV functionality can be enabled on any port. For Bloom-based switches and port blades supporting FICON (SilkWorm 3900, 12000 and 24000), the default behavior is that NPIV is disabled for every port. For Condor-based switches and port blades (SilkWorm 4100 and 48000), the default behavior is that NPIV is enabled for every port.

The following example shows the license required for NPIV:

```
switch:admin> licenseshow
R9cRceRSdSEdSdn:
N_Port ID Virtualization license
```

Use the **portCfgNPIV** command to enable or disable NPIV on a port-by-port basis.

The following example shows NPIV being enabled on port 10 on a SilkWorm 4100:

```
switch:admin> portCfgNPIVPort 10, 1
```

The **portCfgShow** command shows the NPIV capability of switch ports. The following example shows whether or not a port is configured for NPIV:

```
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  AN  AN
Trunk Port         ON  ON  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  ON  ON
```

The output of the commands **switchShow** and **portShow** show NPIV information for a given port. If a port is an F\_Port, and you enter the **switchShow** command, then the port WWN of the N\_Port is returned. For an NPIV F\_Port, there are multiple N\_Ports, each with a different port WWN. The **switchShow** command output indicates whether or not it is an NPIV F\_Port, and identifies the number of virtual N\_Ports behind it. Following is sample output from the **switchShow** command:

```
switch: admin> switchshow
switchName:      swd77
switchType:      32.0
switchState:     Online
switchMode:      Native
switchRole:      Principal
switchDomain:    99
switchId:        fffc63
switchWwn:       10:00:00:05:1e:35:37:40
zoning:          OFF
switchBeacon:    OFF

Area Port Media Speed State
=====
0      0      id      N2      Online      F-Port      50:05:07:64:01:20:73:b8
```

```

1  1  id  N2  Online  F-Port  50:05:07:64:01:60:73:b8
2  2  id  N2  Online  F-Port  65 NPIV public
3  3  id  N2  Online  F-Port  50:05:07:64:01:e0:73:b8
4  4  id  N2  Online  F-Port  50:05:07:64:01:20:73:b5
...

```

<output truncated>

The **portShow** command shows the NPIV attributes and lists all the N\_Port (physical and virtual) port WWNs under “*portWwn of device(s) connected.*” Use the **portLoginShow** command to display the login information for the virtual PIDs of a port. Following is sample output for **portShow** and **portLoginShow**:

```

switch:admin> portshow 2
portName: 02
portHealth: HEALTHY

```

```

Authentication: None
portDisableReason: None
portCFlags: 0x1
portFlags: 0x24b03      PRESENT ACTIVE F_PORT G_PORT NPIV LOGICAL_ONLINE LOGIN
NOELP LED ACCEPT
portType: 10.0
portState: 1      Online
portPhys: 6      In_Sync
portScn: 32      F_Port
port generation number: 148
portId: 630200
portIfId: 43020005
portWwn: 20:02:00:05:1e:35:37:40
portWwn of device(s) connected:
  c0:50:76:ff:fb:00:16:fc
  c0:50:76:ff:fb:00:16:f8
  ...

```

<output truncated>

```

...
  c0:50:76:ff:fb:00:16:80
  50:05:07:64:01:a0:73:b8
Distance: normal
portSpeed: N2Gbps

```

```

Interrupts:      0      Link_failure: 16      Frjt:      0
Unknown:         0      Loss_of_sync: 422      Fbsy:      0
Lli:            294803  Loss_of_sig: 808
Proc_rqrd:      0      Protocol_err: 0
Timed_out:      0      Invalid_word: 0
Rx_flushed:     0      Invalid_crc: 0
Tx_unavail:     0      Delim_err: 0
Free_buffer:    0      Address_err: 1458
Overrun:        0      Lr_in: 15
Suspended:      0      Lr_out: 17
Parity_err:     0      Ols_in: 16
2_parity_err:   0      Ols_out: 15
CMI_bus_err:    0

```

```

switch:admin> portloginshow 2
Type  PID      World Wide Name      credit df_sz cos
=====
fe  630240  c0:50:76:ff:fb:00:16:fc  101  2048  c  scr=3
fe  63023f  c0:50:76:ff:fb:00:16:f8  101  2048  c  scr=3
fe  63023e  c0:50:76:ff:fb:00:17:ec  101  2048  c  scr=3
...
<output truncated>
...

```

```
ff 630202 c0:50:76:ff:fb:00:17:70 192 2048 c d_id=FFFFFFC
ff 630201 c0:50:76:ff:fb:00:16:80 192 2048 c d_id=FFFFFFC
```

Also note the following behaviors relating to NPIV:

- The LIRR database is not updated when a virtual port requests a logout (LOGO). The LIRR database is updated when the base port logs out or the port goes offline.
- An NPIV port can have a maximum of 126 virtual PIDs per port.
- There is no limit on the maximum number of virtual PIDs a switch can support. The maximum number of virtual PIDs per port is the limiting factor.
- Each NPIV device is transparent to the user, and has its own device PID, Port WWN, and Node WWN, and should act the same as all other physical devices in the fabric. The same zoning rules apply to NPIV devices as non-NPIV devices. Zones can be defined by (domain, port) and/or by WWN zoning.

**Note:**

To perform zoning to the granularity of the virtual N\_Port IDs, you must use WWN-based zoning.

In Chapter 7, “Administering FICON Fabrics,” on page 7-1, in the section “FICON Overview,” replace the IBM Redbook Reference with the following:

Refer to the IBM Redbook, *FICON® Implementation Guide* (SG24-6497-00)

In Chapter 7, “Administering FICON Fabrics,” on page 7-1, in the section “FICON Overview,” add the following:

NPIV (N-port ID Virtualization) operation requires a Brocade N\_Port ID Virtualization license.

In Chapter 7, “Administering FICON Fabrics,” on page 7-2, in the section “FICON Overview,” add the following:

FICON is supported for the SilkWorm 4100 and 48000 platforms.

The FICON protocol is supported on the following SilkWorm models and Fabric OS releases:

- SilkWorm 48000, Fabric OS v5.0.1b or later. A single-domain configuration is supported with a mix of 16-port and 32-port SilkWorm 48000 port blades in a SilkWorm 48000. Dual-domain configurations are not supported on the SilkWorm 48000. Mixed port blade configurations of SilkWorm 24000 and SilkWorm 48000 port blades (FC2-16, FC4-16 or FC4-32) in the same director is not supported in a FICON environment.
- SilkWorm 4100, Fabric OS v5.0.1b or later.

Both the SilkWorm 48000 and 4100 require the port-based routing policy either in a single-switch configuration or a cascaded-switch configuration on those switches in the fabric that have FICON devices attached (option 1 of the **aptPolicy** command). Other switches in the fabric may use the default exchange-based routing policy (option 3 of the **aptPolicy** command) only when Open Systems devices are attached to those switches.

CUP is supported on the SilkWorm 4100 and 48000 running Fabric OS v5.0.1b or later.

In Chapter 7, “Administering FICON Fabrics,” on page 7-4, in the section “Configuring Switches,” add the following to the recommended FICON environment configuration settings:

The port-based routing policy is recommended for the SilkWorm 4100 and 48000 on any switch that has FICON devices attached. Other switches in the fabric with Open Systems devices exclusively can still use exchange-based routing.

Some 1-Gbit/sec storage devices cannot auto-negotiate speed with the SilkWorm 48000 or 4100 ports. For these types of devices, configure ports that are connected to 1-Gbit/sec storage devices for fixed 1-Gbit/sec speed.

In Chapter 7, “Administering FICON Fabrics,” on page 7-4, in the section “Preparing a Switch,” add the following to step 2:

- **pkiShow** to determine the existence of PKI objects, such as switch private key, private key passphrase, CSR, root certificate, and switch certificate. If none of these objects exist, refer to the *Secure Fabric OS Administrator's Guide* for information about creating the PKI objects and obtaining the digital certificate file.

In Chapter 7, “Administering FICON Fabrics,” on page 7-4, in the section “Preparing a Switch,” add a new step after step 3:

4. Change the routing policy on the switch from the default exchange-based policy to the required port-based policy for those switches with FICON devices directly attached. For the SilkWorm 4100, refer to the *Fabric OS Command Reference Manual* for details about the **aptPolicy** command. For the SilkWorm 48000, refer to Chapter 12 of the *WebTools Administrator's Guide*.

In Chapter 7, “Administering FICON Fabrics,” on page 7-9, in the section “Setup Summary,” add the following to step 2:

For SilkWorm 48000 only: Use the **portDisable** command to disable (block) port 126.

Port 126 is not supported in a CUP environment. After **fmsmode** has been successfully enabled, port 126 remains disabled. It cannot be used either as an F\_Port or an E\_Port. Because port 126 is not available after enabling **fmsmode**, you should first move any fiber connected to port 126 to another free port.

In Chapter 7, “Administering FICON Fabrics,” on page 7-19, in the section “Sample IOCP Configuration File for SilkWorm 3900, 12000, and 24000 Switches,” replace the IBM Redbook reference with the following:

For more information, refer to the IBM Redbook publication FICON® Implementation Guide (SG24-6497-00) section 2.7.1 on switch numbering.

In Chapter 7, “Administering FICON Fabrics,” on page 7-20, in the section “Sample IOCP Configuration File for SilkWorm 3900, 12000, and 24000 Switches,” add the following switches to the list:

- SilkWorm 4100
- SilkWorm 48000

On page 11-3, replace the section “Choosing an Extended ISL Mode” with the following text:

## Choosing an Extended ISL Mode

Table 11-1 lists the extended ISL modes for switches that have a Bloom ASIC. You can configure extended ISL modes with the **portCfgLongDistance** command when the Extended Fabrics license is activated.

**Table 11-1** Extended ISL Modes: Switches with Bloom ASIC

Mode	Description	Buffer Allocation		Distance @ 1 Gbit/sec	Distance @ 2 Gbit/sec	Earliest Fabric OS Release	Extended Fabrics License Required?
		1 Gbit/sec	2 Gbit/sec				
L0	Level 0 static mode, the default	5 (26) <sup>b</sup>	5 (26)	10 km	5 km	All	No
LE	Level E static mode, supports links beyond 5 km	13	19	n/a	10 km	v3.x, v4.x	No
L0.5	Level 0.5 static mode (designated LM when listed with the <b>portcfgshow</b> command)	19	34	25 km	25 km	v3.1.0, v4.1.0, v4.x, v5.x	Yes
L1	Level 1 static mode	27	54	50 km	50 km	All	Yes
L2	Level 2 static mode	60	64	100 km	60 km	All	Yes
LD <sup>a</sup>	Dynamic mode uses automatic distance detection for a user-specified distance	Auto	Auto	Auto	Auto	V3.1.0, v4.1.0, v4.4.0, v5.x (depending on the model)	Yes

a. The dynamic long-distance mode (LD) automatically configures the number of buffer credits required, based on the actual link distance.

b. For each data channel (in this case, there are 4) there are 5 credits, plus 6 extra credits.

Table 11-2 lists the extended ISL modes for switches that have a Goldeneye ASIC.

**Table 11-2** Extended ISL Modes: Switches with Goldeneye ASIC (SilkWorm 200E only)

Mode <sup>a</sup>	Buffer Allocation			Distance @ 1 Gbit/sec	Distance @ 2 Gbit/sec	Distance @ 4 Gbit/sec	Earliest Fabric OS Release	Extended Fabrics License Required?
	1 Gbit/sec	2 Gbit/sec	4 Gbit/sec					
L0	3 (17) <sup>b</sup>	3 (17)	3 (17)	6 km	3 km	1 km	All	No
LE	10	15	25	n/a	10 km	10 km	v3.x, v4.x	No

a. No LD mode appears because the distances for SilkWorm 3016 and 4012 vary depending on the number of internal and external ports.

b. For each data channel (in this case, there are 4) there are 5 credits, plus 6 extra credits.

Table 11-3 lists the extended ISL modes for switches that have a Condor ASIC.

**Table 11-3 Extended ISL Modes: Switches with Condor ASIC.**

Mode	Buffer Allocation			Distance @ 1 Gbit/ sec	Distance @ 2 Gbit/ sec	Distance @ 4 Gbit/ sec	Earliest Fabric OS Release	Extended Fabrics License Required?
	1 Gbit/ sec	2 Gbit/ sec	4 Gbit/ sec					
L0	5 (26) <sup>b</sup>	5 (26)	5 (26)	10 km	5 km	2 km	All	No
LE	11	16	26	n/a	10 km	10 km	V3.x, v4.x	No
L0.5	18	31	56	25 km	25 km	25 km	v3.1.0, v4.1.0, v4.x, v5.x	Yes
L1	31	56	106	50 km	50 km	50 km	All	Yes
L12	56	106	206	100 km	100 km	100 km	All	Yes
LD <sup>a</sup>	Auto	Auto	Auto	Auto	Auto	Auto	v3.1.0, v4.1.0, v4.4.0, v5.x (depending on the model)	Yes

a. The dynamic long-distance mode (LD) automatically configures the number of buffer credits required, based on the actual link distance.

b. For each data channel (in this case, there are 4) there are 5 credits, plus 6 extra credits.

For dynamic long distance links, you can approximate the number of buffer credits using the following formula:

$$\text{Buffer credits} = [(distance \text{ in km}) * (data \text{ rate}) * 1000] / 2112$$

The data rate is 1.0625 for 1 Gbit/sec, 2.125 for 2 Gbit/sec, and 4.25 for 4 Gbit/sec and Fibre Channel. This formula provides the minimum number of credits that will be allocated to a given port; the actual number will likely be higher.

On page 12-9, in the section “Trunking Over Extended Fabrics,” add the following section:

### Trunking Distances

Enhanced trunking support for SilkWorm 200E (which supports LE mode only) is summarized in Table 12-1.

**Table 12-1 Trunking Support for SilkWorm 200E (Goldeneye ASIC)**

Mode	Distance	Number of 2Gbit/sec ports	Number of 4 Gbit/sec ports
LE	10 km	16 (four 4-port trunks)	8 (two 4-port trunks)

Enhanced trunking support for the SilkWorm 4012 (Goldeneye ASIC) is summarized in Table 12-2.

**Table 12-2 Trunking Support for the SilkWorm 4012 (Goldeneye ASIC)**

Mode	Distance	Number of 2Gbit/sec ports	Number of 4 Gbit/sec ports
LE	10 km	4 (one 4-port trunk)	4 (one 4-port trunk)
L0.5	25 km	4 (one 4-port trunk)	3 (one 3-port trunk)
L1	50 km	3 (one 3-port trunk)	1 (one 1-port trunk)
L2	100 km	1 (one 1-port trunk)	0
LD	200 km	0	0
LD	250 km	0	0
LD	500 km	0	0

Enhanced trunking support for the SilkWorm 3900 (Bloom and Bloom2 ASICs) is summarized in Table 12-3.

**Table 12-3 Trunking Support for the SilkWorm 3900 (Bloom and Bloom2 ASICs)**

Mode	Distance	Number of 2 Gbit/sec ports
LE	10 km	4 (one 4-port trunk)
L0.5	25 km	3 (one 3-port trunk)
L1	50 km	1 (one 2-port trunk)
L2	100 km	0
LD	200 km	0
LD	250 km	0
LD	500 km	0

Enhanced trunking support for the SilkWorm 4100 (Condor ASIC) is summarized in Table 12-4.

**Table 12-4 Trunking Support for the SilkWorm 4100 (Condor ASIC)**

Mode	Distance	Number of 2Gbit/sec ports	Number of 4 Gbit/sec ports
LE	10 km	32 (four 8-port trunks)	32 (four 8-port trunks)
L0.5	25 km	32 (four 8-port trunks)	15 (one 8-port trunk)
L1	50 km	15 (one 2-port trunk)	7 (one 7-port trunk)
L2	100 km	7 (one 7-port trunk)	3 (one 3-port trunk)
LD	200 km	3 (one 3-port trunk)	0
LD	250 km	3 (one 3-port trunk)	0
LD	500 km	0	0

Enhanced trunking support for the SilkWorm 48000 is summarized in Table 12-5 and 12-6.

**Table 12-5 Trunking Support for FC4-16 port blades (SilkWorm 48000)**

Mode	Distance	Number of 2Gbit/sec ports	Number of 4 Gbit/sec ports
LE	10 km	16 (two 8-port trunks)	16 (two 8-port trunks)
L0.5	25 km	16 (two 8-port trunks)	12 (one 8-port trunk, one 4-port trunk)
L1	50 km	12 (one 8-port trunk, one 4-port trunk)	5 (one 5-port trunk)
L2	100 km	5 (one 5-port trunk)	2 (one 2-port trunk)
LD	200 km	2 (one 2-port trunk)	0
LD	250 km	2 (one 2-port trunk)	0
LD	500 km	0	0

**Table 12-6 Trunking Support for FC4-32 port blades (SilkWorm 48000)**

Mode	Distance	Number of 2Gbit/sec ports	Number of 4 Gbit/sec ports
LE	10 km	32 (four 8-port trunks)	32 (four 8-port trunks)
L0.5	25 km	32 (four 8-port trunks)	26 (two 8-port trunks, two 5-port trunks)
L1	50 km	26 (two 8-port trunks, two 5-port trunks)	12 (two 6-port trunks)
L2	100 km	12 (two 6-port trunks)	6 (two 3-port trunks)
LD	200 km	6 (one 2-port trunk)	0
LD	250 km	4 (two 2-port trunks)	0
LD	500 km	0	0

On page 13-15, at the end of the section “Creating and Maintaining Zones,” add the following text:

## Merging Zones

Before linking two switches together, it is important that you know the zone database limit of adjacent switches. For example, when switches running Fabric OS v3.2, v4.4.0, or v5.x discover that the zone merge database is larger than its pre-determined zone database size limit, they issue a reject notification before symmetrically segmenting their own ends of the ISL, thereby preventing the new switch from joining the fabric.

Symmetrical segmentation occurs when both ends of an ISL are shut down. Subsequently, no frames are exchanged between those two switches.

Asymmetrical segmentation not only prevents frames from being exchanged between switches, but also causes routing inconsistencies.

The best way to avoid either type of segmentation is to know the zone database size limit of adjacent switches. The following tables provide the expected behavior based on different database sizes after a zone merge is specified.

**Table 1** Resulting Database Size: 0 to 96K

<b>Receiver Initiator</b>	<b>FOS v2.6</b>	<b>FOS v3.1</b>	<b>FOS v3.2</b>	<b>FOS v4.0/ v4.1/v4.2</b>	<b>FOS v4.3/ v4.4.0</b>	<b>FOS v5.0.0/ v5.0.1</b>	<b>Fibre Channel Router</b>	<b>XPath v7.3</b>
FOS v2.6/v3.1	Join	Join	Join	Join	Join	Join	Join	Join
FOS v3.2	Join	Join	Join	Join	Join	Join	Join	Join
FOS v4.0/v4.1/ v4.2	Join	Join	Join	Join	Join	Join	Join	Join
FOS v4.3/v4.4.0	Join	Join	Join	Join	Join	Join	Join	Join
FOS v5.0.0/v5.0.1	Join	Join	Join	Join	Join	Join	Join	Join
Fibre Channel Router	Join	Join	Join	Join	Join	Join	Join	Join
XPath v7.3	Join	Join	Join	Join	Join	Join	Join	Join

**Table 2** Resulting Database Size: 96K to 128K

<b>Receiver Initiator</b>	<b>FOS v2.6</b>	<b>FOS v3.1</b>	<b>FOS v3.2</b>	<b>FOS v4.0/ v4.1/v4.2</b>	<b>FOS v4.3/ v4.4.0</b>	<b>FOS v5.0.0/ v5.0.1</b>	<b>Fibre Channel Router</b>	<b>XPath v7.3</b>
FOS v2.6/v3.1	Segment	Segment	Segment	Segment	Segment	Segment	Join	Segment
FOS v3.2	Segment	Segment	Join	Join	Join	Join	Join	Join
FOS v4.0/v4.1/ v4.2	Segment	Segment	Segment	Join	Join	Join	Join	Join
FOS v4.3/v4.4.0	Segment	Segment	Join	Join	Join	Join	Join	Join
FOS v5.0.0/v5.0.1	Segment	Segment	Join	Join	Join	Join	Join	Join
Fibre Channel Router	Join	Join	Join	Join	Join	Join	Join	Join
XPath v7.3	Segment	Segment	Segment	Join	Join	Join	Join	Join

**Table 3** Resulting Database Size: 128K to 256K

<b>Receiver Initiator</b>	<b>FOS v2.6</b>	<b>FOS v3.1</b>	<b>FOS v3.2</b>	<b>FOS v4.0/ v4.1/v4.2</b>	<b>FOS v4.3/ v4.4.0</b>	<b>FOS v5.0.0/ v5.0.1</b>	<b>Fibre Channel Router</b>	<b>XPath v7.3</b>
FOS v2.6/v3.1	Segment	Segment	Segment	Segment	Segment	Segment	Join	Segment
FOS v3.2	Segment	Segment	Join	Segment	Join	Join	Join	Segment
FOS v4.0/v4.1/ v4.2	Segment	Segment	Segment	Segment	Segment	Segment	Segment	Segment
FOS v4.3/v4.4.0	Segment	Segment	Join	Segment	Join	Join	Join	Segment
FOS v5.0.0/v5.0.1	Segment	Segment	Join	Segment	Join	Join	Join	Segment
Fibre Channel Router	Join	Join	Join	Segment	Join	Join	Join	Segment
XPath v7.3	Segment	Segment	Segment	Segment	Segment	Segment	Segment	Segment

**Table 4** Resulting Database Size: 256K to 1M

Receiver Initiator	FOS v2.6	FOS v3.1	FOS v3.2	FOS v4.0/ v4.1/v4.2	FOS v4.3/ v4.4.0	FOS v5.0.0/ v5.0.1	Fibre Channel Router	XPath v7.3
FOS v2.6/v3.1	Segment	Segment	Segment	Segment	Segment	Segment	Segment	Segment
FOS v3.2	Segment	Segment	Segment	Segment	Segment	Segment	Segment	Segment
FOS v4.0/v4.1/ v4.2	Segment	Segment	Segment	Segment	Segment	Segment	Segment	Segment
FOS v4.3/v4.4.0	Segment	Segment	Segment	Segment	Segment	Segment	Segment	Segment
FOS v5.0.0/v5.0.1	Segment	Segment	Segment	Asymmetrical Segment	Segment	Join	Join	Segment
Fibre Channel Router	Segment	Segment	Segment	Segment	Segment	Join	Join	Segment
XPath v7.3	Segment	Segment	Segment	Segment	Segment	Segment	Segment	Segment

## Fabric OS Command Reference Manual

(Publication number 53-0000519-10)

In Fabric OS v5.0.1b or later, the **portCfgNPiVPort** command is supported. See the online (CLI) help for command details.

In Chapter 2, “Fabric OS Commands,” remove the following commands:

- **diagEsdPorts**
- **portCfgMcastLoopback**

On page 2-21, add the following note to the **aptPolicy** “Description” section:

“Note: This command is supported only on SilkWorm 200E, 4012, 4100, and 48000 platforms.”

“Note: On the SilkWorm 4100 all three options can be changed from the Command Line interface. On SilkWorm 48000 platforms in chassis mode 5, only options 2 and 3 can be changed at the Command Line.”

On page 2-36, 2-107, and 2-108, for the **burninErrClear**, **diagSetBurnin**, and **diagSetCycle** commands, respectively, add the following note to the “Description” sections:

“It is advisable to run the **burninErrClear** command prior to running **diagSetBurnin** and **diagSetCycle**.”

On page 2-76, remove the reference to “fabric.ops.mode.vcEncode: 0” from the **configShow** output in the “Example” section.

On page 2-85, remove the HTTP and RPCd content from Table 2-7 for the **configure** command.

On page 2-102, add the following note to the **diagHelp** “Description” section:

“Use default operands when running diagnostics commands. Nondefault settings require detailed knowledge of the underlying hardware and are intended for support personnel only. Contact support if you want to use these operands.”

On page 2-176, in the **firmwareDownloadStatus** “Example” section, change the two instances of “It may take up to 10 minutes.” to “This step will take up to 30 minutes.”

On page 2-224, in the **ifModeShow** “Example” section, replace the existing output with the following:

```
switch:admin> ifmodeshow eth0
Link mode: negotiated 100baseTx-HD, link ok
MAC Address: 00:60:69:D0:24:40
```

On page 2-496, add the following note to the **slTest** “Description” section:

“NOTE: This command is supported only on SilkWorm 200E, 4012, 4100, 4900, and 48000 platforms”

On page 2-544, in the **switchName** “Operands” section, add the hyphen character to the list of supported characters for switch names.

On page 2-318, 2-324, and 2-327, change the availability for **perfMonitorShow**, **perfShowEEMonitor**, and **perfShowFilterMonitor** from all “all users” to “admin”.

On page 2-345, replace the **portCfgLongDistance** “Description” section with the following:

“Use this command to allocate enough full-size frame buffers on a particular port to support a long-distance link up to 500 km. The port can be used as an F/FL/E\_Port. F/FL\_Ports can be configured only for long distance using LE, L0.5, L1, or L2 modes. Changes made by this command are persistent across switch reboots or power cycles.

The value of *distance\_level* can be one of the following (the numerical value representing each *distance\_level* is shown in parentheses):

- L0** (0) Reconfigure the port to be a regular switch port. A total of 26 full-size frame buffers are reserved for data traffic, regardless of the port’s operating speed.
- L0.5** Level 0.5 (**portCfgShow** displays the two-letter code as LM) long distance, up to 25 km.
- L1** (1) Level 1 long distance, up to 50 km.
- L2** (2) Level 2 long distance, up to 100 km. For previously released switches (Bloom1-based), the number of frames buffers is limited to 63.
- LE** (3) Level E mode is for E\_Ports for distances beyond 5 km and up to 10 km. LE does not require an Extended Fabrics license.
- LD** Automatic long-distance configuration. The buffer credits for the given E\_Port are automatically configured, based on the actual link distance. Up to a total of 250 full-size frame buffers are reserved, depending upon the distance measured during E\_Port initialization. If the desired distance is provided, it is used as the upper limit to the measured distance. For Bloom1-based systems, the number of frame buffers is limited to 63.

A long-distance link also can be configured to be part of a trunk group (refer to **portCfgTrunkPort**). Two or more long-distance links in a port group forms a trunk group when they are configured for the same speed, the same distance level, and their link distances are nearly equal.

**Note:** For details about buffer allocation at specific speeds and distances, refer to the “Administering Extended Fabrics” chapter of the *Fabric OS Administrator’s Guide*.

The *vc\_translation\_link\_init* option is used to enable the long-distance link initialization sequence.

*desired\_distance* is a required parameter to configure a port as an LD-mode link. The desired distance is used as the upper limit of the link distance to calculate buffer availability for other ports in the same port group. When the measured distance is more than *desired\_distance*, the *desired\_distance* is used to allocate the buffers. In this case, the port operates in degraded mode instead being disabled due to insufficient buffers.

Pressing **Ctrl-D** cancels the configuration update.

When a port is configured to be a long-distance port, the output of **portShow** and **switchShow** displays the long-distance level. In the **portShow** output, the long-distance level is indicated as follows:

- L0      normal
- LE      standard <= 10 km
- LM      medium long <= 25 km
- L1      long <= 50 km
- L2      super long <= 100 km
- LD      auto

In the **switchShow** output, the long distance mode displays as Lx, where x is the second letter in two-letter distance-level code described earlier; however, L0.5 mode displays LM.

**Note:** The **portCfgISLMode** and **portCfgLongDistance** mode cannot both be enabled at the same time; otherwise, fabric segmentation occurs.

If a port is configured as a long distance port, the remaining ports of that port group could be disabled, fail to initialize, or move to “buffer limited” mode due to a lack of frame buffers. SilkWorm 3014, 3016, 3250, 3850, and 3900 switches and 12000 and 24000 directors do not support “buffer limited” mode and can have up to four ports per port group. SilkWorm 200E, 4100, and 4012 switches support “buffer limited” mode and can have up to eight ports per port group. On SilkWorm 48000 directors, the FC4-16 and FC4-32 port blades support “buffer limited” mode and can have up to four ports per port group.”

On page 2-409 and 2-541, change the availability for **portSwapShow** and **supportShowCfgShow** from “admin” to “all users”.

On page 2-496, add the following note to the “Description” section:

**Note:** This command is supported only on SilkWorm 200E, 4012, 4100, 4900, and 48000 platforms.”

In Chapter 5, “MUA-Based Roles,” add the following to table 5-1:

Command	Description
<b>burninLevel</b>	Sets the diagnostics burn-in level.
<b>burninStatus</b>	Displays the diagnostics burn-in level.
<b>configDownload</b>	Downloads a switch configuration file from a host file, omitting zoning and security configurations.
<b>errModuleShow</b>	Displays all the defined error log modules.
<b>fabricLog</b>	Displays or manipulates the fabric log.
<b>fabStateResize</b>	Changes the number of state entries.
<b>historyMode</b>	Displays the mode of the history log.
<b>minisPropShow</b>	Displays ASIC pair properties.
<b>portCfg</b>	Sets a port’s configuration to be disabled or enabled.
<b>setEsdMode</b>	Enables or disables ESD mode.
<b>setGbicMode</b>	Enables or disables media mode.
<b>setMediaMode</b>	Enables or disables media mode.
<b>setModem</b>	Enables or disables modem dial-in to a control processor (CP).
<b>setSfpMode</b>	Enables or disables media mode.

<b>supportShowCfgDisable</b>	Disables a group of commands under the <b>supportShow</b> command.
<b>supportShowCfgEnable</b>	Enables a group of commands under the <b>supportShow</b> command.
<b>supportShowCfgShow</b>	Displays the groups of commands enabled for display by the <b>supportShow</b> command.
<b>traceDump</b>	Displays, initiates, or removes a trace dump.
<b>traceFtp</b>	Displays, enables, or disables the trace auto-FTP or FTPs a trace dump file to the customer FTP server.
<b>traceTrig</b>	Sets, removes, or displays trace triggers.
<b>voltShow</b>	Displays current level of the voltage sensors on a system.

In table 5-1, remove the following commands:

- backplaneTest
- backport
- bladeBeacon
- bladeDisable
- bladeEnable
- camTest
- centralMemoryTest
- crossPortTest
- fanDisable
- fanEnable
- ficonHelp
- filterTest
- haDisable
- haDump
- haEnable
- haFailover
- haShow
- haSyncStart
- haSyncStop
- itemList
- loopPortTest
- miniCycle
- powerOffListSet
- powerOffListShow
- spinFab
- spinJitter
- spinSilk
- statsClear
- statsTest
- switchReboot
- switchShutdown
- switchStart

- turboRamTest
- txdPath
- userRename

The following table lists platform support for legacy and new diagnostic commands.

Diagnostic Command	Supported SilkWorm Platforms
<b>backplaneTest</b>	3014, 3016, 3250, 3850, 3900, 12000, 24000
<b>camTest</b>	3014, 3016, 3250, 3850, 3900, 12000, 24000
<b>centralMemoryTest</b>	3014, 3016, 3250, 3850, 3900, 12000, 24000

Add the following paragraph to the **switchShow** on page 2-551:

**Note:**

For all Bloom or Bloom2 based switches with Fabric OS v5.0.1 firmware, private device targets are displayed in **switchShow**. For Condor or Goldeneye based switches, private device targets are not displayed in **switchShow**."

## Fabric OS MIB Reference Manual

(Publication number 53\_0000521\_09)

Add the following section at the end of Chapter 1.

### Firmware Upgrades and Enabled Traps

Prior to Fabric OS v4.4, traps were turned on and off as a group (for example, the SW-Trap, or FA-Trap). In these versions of the Fabric OS it was not possible to set individual traps (such as, swSensorStatusChangeTrap, swTrackChangesTrap, or connUnitEventTrap).

In Fabric OS v4.4 or above you can to turn on and off traps individually within a trap group. The individual traps need to be enabled explicitly after the corresponding trap group is enabled.

Because the pre- Fabric OS v4.4 firmware only has trap group level settings, when you upgrade to the Fabric OS v4.4 firmware or above, individual traps are turned off by default even if the corresponding trap group was enabled before upgrading. When moving from a downlevel version to Fabric OS v4.4 or above you must use either **snmpmibcapset** or **snmpconfig** command to turn on explicitly the individual traps within each trap group.

Add the following note to page 1-1 under System Message Log (RASlog) section:

**Note:**

When the fabric is formatted in PID format 2, the error messages do not reflect the change. Port numbers in all error messages reflect the PID mode 1 port-numbering scheme.

Add the following note to page 1-1 under System Message Log (RASlog) section:

**Note:**

When the fabric is formatted in PID format 2, the error messages do not reflect the change. Port numbers in all error messages reflect the PID mode 1 port-numbering scheme.

On Page 1-7, Heading "Before Loading Mibs" replace the v4.2.0, v4.4.0, and v5.0.1 entries Table 1-1 with the following:

Fabric OS v4.2.0 and previous	Yes	No 2	No
Fabric OS v4.4.0	Yes	No 2	Yes 3
Fabric OS v5.0.1	Yes	No 2	Yes 3

**Note:**

1. The corresponding Fabric OS has SNMPv2 capabilities, but it is not officially supported by Brocade.
2. The Structure of Management Information version 2 (SMIv2) framework is used in defining the MIBs.
3. Fabric OS v4.4.0 and v5.0.1 support SNMPv3-USM (snmpUsmMIB) MIB, which is available as RFC 3414.

Add the following descriptions on page 3-6 in Table 3-2:

Display string	Represents textual information taken from the NVT ASCII character set, as defined in pages 4, 10-11 of RFC 854.
Milliseconds	Represents time unit value in milliseconds.
Microseconds	Represents time unit value in microseconds.

Add the following descriptions on page 3-32 in Table 3-3:

Display string	Represents textual information taken from the NVT ASCII character set, as defined in pages 4, 10-11 of RFC 854.
Milliseconds	Represents time unit value in milliseconds.
Microseconds	Represents time unit value in microseconds.
FcphVersion	Represents the version of FC-PH supported by an NxPort or FxPort.

Add the following descriptions on page 3-34 in Table 3-3:

FcFeModuleCapacity	Represents the maximum number of modules within a Fabric Element.
FcFeFxPortCapacity	Represents the maximum number of FxPorts within a module.
FcFeModuleIndex	Represents the module index within a conceptual table.
FcFeFxPortIndex	Represents the FxPort index within a conceptual table.
FcFeNxPortIndex	Represents the NxPort index within a conceptual table.

Add the following note on Page 5-13 to the end of the "SW Traps" section:

NOTE: The swGroupName, swGroupType, and swGroupMemPos variables are optional trap variables in Fabric OS v2.6.x. These variables are not supported in Fabric OS v4.x and above.

On Page 5-6 in the "swFabricWatchTrap" section the following variable is missing from the swFabricWatchTrap list of variables:

"swFwLastSeverityLevel 1.3.6.1.4.1.1588.2.1.1.1.10.3.1.12"

On page Page 8-51 in the "Unsupported Traps" section these traps are supported and the heading should read "FibreAlliance MIB Traps". Only the connUnitDeletedTrap is not supported by Brocade.

Add the following descriptions on page 8-8 in Table 8-1:

FcNameId	The Port Name for this entry in the SNS table.
FcGlobalId	An optional global-scope identifier for this connectivity unit. It MUST be a WWN for this connectivity unit or 16 octets of value zero.
FcAddressId	The Port Identifier for this entry in the SNS table.

# Fabric OS System Error Message Reference Manual

(Publication number 53-0000515-10)

On Page 3-1 the BL-1000 message states, “This message occurs on only the SilkWorm 12000.” However the message may also occur on a Silkworm 3250, 3850, or 3900 switch.

On Page 3-2 the BL--1003 message states, “This message occurs on only the SilkWorm 12000, 24000, and 48000.” However the message may also occur on a Silkworm 3250, 3850, or 3900 switch.

The following messages were added after the document publication.

## CDR-1001

### Message

```
<timestamp>, [CDR-1001], <sequence-number>,, WARNING, <system-name>, Port <port number> port fault. Please change the SFP or check cable
```

### Probable Cause

Indicates a deteriorated SFP, an incompatible SFP pair, or a faulty cable between peer ports.

### Recommended Action

Verify that the SFPs have not deteriorated and that the Fibre Channel cable is not faulty. Replace the SFPs or cable if necessary.

### Severity

WARNING

## CONF-1000

### Message

```
<timestamp>, [CONF-1000], <sequence-number>,, WARNING, <system-name>, configDownload completed successfully but Zoning and Security parts were ignored
```

### Probable Cause

Indicates that the user with switchadmin role does not have permission to update Zoning and Security configurations, so Zoning and Security configurations are skipped while downloading the configuration file

### Recommended Action

No action is required. Run the **configShow** command to view the configuration.

### Severity

WARNING

## FICU-1010

### Message

```
<timestamp>, [FICU-1010], <sequence-number>,, WARNING, <system-name>, FMS Mode enable failed due to address conflict with port <port number>.
```

### Probable Cause

Indicates that the FICON Management Server mode (fmsmode) was not enabled because the specified port has an address conflict with the CUP management port.

### Recommended Action

Use the **portDisable** command to disable the specified port causing the port address conflict.

### Severity

WARNING

## HAMK-1004

### Message

```
<timestamp>, [HAMK-1004], <sequence-number>,, INFO, <system-name>, Resetting  
standby CP (double reset may occur).
```

### Probable Cause

Indicates that the standby CP is being reset due to a loss of heartbeat. This message is typically seen when the standby CP has been rebooted. Note that in certain circumstances a CP may experience a double reset and reboot twice in a row. A CP can recover automatically even if it has rebooted twice.

### Recommended Action

No action is required.

### Severity

INFO

## PLAT-1001

### Message

```
<timestamp>, [PLAT-1001], <sequence-number>,, INFO, <system-name>, Resetting  
standby CP (double reset may occur).
```

### Probable Cause

Indicates that the standby CP is being reset. This message is typically generated by a CP that is in the process of becoming the active CP. Note that in certain circumstances a CP may experience a double reset and reboot twice in a row. A CP can recover automatically even if it has rebooted twice.

### Recommended Action

No action is required.

### Severity

INFO



## Fabric Watch User's Guide

(Publication number 53-0000524-06)

The following row replaces the existing rows “Invalid CRC Count,” “Link Failure Count,” and “State Changes” in Table A-6, “Port Class Threshold Defaults,” on page A-6:

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Link Failure Count	Monitors the number of link failures	Unit: Error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range

### Alarm behavior of CF monitor

Fabric watch alarm behavior depends on the state of Above, Below and In-between thresholds configured for a specific monitor. In case of CF monitor, the monitor state configurations are as shown below:

- Below threshold monitor state is STATE\_IN\_RANGE
- In-Between threshold monitor state is STATE\_INFO
- Above threshold monitor state is STATE\_OUT\_OF\_RANGE

Alarms are only generated when a monitor state changes from good to bad or from bad to good. In case of CF monitor, the alarm behavior is described below:

1. If the state changes from Below (STATE\_IN\_RANGE – good state) to In-between (STATE\_INFO – good state), no alarm will be generated. If the CF usage is within a reasonable range, there is no need to raise an alarm.
2. An alarm is generated when CF monitor state goes from In-between (STATE\_INFO – good state) to Above (STATE\_OUT\_OF\_RANGE – bad state). This is to inform you that the CF usage is above the high boundary.
3. An alarm is generated when CF monitor state changes from Above to In-between. This informs the user that CF usage has returned to normal.

## Secure Fabric OS Administrator's Guide

(Publication number 53-0000526-05)

On page 2-24, in the second example box, replace the following information:

“Address-file: -a

Path/file-name of optional input file containing IP addresses or aliases of fabrics to which sessions should be established. If this argument is not provided, this data is read from the file indicated by environment variable ‘FABRIC\_CONFIG\_FILE’.”

With this information:

“Address-file: -a addr-file

“addr-file” is the path/file-name of optional input file containing IP addresses or aliases of fabrics to which sessions should be established. If this argument is not provided, this data is read from the file indicated by environment variable ‘FABRIC\_CONFIG\_FILE’ if defined. Use Microsoft Notepad to create the addr-file.”

# SilkWorm 200E Hardware Reference Manual

(Publication number 53-0000633-01)

On page v, in the “How This Document Is Organized” section, a glossary is listed; however there is no glossary in this manual.

On page 2-7, "Configuring the SilkWorm 200E

On page 1-4 under the heading “Supported Fabric Configurations” the text should read:

The SilkWorm 200E is supported as an edge device in fabrics of up to 53 domains.

The order of tasks is incorrect, that is, the steps are the same but you must perform them in a slightly different order.

To configure the SilkWorm 200E, you must first:

1. Power on the switch.
2. Establish a physical serial connection to the switch.
3. Log in to the switch as the admin user using a hyperterminal application.  
Step number 1 in the document details how to set up the hyperterminal connection.

On page 2-6, Table 2-3, replace the BTU Rating and Input Electrical Power value:

Delete the following: 266 BTU

Replace with the following: “38 W/ 130 BTU”

On page 2-6, Table 2-3, above the row title "Input Voltage" add a row "Input Electrical Power":

Input Electrical Power / 45VA

On page 2-6, Table 2-3, replace the BTU Rating and Input Electrical Power value:

Delete the following text: 266 BTU

Replace with the following text: 38 W/ 130 BTU

On page 2-8, “Set the IP Address,” the note should read as follows:

Note: Any time the Ethernet or serial connection is not in use, the safety plug should be installed to protect it from dust or other foreign material.

On page 2-9, “Modify the Domain ID (Optional)” section a) delete the last sentence in the second paragraph and b) replace the fourth paragraph with the following :

The domain ID is a number assigned to the switch by the Fabric OS and is used when routing frames to the switch. If you do not set the Domain ID for the switch and it is attached to a fabric, the Principal switch of the fabric will assign it a new domain ID. If you set the domain ID for the switch, using the **configure** command, then this number must be unique to the fabric the switch is connecting to, or the switch will segment.

On page 4-1, “Management Features of the SilkWorm 200E,” add the following note before the table:

Note: Some of the management tools listed below are available only with the appropriate license key installed.

## SilkWorm 3250/3850 Hardware Reference Manual

(Publication number 53-0000623-02)

On page 2-3, replace the “Note” text:

“The 0° - 40° Celsius range applies to the ambient air temperature at the air intake vents on the nonport side of the switch. The temperature inside the switch can be up to 75° Celsius during switch operation.

If the internal temperature range exceeds the operating ranges of the components, the LEDs, error messages, and Fabric Watch alerts will indicate a problem. Enter the **tempShow** or Fabric Watch commands to view temperature status.”

With this text:

“The 0° - 40° Celsius range applies to the ambient air temperature at the air intake vents on the nonport side of the switch. The temperature inside the switch can be up to 65° Celsius during switch operation.

If the internal temperature range exceeds the operating ranges of the components, the LEDs, error messages, and Fabric Watch alerts will indicate a problem. Enter the **tempShow** or Fabric Watch commands to view temperature status.

If the internal temperature range exceeds the safe range, the SilkWorm 3250/3850 reboots. To remove power from the SilkWorm 3250/3850, refer to "Powering the SilkWorm 3250/3850 On and Off" on page 3-1.”

## SilkWorm 4020 Hardware Reference Manual

(Publication number 53-000688-01)

Add the following text at the end of the first paragraph under the heading “Interpreting SilkWorm 4020 LEDs” on page 4-2:

Note: The blinking rate for RX/TX LED and the internal LED is slower than the physical switch when I/O activity is present.

## SilkWorm 4100 Hardware Reference Manual

(Publication number 53-0000563-01)

On page 1-1, under the heading “Ports on Demand”, replace this text:

“The SilkWorm 4100 has 32 ports. By default, ports 0-15 are enabled. To enable additional ports, you must install Ports On Demand (POD) licenses. To enable ports 16 through 23, you must install the POD1 license. To enable ports 24 through 31, you must install the POD2 license. Although you can install the POD2 license without having the POD1 license installed, you cannot use ports 16 through 23 until the POD1 license is enabled. For detailed information on enabling additional ports using the Ports on Demand license, refer to the *Fabric OS Administrator's Guide*.”

With this text:

“The SilkWorm 4100 model can be purchased with 16, 24, or 32 licensed ports. As your needs increase, you can activate unlicensed ports (up to the maximum of 32 ports) by purchasing and installing the Brocade Ports on Demand optional licensed product.

By default, ports 0 through 15 are activated on the SilkWorm 4100. Each Ports on Demand license activates the next group of eight ports, in numerical order. Before installing a license key, you must insert transceivers in the ports to be activated. Remember to insert the transceivers in the lowest group of inactive port numbers first. For example, if only 16 ports are currently active and you are installing one Ports on Demand license key, make sure to insert the transceivers in ports 16 through 23. If you later install a second license key, insert the transceivers in ports 24 through 31.

After you install a license key, you must enable the ports to complete their activation. You can do so without disrupting switch operation by using the **portEnable** command on each port. Alternatively, you can disable and reenabling the switch to activate ports.

For more information on activating ports on demand, refer to the *Fabric OS Administrator's Guide*."

On page A-6, under the heading "Fibre Channel Port Specifications" (on page A-6), replace this text:

"The ports are capable of operating at 1, 2, or 4 Gbit/sec and are able to autonegotiate to the higher of 1 or 2 Gbit/sec. Operation at 4 Gbit/sec must be manually set"

With this text:

"The ports are capable of operating at 1, 2, or 4 Gbit/sec and are able to autonegotiate to the higher of 1, 2, or 4 Gbit/sec."

## SilkWorm 12000 Hardware Reference Manual

(Publication number 53-0000148-05)

The following statement within the "Operating Information for Power Supplies" section on page 2-12 is incorrect:

The left power connector provides power to the power supplies in power supply bays #1 and #3 (color-coded blue), which provide power to the left side of the chassis (slots 1-5). The right power connector provides power to the power supplies in power supply bays #2 and #4 (color-coded yellow), which provides power to the right side of the chassis (slots 6-10).

As long as one power supply is operating, all the card slots (1-10) have power. The statement should read:

Power to the backplane is load sharing and redundant across all power supplies. The left and right power feeds control INPUT power to power supplies 1 and 3, and 2 and 4 respectively. Because 2 power supplies are required to support a fully populated 12000, we recommend filling all 4 power supply slots to ensure that in the case of a power feed failure, the chassis will have enough power for both switches.

On page 2-2, under the heading, "Powering the SilkWorm 12000 On and Off," replace the following information:

To power the SilkWorm 12000 off:

Flip both AC power switches to "0". To remove all sources of power from the switch, disconnect both cables from the power source.

**Note:** Removing all power from the switch triggers a system reset. When power is restored, all devices are returned to the initial state and the switch runs POST.

With this information:

To power the SilkWorm 12000 off:

1. Shut down both logical switches (see Figure 2-1):
  - a. Enter the **switchShutdown** command to ensure a graceful shutdown of Switch 1, and verify the command has completed and displayed the message "Cleaning up kernel modules.....Done".
  - b. From the active CP card session, log into Switch 0 by entering the login command, logging in as admin, then entering "0" to log into Switch 0.
  - c. Enter the **switchShutdown** command to ensure a graceful shutdown of Switch 0, and verify the command has completed and displayed the message "Cleaning up kernel modules.....Done".

**Figure 2-1** Sample Output for the **switchShutdown** Command on Both Switches

```
SW1:admin> switchshutdown
Stopping all switch daemons...Done.
Powering off slot 7...Done.
Powering off slot 10...Done.
Checking all slots are powered off...Done.
Cleaning up kernel modules.....Done
SW1:admin>
```

```

SW1:admin> login
login: admin
Enter Switch Number to Login <0 or 1>: 0
password: xxxx
SW0:admin>
SW0:admin> switchshutdown
Stopping all switch daemons...Done.
Powering off slot 1...Done.
Powering off slot 4...Done.
Checking all slots are powered off...Done.
Cleaning up kernel modules....Done
SW0:admin>

```

For details on the **switchShutdown** command, refer to the Fabric OS Command Reference Manual, or the online help.

2. Power off the chassis by flipping both AC power switches to “0” (LEDs inside AC power switches should turn off). See Figure 1-1 on page 1-2 for location of switches. To maintain the ground connection, leave both power cords connected to the chassis and to an electrical outlet.

## SilkWorm 24000 Hardware Reference Manual

(Publication number 53-0000619-01)

On page A-2, table A-1, "System Architecture," replace the following table entry:

"Switch latency <2.1 µsec any port to any port at 2 Gb/sec, cut-through routing"

With this table entry:

"Switch latency 2.05 < 2.35 µsec any port to any port at 2 Gbit/sec, cut-through routing"

Step 1 of the “Replacing a Power Supply and Filler Panel” on page 5-21 is incorrect.

Determine whether power adequate to keep the chassis operating will be available throughout the replacement. If adequate power will *not* be consistently available, shut down the SilkWorm 24000 gracefully, as follows:

- a. Open a telnet session to the active CP card and log in to the switch as admin.
- b. Enter the **switchshutdown** command.
- c. Power off the chassis by flipping both AC power switches to the off position (the “0” on the AC switch).

Replace Step 1 with this information:

Determine whether power adequate to keep the chassis operating will be available throughout the replacement. If adequate power will *not* be consistently available, shut down the SilkWorm 24000 gracefully, as follows:

- a. Open a telnet session to the active CP card and log in to the switch as root.
- b. Enter the following command:  
`/usr/bin/shutdown -h now`
- c. Watch the console log for the following power down message. The director will automatically reboot, so hit the ESC key to stop at the bootprom. This will stop the standby CP from rebooting.

```

The system is going down for system halt NOW !!
INIT: Switching to runlevel: 0
INIT: Sending processes the TERM signal
2005/08/17-18:10:01, [FSSM-1003], 19,, WARNING, Silkworm12000, HA State out
of sync
Unmounting all filesystems.

```

```
The system is halted
flushing ide devices: hda
Power down.
```

```
The system is coming up, please wait...
Checking system RAM - press any key to stop test
00b00000
System RAM check terminated by keyboard
System RAM check complete
Press escape within 4 seconds to enter boot interface.
```

- 1) Start system.
- 2) Recover password.
- 3) Enter command shell.

d. Login to the active CP and repeat steps b and c for the active CP. Once both CPs are stopped at the boot prom, you can power off the system safely.

e. Power off the chassis by flipping both AC power switches to “0” (LEDs inside AC power switches should turn off). See Figure 1-1 on page 1-2 for location of switches. To maintain the ground connection, leave both power cords connected to the chassis and to an electrical outlet.

On Page 5-21 under the heading "Replacing the Power Supply and Filler Panel" replace Step 1 with the following:

1. Determine whether power adequate to keep the chassis operating will be available throughout the replacement. If adequate power will *not* be consistently available, shut down the SilkWorm 24000 gracefully as follows:

- a. From the active CP card, log into Switch 1 by entering the login command, logging in as admin, then entering “1”.
- b. Enter the **switchShutdown** command to ensure a graceful shutdown of Switch 1, and verify the command has completed and displayed the message “Cleaning up kernel modules.....Done”.
- c. From the active CP card, log into Switch 0 by entering the login command, logging in as admin, then entering “0”.
- d. Enter the **switchShutdown** command to ensure a graceful shutdown of Switch 0, and verify the command has completed and displayed the message “Cleaning up kernel modules.....Done”.
- e. Power off the chassis by flipping both AC power switches to the off position (the “0” on the AC switch).

On page 3-2, under the heading "Configure IP Addresses for CP Cards," remove the first sentence in the following note:

"Note: Use a block of three IP addresses that are consecutively numbered in the last octet. The IP and gateway addresses must reside on the same subnet."

Table 4-7 on page 4-15 within the “WWN Card” section in Chapter 4 needs to be revised. Replace Table 4-7 with the following:

**Table 4-7 WWN Bezel LED Patterns**

LED Location/Purpose	Color	Status	Recommend Action
16-Port card/CP card Power	Steady green	Power is OK.	No action required.
	Flashing green	Power to port card is OK; however, this LED flashes if the port card status LED is flashing.	Check port card status LED and determine if it is flashing slow (2 second increments) or fast (1/2 second increments) and then take appropriate action.
	No light (LED is OFF)	No port card present or power source is unavailable.	Insert port card, or check AC switch or power source.
	NOTE: Check the individual port card (see Figure 4-1 on page 4-2) or CP card power LEDs (see Figure 4-2 on page 4-6) on the port side of the chassis to confirm the LED patterns.		
16-Port card/CP card Status	Steady amber	Port card is faulty.	Check port card.
	Slow-flashing amber (on 2 seconds; then off 2 seconds)	Port card is not seated correctly or is faulty.	Pull card out and reseal it. If LED continues to flash, replace card.
	Fast-flashing amber (on 1/2 second; then off 1/2 second)	Environmental range exceeded or port card failed diagnostics (run during POST or manually).	Check for out-of-bounds environmental range and correct it. Replace card if it fails diagnostics.
	No light (LED is OFF)	Port card is either healthy or does not have power.	Verify that the port card power LED is on.
	NOTE: Check the individual port card (see Figure 4-1 on page 4-2) or CP card status LEDs (see Figure 4-2 on page 4-6) on the port side of the chassis to confirm the LED patterns.		
Power supply/ Power/Status	Steady green	Power is OK.	No action required.
	Steady amber	Power supply is faulty.	Ensure that the correct AC power switch is on and the power supply is seated. If LED remains on, replace the power supply.
	Slow-flashing amber	FRU header (SEEPROM cannot be read) due to I2C problem.	Replace power supply.
	Fast-flashing amber	Power supply is about to fail due to failing fan inside the power supply.	Replace power supply.

	No light (LED is OFF)	No power supply present or is not inserted/seated properly, or power source is unavailable.	Insert power supply module, ensure it is seated properly, or check AC switch or power source.
	NOTE: Check the individual power supply LEDs on the port side of the chassis to confirm the LED patterns (see Figure 4-3 on page 4-9).		

**NOTE:** If a port card slot or power supply bay has a filler panel installed, the corresponding LEDs on the WWN card do not light up.

On page 5-20 , “Replacing a Power Supply and Filler Panel, add the following paragraph:

“A SilkWorm 24000 that is fully populated with FC2-16 blades can function on one power supply. Redundancy of the power supply is achieved using power supply FRUs in slots 1 and 2. You can populate all 4 power supply slots in the SilkWorm 24000 for maximum redundancy. Power supply FRUs are interchangeable between SilkWorm 12000 and SilkWorm 24000.”

## **SilkWorm 48000 Hardware Reference Manual** (Publication number 53-0000645-01)

On page A-8, Table A-6, replace the Heat dissipation values as follows.

Delete the following:

913 Watts or 3115 BTU (Eight  
FC4-32 blades and two CP4 blades)  
711 Watts or 2426 BTU (Eight  
FC4-16 blades and two CP4 blades)

Replace with the following:

720 Watts or 2457 BTU (Eight  
FC4-32 blades and two CP4 blades)

## **SilkWorm Director Blade Support Notes** (Publication number 53-0000761-01)

On page 11, in the section “Adding FC2-16 Blades to a SilkWorm 48000,” replace the second paragraph:

If you are using **chassisConfig** mode 1 you can add **FC2-16 cards** with minimal disruption. If you are using **chassisConfig** mode 5, you **MUST** change to mode 1 prior to executing this procedure. Changing the **chassisConfig** mode requires a reboot and is disruptive.

## **Web Tools Administrator’s Guide** (Publication number 53-0000522-08)

On page 3-7, in the section “Refresh Rates,” add the following paragraph after the first paragraph:

The refresh, or polling, rates listed in this section and throughout the book indicate the time between the end of one polling and the start of the next, and *not* how often the screen is refreshed. That is, a refresh rate of 15 seconds does not mean that a refresh occurs every 15 seconds. It means that a new refresh starts 15 seconds after the previous refresh finished.

On page 3-7, in the section “Fabric Tree,” delete the fourth paragraph:

The Fabric Tree is updated at time intervals depending on the number of switches in the fabric. On average, for a fabric with up to 12 switches, the Fabric Tree is updated every 30 seconds. For every additional 12 switches in the fabric, it takes an additional 30 seconds to update the Fabric Tree. The Switch Information View displays a field, “Polled At”, that identifies the last time the information was updated.

On page 3-7, in the section “Fabric Tree,” replace the last paragraph:

You can also manually refresh the status of a switch within the fabric by right-clicking that switch in the Fabric Tree and clicking **Refresh**.

With this paragraph:

You can manually refresh the status of a switch within the fabric by right-clicking that switch in the Fabric Tree and clicking **Refresh**.

On page 4-27, in the section “Displaying the Name Server Entries,” replace the following text in the Note:

You must click **Refresh** from the Name Server window to poll Name Server entries.

You can also specify a time interval at which the Name Server entries will be automatically refreshed.

With this text:

Click **Refresh** in the Name Server window to poll Name Server entries.

You can also click the Auto Refresh checkbox and specify a time interval at which the Name Server entries will be automatically refreshed.

On page 4-27, in the section “To view a list of the switches in the Name Server,” replace the following steps:

2. *Optional:* Check the **Auto Refresh** checkbox on the Name Server window.
3. *Optional:* Enter an autorefresh interval (in seconds), at a minimum of 15 seconds. The Name Server entries will refresh at the rate you set.

With this step:

2. *Optional:* Check the **Auto Refresh** checkbox on the Name Server window. Type an auto-refresh interval (in seconds); the minimum (and default) interval is 15 seconds. The Name Server entries will refresh at the rate you set.

In Chapter 12, “Administering FICON CUP Fabrics,” on page 12-1, in the section “This chapter contains” add the following bullet:

- “Enabling Port Based Routing on the SilkWorm 4100 and SilkWorm 48000,” next

In Chapter 12, “Administering FICON CUP Fabrics,” on page 12-1, add a new section “Enabling Port Based Routing”

- Enabling Port Based Routing on the SilkWorm 4100 and SilkWorm 48000

Port-based path selection is a routing policy in which paths are chosen based on ingress port and destination only. This also includes user-configured paths. All SilkWorm 4100 and 48000 switches with FICON devices attached must have port-based routing policy enabled. Port-based routing is a per-switch routing policy. After port-based routing is enabled, you can continue with the rest of the FICON implementation.

#### **To enable or disable port-based routing**

1. Click a switch with FICON devices attached from the Fabric Tree.
2. Launch the Switch Admin module as described on page 4-3.
3. Click the FICON CUP tab.

The FICON CUP tab displays, with the FICON Management Server subtab in front, as shown in Figure 12-1.

4. Click the **Enable** radio button to enable the port-based routing policy.

**Figure 12-1** FICON CUP Management, Port Based Routing.

On page 14-1, in the section “Monitoring Performance Using Web Tools,” replace the following paragraph:

Each graph is displayed individually in a window, so it can be minimized, maximized, resized, and closed. Graphs within the Performance Monitor module are updated every 30 seconds.

With these paragraphs:

Each graph is displayed individually in a window, so it can be minimized, maximized, resized, and closed.

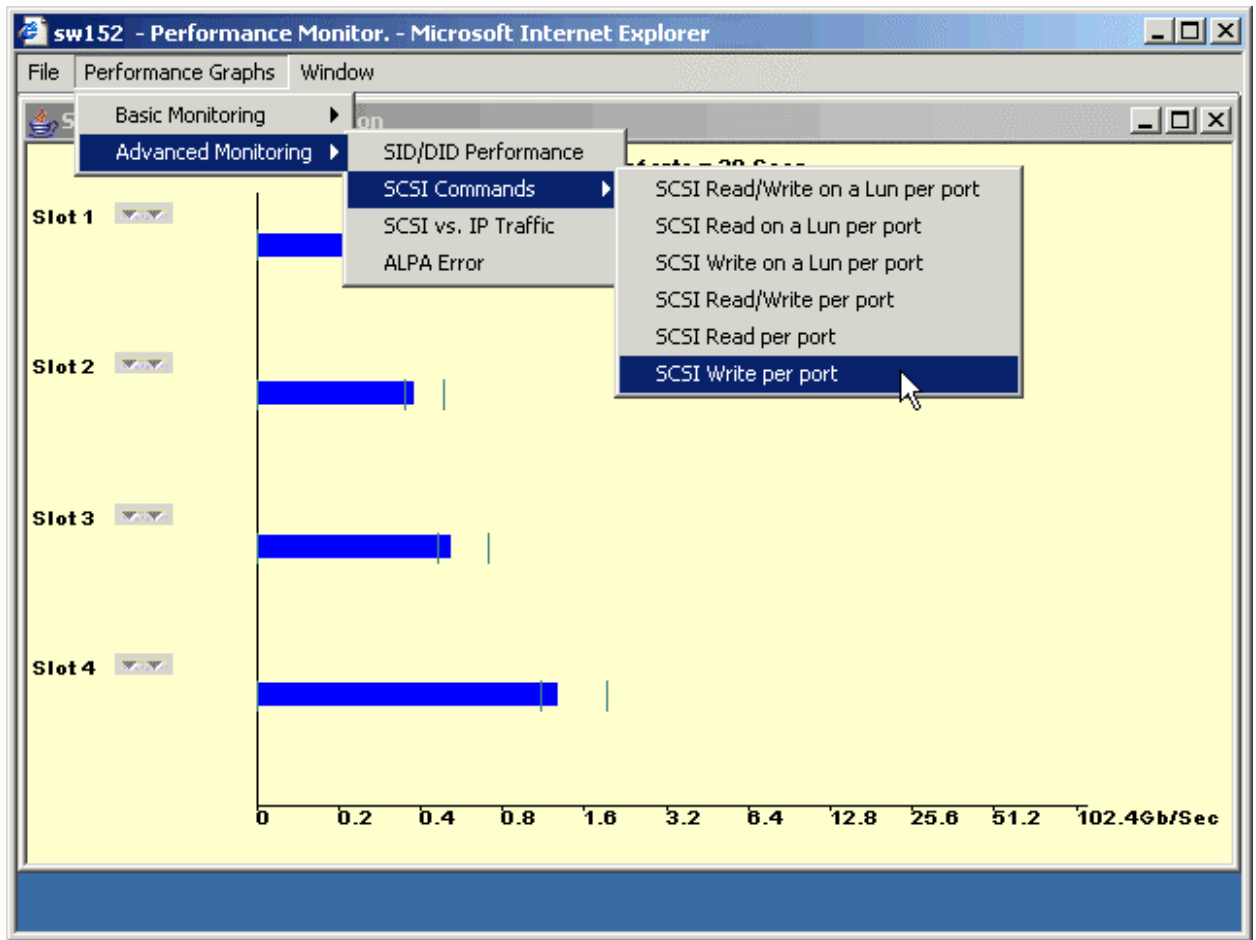
Graphs within the Performance Monitor module are updated every 30 seconds. When you first display the graph or if you modify the graph (such as to add additional ports), you might have to wait up to 30 seconds before the new values are shown.

On page 14-3, add this paragraph after the first paragraph:

Port throughput utilization is represented by a horizontal bar for each selected port, which gets longer or shorter depending on the percent utilization for that port at the last poll time. Thin short vertical intersecting bars give a historical perspective by representing the highest and lowest values reached for each selected port since the graph was opened. A third bar between them represents the average of all values polled. (See Figure 14-1.)

On page 14-3, replace Figure 14-1 with this one:

**Figure 14-1** Accessing Performance Graphs



## Closed Defects in Fabric OS v5.0.3 GA

This table lists the defects that have been newly closed in Fabric OS v5.0.3.

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000054120	High	<p>Summary: SNMP walk on MIB-2 increases the memory usage of SNMP daemon</p> <p>Symptom: Frequent repeated SNMP poll on switch entPhysicalTable will eventually cause an out-of-memory panic and a switch reboot.</p> <p>Solution: Fixed memory leaks in a function that retrieves SNMP MIB2 entPhysicalTable for switch physical attribute.</p> <p>Customer Impact: Continuous walk on MIB-2 exposes this memory leak. A 3rd party storage application can also expose this problem when polling the entPhysicalTable.</p> <p>Probability: Medium</p> <p>Reported in Release: V5.0.0</p>
DEFECT000055410	High	<p>Summary: API returns error intermittently when trying to establish a session with the proxy switch when FM tries to retrieve Port Stats and End-to-End Monitoring.</p> <p>Symptom: When Fabric Manager uses API, it returns -21 error code when the FabAPI_EstablishFabricSessionEx call is being made.</p> <p>Solution: To avoid potentially locking up the local switch, ensure that only one thread or process at a time gets access to the shared memory area used by SAPI library to pass management data to the target switch.</p> <p>Customer Impact: PM/APM features are not guaranteed to gather data at every 5-minute interval. Workaround exists for creating CM profile: re-create the profile. But there is no workaround when an existing CM profile is scheduled to be run.</p> <p>Reported in Release: V5.0.0</p>

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000056369	High	<p>Summary: Common access layer daemon (cald)/msarr memory leak.</p> <p>Symptom: Port Stats not retrieved on 2+6 fabric until fabric (or problematic switches) are rebooted. Switch reboot results.</p> <p>Solution: Fixed various issues identified during FABOS manageability stress test. The fixes include plugging memory leaks and handling corner cases such as port stats retrieval failure when ARR server is suddenly unreachable, etc.</p> <p>Workaround: N/A.</p> <p>Customer Impact: Not likely to occur on a customer system, since the problem was the result of highly stressful testing on uncommon configurations.</p> <p>Probability: Low</p> <p>Reported in Release: V5.0.1</p>
DEFECT000056405	High	<p>Summary: Switch panics with OOM (out of memory) panic after Fabric Watch monitor change.</p> <p>Symptom: After firmware download from FOS v5.0.1 to v4.4.1a on a SW12000, FOS v4.4.1a panics with OOM (out of memory) kill when there is a change in the Fabric Watch configuration to set thresholds in fabric class and SFT state. Configuring an email alert upon any change in SFP voltage caused an excessive number of emails to be generated at a rate greater than the SW12000 CPU could process and deliver. Each email consumes about 300K of memory and can eventually consumed all remaining memory.</p> <p>Solution: This fix limits the number of sendmail processes running in the switch by implementing an overflow control mechanism. When overflow occurs, mail alerts will be discarded and user will be informed through a raslog warning message. When the overflow clears, the number of discarded mail alerts will be displayed to the user.</p> <p>Workaround: Disable mail alerts using 'fwconfigure' command.</p> <p>Customer Impact: This problem is caused by an unusual configuration and excessive Fabric Watch email alerts. This configuration is neither recommended nor expected. This problem has been observed only once and several attempts to reproduce it failed.</p> <p>Probability: Low</p> <p>Reported in Release: V5.0.1</p>

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000056819	High	<p>Summary: Common access layer daemon (cald) stopped by software watchdog when faulty devices are connected to the fabric.</p> <p>Symptom: Switch reset after cald is stopped by kSWD, then switch is back to normal.</p> <p>Solution: cald used a timer thread to periodically check environmental monitor daemon (EMD) for readiness to accept data. If there are fault devices connected, name server and cald timer thread compete for the same message queue. Timer thread asserts if it cannot write to queue. The solution is to simplify cald design to use an existing SCN notification mechanism rather than a timer thread for polling when emd is ready.</p> <p>Workaround: Disable unstable ports to reduce SCN.</p> <p>Customer Impact: cald may crash after a system reboot caused by too many scn's in the queue.</p> <p>Probability: Medium</p> <p>Reported in Release: V5.0.1</p>
DEFECT000056966	High	<p>Summary: After upgrade to v4.4.0c, portState of persistent not reported by switchshow and portshow from Web Tools.</p> <p>Symptom: After upgrading from 4.2.2a to 4.4.0c, portState of persistent is lost in the following outputs: switchshow and portshow. Traffic and switch functionality are not affected.</p> <p>Solution: Derive IsportCfg from portCfg if it is not already in configuration. This will preserve persistence following upgrade.</p> <p>Workaround: N/A.</p> <p>Customer Impact: Usability issue where portcfgshow shows the correct state, but switchshow and portshow from Web Tools do not show the correct state.</p> <p>Probability: High</p> <p>Service Request# RQST00000037683</p> <p>Reported in Release: V4.4.0</p>

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000057028	High	<p>Summary: MSD killed during PID format change from 1 to 2.</p> <p>Symptom: When the PID format was changed from 1 to 2 on a SW48000, the Management Service Daemon (msd) terminated unexpectedly, followed by CP failover.</p> <p>Solution: This problem is related to MS Topology Discovery. On ELS_RJT with Logical Busy, the node object is being placed in the retry list. In this case the original IU should not be freed, because it will be used later to retry on that node.</p> <p>Workaround: Pre-configure the PID format and then add the switch to an existing fabric running the same PID.</p> <p>Customer Impact: This issue should not occur under normal maintenance operation. It resulted from changing PID formats on an active fabric.</p> <p>Probability: Low</p> <p>Reported in Release: V5.0.1</p>
DEFECT000058383	High	<p>Summary: firmwareDownload finishes with the message "Verification succeeded" while 8 rpm packages generated errors during install.</p> <p>Symptom: May see the following in the install log:  error: /tmp/rpm-32158/lkcd-4.1_1_2.4.19-1.ppc.rpm does not appear to be a RPM package  #####  Write kernel image into flash.  .....  Verification SUCCEEDED</p> <p>Solution: Removed the misleading "Verification SUCCEEDED" message upon detecting errors generated by rpm packages.</p> <p>Customer Impact: The user might believe the install was successful, when it in fact failed.</p> <p>Service Request# RQST00000038713</p> <p>Reported in Release: V4.4.0</p>

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000058823	High	<p>Summary: Memory leak when using security API and license module.</p> <p>Symptom: Memory usage increase.</p> <p>Solution: Fix a memory leak in the open source security password authentication module and FOS license "port on demand" license check code.</p> <p>Workaround: Restart weblinker, with temporary loss of web page access.</p> <p>Customer Impact: Web Tools polling page can cause web tool daemon (weblinker) to stop after it accumulates a certain amount of memory. Since weblinker can be restarted, the impact may be a temporary loss of web page access.</p> <p>Probability: Medium</p> <p>Reported in Release: V4.4.0</p>
DEFECT000059427	High	<p>Summary: Server link down occurred during HAfailover.</p> <p>Symptom: Traffic disruption (port reset) is observed during the HAfailover.</p> <p>Solution: When a buffer credit mismatch is detected, reset the buffers (if possible) or reset the port as a last resort.</p> <p>Workaround: Locking the port to G-port should help.</p> <p>Customer Impact: This will only happen when switch port becomes an E-port (segmented), when the device is initializing and in bypass mode. Later when the device sends OLS and eventually FLOGI, the switch port comes up as an F-port, causing the buffer credit mismatch. This is observed with a specific 3rd party device only.</p> <p>Probability: Low</p> <p>Service Request# RQST00000038681</p> <p>Reported in Release: V4.2.2</p>

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000059590	High	<p>Summary: In interopmode, name server daemon (nsd) panics due to domain address RSCN.</p> <p>Symptom: nsd panics in interopmode after "I/O Stream Guard" setting for 3rd party switch E-port is changed.</p> <p>Solution: Add the domain address rscn to the pending rscn list in interop mode.</p> <p>Customer Impact: Domain address RSCN is not handled in interopmode. If switch name and ipaddress are changed or the I/O Stream Guard is turned on in a 3rd party switch, name server could panic, causing the switch to panic or failover.</p> <p>Probability: High</p> <p>Service Request# RQST00000039840</p> <p>Reported in Release: V4.4.0</p>
DEFECT000059881	High	<p>Summary: Panic happens after firmwaredownload between v4.2.x and v5.0.1</p> <p>Symptom: Running in Interopmode downgrading the firmware on one CP to 4.4.x/4.2.x, while leaving the other CP at 5.0.1, can cause a panic after the failover operation is complete.</p> <p>Solution: Zone enforcement control mechanism changed from zone daemon to name server daemon in later release. For backward compatibility, the fix is to re-load the port's zone type from the name server only in non-Interopmode and when downgrading from common HA database version.</p> <p>Customer Impact: This will only be seen when downgrading firmware from version 5.0.1 while operating in "Interop Mode." Switch will panic and cause a cold-failover.</p> <p>Probability: Medium</p> <p>Reported in Release: V5.0.1</p>

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000060761	High	<p>Summary: Switch rejects a series of RFT_IDs and PLOGI from NPIV ports to targets.</p> <p>Symptom: Running test with NPIV setup may cause switch to reject RFT_ID and miss frames</p> <p>Solution: Memory corruption identified and fixed in name server area update handling when there are devices on line and off line from the same port during one update area event. In this case, the name server would first handle the online device and use a data structure to set up zone enforcement. When handling the offline device, the same data structure is reused to do zone enforcement again, but the data structure was not reinitialized. The fix is to reinitialize the zone enforcement structure before handling the offline device.</p> <p>Customer Impact: This is only seen in NPIV environment.</p> <p>Probability: Medium</p> <p>Reported in Release: V5.0.1</p>
DEFECT000060886	High	<p>Summary: The Duplex mode of Ethernet port will be reset to autonegotiation mode by changing the IP address or subnet mask thru ipaddrset.</p> <p>Symptom: The Ethernet port operating mode which the user set up will be reset by switch IP address change, and Ethernet port goes back to autonegotiation mode.</p> <p>Solution: Ethernet mode is getting reset whenever the IP address is changed, so ethernet setting is restored after IP address changes.</p> <p>Customer Impact: Use default setting rather than user specific setting to avoid unexpected behavior during ipaddress change.</p> <p>Probability: High</p> <p>Service Request# RQST00000041373</p> <p>Reported in Release: V5.0.1</p>

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000061214	High	<p>Summary: Dual CP based switch crashed after firmwaredownload command.</p> <p>Symptom: Telnet into switch results in ipadmaddrget ret=-1 and most daemons have stopped..</p> <p>Solution: Use an internal command to force failover during firmware download rather than depending on a Linux system call. As Linux system call uses more resources, it could fail, stopping all daemons.</p> <p>Workaround: N/A.</p> <p>Customer Impact: This should only impact dual CP based systems, and only during firmware upgrade.</p> <p>Probability: Medium</p> <p>Reported in Release: V4.4.2</p>
DEFECT000061277	High	<p>Summary: Telnet to switch failed for at least one hour during firmwaredownload w/wo option -s.</p> <p>Symptom: Telnet to switch ip address fails.</p> <p>Solution: Switch is not reachable after firmware download until gateway ARP cash is flushed approximately 1 hour later. Gratuitous ARP packets sent during fail over are getting dropped because of network congestion or at 3rd party router block out window. Added retry code and also will now send both ARP request and ARP reply during gratuitous ARP as per RFC.</p> <p>Customer Impact: User may not be able to telnet back to the switch after using "firmwaredownload". Console and FC traffic works fine. This is observed with one specific connected ip router only.</p> <p>Probability: Medium</p> <p>Reported in Release: V5.0.1</p>

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000061425	High	<p>Summary: Memory leak in common access layer daemon (cald) with mixed versions of FOS 4.4.x and FOS 5.0.x in the fabrics.</p> <p>Symptom: OOM stops cald without cald corefile.</p> <p>Solution: Fix cald to free memory allocated during handling an unrecognized command from a later FOS version.</p> <p>Workaround: Ensure all switches are running the same level of FOS, either FOS 4.4.x or FOS 5.0.x.</p> <p>Customer Impact: The problem happens if and only if there is a mix of FOS 4.4.x and FOS 5.0.x switches in the fabric.</p> <p>Probability: High</p> <p>Reported in Release: V4.4.2</p>
DEFECT000061429	High	<p>Summary: Name server daemon (nsd) panics upon receiving bad frame over the wire.</p> <p>Symptom: An HBA located in the extension PCI Bus sends bad frames over the wire, causing the switch to panic.</p> <p>Solution: For NS query request by port id, if the first byte of the data is not zero, it should be recognized as invalid data and filtered out by rejecting the request, rather than processing it.</p> <p>Workaround: N/A.</p> <p>Customer Impact: This only happens when bad frames are received.</p> <p>Probability: Low</p> <p>Service Request# RQST00000041757</p> <p>Reported in Release: V4.4.0</p>

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000061490	High	<p>Summary: Voltage errors result in a switch fault.</p> <p>Symptom: 0x32d (fabos): Dec 26 17:27:20 Switch shut down with following message logged: Switch: 0, Error EM-SENSOR, 2, Switch error, 2.5V (3.30) above threshold.</p> <p>Another example: 0x258 (fabos): Dec 26 17:27:20 , Switch: 0, Critical EM-POWER_DOWN, 1, Slot 0 is shutting down</p> <p>Solution: Make SilkWorm 4020 match other platforms so it will not shut down due to voltages out of range. Log the condition and continue. Furthermore, do not consider the sensor dumps that EM creates to be critical problems.</p> <p>Customer Impact: This issue applies to the SilkWorm 4020 only.</p> <p>Probability: Low</p> <p>Reported in Release: V4.4.1</p>
DEFECT000061517	High	<p>Summary: Blade fault due to transient pci misread.</p> <p>Symptom: Error log shows: 2005/10/02-04:02:40, [BLM-5020], 1003/0,, CRITICAL, SilkWorm24000, S10,P113(6): quadpt 1 excessive busy_mini for ep: 0x3001, bloom.c, line: 4251</p> <p>Solution: Changing the code to read the same register multiple times and interleave the reads with the read of other bloom register to be able to identify the situation and recover from it.</p> <p>Workaround: Reset the blade recovers.</p> <p>Customer Impact: This was observed at a particular customer site, but Brocade was unable to recreate this in house with returned port blades and CPs. The code changes only impact bloom asic based platforms such as Silkworm 3900, 12000, 24000</p> <p>Probability: Low</p> <p>Service Request# RQST00000041800</p> <p>Reported in Release: V4.4.0</p>

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000061659	High	<p>Summary: Nscam does not show device at edge fabric, though backbone switch shows device correctly.</p> <p>Symptom: One switch in an edge fabric does not show the switch name in fabricshow and the name server entries have vanished for translated domains. But the nscamshow on a different switch in the edge fabric shows the entries against the same translated domains.</p> <p>Solution: When FCR is not ready, fabric inquiry responses could be rejected. FOS retry fabric inquiry did not occur due to code error.</p> <p>Workaround: N/A.</p> <p>Customer Impact: This would only occur when first fabric inquiry response was rejected.</p> <p>Probability: Low</p> <p>Reported in Release: V5.1.0</p>
DEFECT000062281	High	<p>Summary: LIP from storage does not generate RSCN for host when fcAL.alwaysSendRSCN is enabled.</p> <p>Symptom: With fcAL.alwaysSendRSCN enabled, when unplugging a disk in a JBOD and plugging the same disk back in (thus, with the same pid and same WWN): once the loop port is online, the switch will not send out the RSCN to registered host ports when the device LIPs.</p> <p>Solution: When updating Area, check if the config flag alwaysSendRSCN is on. If it is on, always send the RSCN, even when the wwn is the same one as before as per documented in the man page since FOS 4.2.</p> <p>Customer Impact: This change only impacts a loop device.</p> <p>Probability: Medium</p> <p>Service Request# RQST00000042165</p> <p>Reported in Release: V5.0.1</p>

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000062300	High	<p>Summary: Memory leak fixes for error condition with weblinker.</p> <p>Symptom: N/A.</p> <p>Solution: Fix corner case memory leak with weblinker.</p> <p>Workaround: N/A.</p> <p>Customer Impact: Memory leaks identified during code review. These are not in polling pages, and will not have significant impact to the switch memory.</p> <p>Probability: Low</p> <p>Reported in Release: V5.0.1</p>
DEFECT000062407	High	<p>Summary: Time server daemon (tsd) panic due to i2c contention.</p> <p>Symptom: corefump frame has: #2 0x0f3c2a34 in __libc_system (line=0x105363d4 "hwclock -w --utc") at ../sysdeps/posix/system.c:136</p> <p>Solution: Further reduce the chance of i2c contention by changing the license library/em/hil so it will cache license data rather than have each application call into the EM access WWN card through i2c. This is a continuing effort from DEFECT56206 changed in FOS 4.4.0e.</p> <p>Customer Impact: The problem is likely to be seen with a large number of manageability applications frequently accessing the license database at the same time.</p> <p>Service Request# RQST00000042411</p> <p>Reported in Release: V5.0.1</p>

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000062566	High	<p>Summary: Executing the nsallshow command caused the name server daemon (nsd) to stop and the CP to panic and reboot.</p> <p>Symptom: When user issues nsallshow command with invalid input, it will cause data corruption.</p> <p>Solution: Ignore and reject any invalid nsallshow request with invalid input.</p> <p>Workaround: Ensure that only small positive values are entered with this command.</p> <p>Customer Impact: The nsallshow command may cause the switch to panic if negative or big positive values are entered on the command line.</p> <p>Probability: High</p> <p>Service Request# RQST00000042486</p> <p>Reported in Release: V4.4.0</p>
DEFECT000062652	High	<p>Summary: Common access layer daemon (cald) panic on SilkWorm 24000 switch in long running fabric.</p> <p>Symptom: During longevity testing in a given fabric, the launch switch (SilkWorm 24000) has cald core files.</p> <p>Solution: After performing realloc, the stale pointer was being used, causing segmentation violation in cald.</p> <p>Customer Impact: This is a random access error. It was seen once in the longevity test fabric with 9 switches, and 1 switch experienced the panic.</p> <p>Probability: Medium</p> <p>Reported in Release: V5.1.0</p>

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000063350	High	<p>Summary: After firmware upgrade/downgrade, hosts lost device on SilkWorm3900 and SilkWorm12000.</p> <p>Symptom: After firmware upgrade/downgrade on a SilkWorm3900 and SilkWorm 12000, a host reboot/shutdown might cause the other host sharing the same internal route to lose the device connection. When the down host comes back up, all is recovered.</p> <p>Solution: The problem is caused by miscalculating shared routes when the internal trunk master used for routing is an odd port on a SilkWorm3900 and SilkWorm 12000. It may only happen on switches with multiple E or F source ports connected to the same target F port on the same switch, but with different mini-switches. The code has been fixed to respond in these situations with the appropriate route reconstruction during HAreboot.</p> <p>Workaround: portdisable/portenable the shared port that lost the shared internal route and/or reboot the switch.</p> <p>Customer Impact: The problem exists since FOS4.2 on SilkWorm3900 and SilkWorm 12000. It is more likely after an HAreboot or firmwaredownload and may be exposed when F/E ports go down.</p> <p>Probability: Medium</p> <p>Service Request# RQST00000041351</p> <p>Reported in Release: V4.4.0</p>
DEFECT000051403	Medium	<p>Summary: Persistentdisable ports 9 - 14 displayed in Web Tools are not blinking amber</p> <p>Symptom: Web Tools shows the wrong status (no blinking light) on the persistently disabled ports.</p> <p>Solution: Always leave permanently disabled ports with status LED the color black.</p> <p>Customer Impact: This issue impacts the customer using Web Tools to monitor switch port status.</p> <p>Probability: High</p> <p>Reported in Release: V4.4.1</p>

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000057985	Medium	<p>Summary: Supportsave saves a tracedump assuming a panic. If there was no panic, the trace info will be misleading unless the memory is flushed first.</p> <p>Solution: First, SupportSave will retrieve the existing trace dump file from the switch. This will be named old, then it will automatically generate a new trace dump (named new) and transfer out. Note: If using interactive mode, the warning of the trace dump is removed. The first option (OK to Proceed[Y/N]) is also removed. Automated Supportsave scripts need to be changed. Frame Filter logs are also changed to reduce flood message during setdbg.</p> <p>Customer Impact: No external customer impact.</p> <p>Probability: Low</p> <p>Reported in Release: V5.0.1</p>
DEFECT000060454	Medium	<p>Summary: FDISC request gets rejected on some platforms for NPIV ports after firmware upgrade.</p> <p>Symptom: Not able to create NPIV virtual ports on SilkWorm 3900 switch after code upgrade to later FOS.</p> <p>Solution: On future FOS version, a virtual PID request will be rejected if the standby HA component SWC version is lower than 3. The SWC version of the standby for a single CP system running FOS5.0.x firmware is shown as 2 instead of 3, which will cause problem when upgrading to future FOS.</p> <p>Workaround: Note: Fix resolves FOS v5.0.3 to future FOS upgrade. Does not address FOS v5.0.1-&gt;future FOS upgrade (i.e., the fix has to be in the originator FOS version). For the workaround, after firmwaredownload, perform a non-disruptive HAreboot before running the FDISC script.</p> <p>Customer Impact: The NPIV functionality on single CP platforms and the SilkWorm12000 will not work without this fix. But the problem won't be seen until a future FOS v5.1 upgrade with NPIV ports.</p> <p>Reported in Release: V5.1.0</p>

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000060689	Medium	<p>Summary: Non-persistent banner after upgrading from 4.2.2 to 4.4.0d if viewed with SSH session.</p> <p>Symptom: After a firmware upgrade from version 4.2.2 to version 4.4.0d, the previously set banner does not display when the user logs in with ssh (using Putty). It does work with a regular telnet session or a telnet session using Putty.</p> <p>Solution: Fixed ssh banner not getting displayed for admin/user accounts.</p> <p>Customer Impact: No major impact from switch traffic and function point of view, but a feature for regulatory compliance.</p> <p>Probability: High</p> <p>Service Request# RQST00000041185</p> <p>Reported in Release: V4.4.0</p>
DEFECT000061954	Medium	<p>Summary: "Total" in portPerfShow not calculated correctly on the SilkWorm 4020.</p> <p>Symptom: Individual port performance does not add up to the "total" number displayed.</p> <p>Solution: For SilkWorm 4020 and similar boxes and embedded switches with more than 16 ports, if there is a large amount of I/O on most ports, the total shown by portperfshow will be too low by a factor of three or four. The reason is that the code that keeps track of the order of magnitude of the total gets confused when the display finishes the first row of output. In effect the total shown is the total of ports 16-19 + .001 of the total of ports 0-15. The fix is simply to keep track of the magnitude.</p> <p>Customer Impact: There is no functional impact.</p> <p>Probability: Medium</p> <p>Reported in Release: V5.0.2</p>

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000062401	Medium	<p>Summary: Setting the Domain ID to 238 in Interopmode causes a POSTerror.</p> <p>Symptom: If Interopmode is turned on and then the Domain ID is configured to an invalid number ( &gt; 127), the switch will fail to initialize properly after a reboot and the switch will be faulted.</p> <p>Solution: Add a step to commit the configuration after the interopMode command so that subsequent "configure" operations will use an update MAX Domain number to validate user input.</p> <p>Workaround: To avoid this symptom, always follow the recommendation for the "interopMode" command and reboot after changing the mode. This will allow the switch to readjust the domain ID validation limits for interopMode such that the user will not be able to configure the domain ID to an invalid number. If this symptom has already occurred and the switch is in a non-functioning state, a valid configuration can be re-established by requesting a reboot with "Restore Factory Configuration" option.</p> <p>Customer Impact: This is a negative test. Switch will fail to initialize properly after a reboot and the customer will have to Restore Factory Default to recover the switch.</p> <p>Probability: Low</p> <p>Reported in Release: V5.0.2</p>
DEFECT000062793	Medium	<p>Summary: PCI errors are reported while POST is running.</p> <p>Symptom: It is possible that if enough recoverable PCI errors occur during diagnostic POST, the switch may be classified as Faulted.</p> <p>Solution: Remove a code change made in FOS 5.0.2 for port performance data polling on asic registers, causing PCI errors during the execution of diagnostic POST</p> <p>Workaround: Two possible workarounds: 1) Reboot the switch. This might result in a successful POST. OR 2) Use "diagDisablePost" to avoid the false POST failure.</p> <p>Customer Impact: This symptom could lead to a functional switch being removed from operation due to a reported POST failure. This defect only exists in the FOS 5.0.2 code stream.</p> <p>Probability: Low</p> <p>Reported in Release: V5.0.2</p>

Defects Newly Closed in Fabric OS v5.0.3 GA		
Defect ID	Severity	Description
DEFECT000062868	Medium	<p>Summary: Launching Switch View from FOSv5.0.3 switch will work correctly, but it will not work from a non-FOSv5.0.3 switch from FM Fabric Tree.</p> <p>Symptom: Web Tools will hang when trying to bring up FOS v5.0.2/5.0.3 switches from other switches.</p> <p>Solution: Fix switchview applet code such that launching Switch View for a FOSv5.0.3 switch from FM and other switches from the switch explorer tree works.</p> <p>Workaround: Launch Web Tools from FOS v5.0.2/V5.0.3 switch directly. For FM, it has a workaround from menu items for some features, such as Admin, Fabric Watch, Event, Status, Telnet, etc.</p> <p>Customer Impact: GUI interface is not fully working for switchview. This is a FOS 5.0.2 regression. With this fix, 5.0.3 no longer has any problem, but FOS 5.0.2 still faces the same issue.</p> <p>Probability: High</p> <p>Reported in Release: V5.0.2</p>
DEFECT000063339	Medium	<p>Summary: Port base routing requirement and configuration change accessibility with aptpolicy.</p> <p>Symptom: When running the aptpolicy, the port based routing option is only available to root, not admin. For some customer applications, port based routing is needed.</p> <p>Solution: Make port based routing option available to admin in the aptpolicy command.</p> <p>Workaround: On SilkWorm 48000, port based routing setting can be enabled by admin by using web-tools "ficon cup" tab.</p> <p>Customer Impact: This only impacts SilkWorm 48000 with a 3rd party customer application that needs to use port based routing to work properly.</p> <p>Service Request# RQST00000042205</p> <p>Reported in Release: V5.0.1</p>

## Closed Defects in Fabric OS v5.0.1d

Defects Closed in Fabric OS v5.0.1d		
Defect ID	Severity	Description
DEFECT000061239	High	<p>Summary: cfgdisable results in loss of access between ports in soft zoning</p> <p>Symptom: Brocade has identified a latent defect in Fabric OS v5.0.1x due to code change in 5.0.1c. When a new device is introduced, or when a zone configuration is changed in a fabric, the host will not see the targets in session based zoning and the host may not see targets in hardware based zoning.</p> <p>Solution: This defect is in the area of PLOGI frame handling, where the name server daemon has a generation number to compare for stale PLOGI frames. The defect causes the good PLOGI frames to be dropped. The unnecessary "generate-number" code path was not exercised and has since been removed.</p> <p>Workaround: There is no workaround for this issue unless the host has a retry plugin capability.</p> <p>Customer Impact: This issue is applicable only to Fabric OS v5.0.1c on the following platforms: SW4100, 48000, 200E, and SW3014. Previous Fabric OS v5.0.1x releases will not encounter this defect because the code path containing this defect is invoked only as a result of the change in 5.0.1c running on the above-mentioned platforms. Upgrading from any Fabric OS releases to v5.0.1c without adding a new device and without changing zone configuration will not encounter this problem initially. However, subsequent changes to the fabric, causing the host to issue PLOGI to the targets, will encounter the problem.</p> <p>Probability: High</p> <p>Reported in Release: V5.1.0</p>

## Closed Defects in Fabric OS v5.0.1c

Defects Closed in Fabric OS v5.0.1c		
Defect ID	Severity	Description
DEFECT000059548	High	<p>Summary: If a switch fails in a fabric that has blocked FSPF traffic, the neighboring core switch loses links and appears to hang. All links remain online.</p> <p>Symptom: After an AP7420 reported a parity error on a hardware component, the FOS switch topologyshow and portregshow indicated 2 connected domains lost the route to each other.</p> <p>Solution: Fabric Shortest Path First (FSPF) maintains a bi-directional Link State Record (LSR) database about links in the fabric and uses it to dynamically compute the shortest path from a local domain to all other domains in the fabric. When an ISL has only a 1-directional communication mode available, the 1-directional LSR causes the FSPF shortest path computation to remove the wrong route. The fix is not to remove the route that was just added if the bi-directional communication is no longer available for an ISL.</p> <p>Workaround: Identify and portdisable the problematic ISL port.</p> <p>Customer Impact: This unlikely event results in losing some routes in the fabric, and the host-to-target traffic is impacted.</p> <p>Probability: Low</p> <p>Service Request# RQST00000039984</p> <p>Reported in Release: V4.2.0</p>
DEFECT000059855	High	<p>Summary: rpcd coredump caused switch panic or failover.</p> <p>Symptom: rpcd0 core dump with signal 11, Segmentation fault, but no stack back trace can be generated on the panic thread.</p> <p>Solution: Fixed an error code handling path of secure connection, where RPCd has a pointer defined as local variable and located on stack, and same pointer is also inserted to a global list. At some point when the function exits, these pointers could be no longer valid, but still accessed through global list. As the stack being overwritten, it could cause rpcd to crash.</p> <p>Customer Impact: Switch may panic if the stack is badly corrupted and accessed. This problem is only observed when there is security scan application running.</p> <p>Probability: Low</p> <p>Service Request# RQST00000040243</p> <p>Reported in Release: V4.4.0</p>

Defects Closed in Fabric OS v5.0.1c		
Defect ID	Severity	Description
DEFECT000060267	High	<p>Summary: On condor ASIC based platform, port fault due to busy buffer stuck error on switch ISL with a 3rd party storage.</p> <p>Symptom: CDR-1002: Port 27 chip faulted due to internal error which took down ISLs on Silkworm 4100.</p> <p>Solution: The problem was that a remote device sent a PLOGI to a non-existent loop device. The filter message that name server daemon received has to be released when it detects the loop device is no longer there. But the port number passed to filter resource release code is incorrect caused the resource not being freed and receive buffer being tied up. The fix is to pass the correct port number so filter resource is release correctly.</p> <p>Customer Impact: The issue is observed with a 3rd party storage controller during controller fail over test: when one controller takes over for another, it appears to the Hosts that one of the PL devices simply moved ports which introduce the scenario of Plogin to a loop device that disappeared.</p> <p>Probability: Low</p> <p>Service Request# RQST00000040731</p> <p>Reported in Release: V5.0.1</p>

### ***Closed Defects in Fabric OS v5.0.1b***

Defects Closed in Fabric OS v5.0.1b		
Defect ID	Severity	Description
DEFECT000059540	Critical	<p>Summary: SW24000 dropping frames and causing IFCCs (Interface Control Checks - FICON)</p> <p>Symptom: After placing the fabric into a long distance mode, and adding a SW24000 into a fabric and reconfiguring the fabric, devices attached to the SW24000 that were cascaded to other switches started getting IFCCs (Interface Control Checks).</p> <p>Solution: Corrected programming of back-end port VC mapping while the fabric is programmed in a long distance fabric mode setting.</p> <p>Customer Impact: Interface Control Checks blocking access to some devices. This has only been observed in a FICON environment.</p> <p>Probability: High</p> <p>Reported in Release: V5.0.1</p>

Defects Closed in Fabric OS v5.0.1b		
Defect ID	Severity	Description
DEFECT000058000	High	<p>Summary: When a disk drive on a loop is replaced, the Nameserver still shows the WWN of the old drive.</p> <p>Symptom: During JBOD drive replacement testing, the new drive WWN information is not listed in the switch name server table. The portloginshow command displays the correct WWN of the drive, but the old wwn shows up in the name server table.</p> <p>Solution: When one of the loop devices is hot swapped, NS receives a UPD_AREA SCN indicating same device PID with different WWNs. To be able to support this behavior, NS is changed to treat this as the old device offline and new device with same PID online. The zone enforcement CAM is also updated accordingly.</p> <p>Workaround: After swapping the device, portdisable and portenable will correct the portwwn in the NS database.</p> <p>Customer Impact: After hotswapping a disk drive, the user sees the WWN of the old disk drive, instead of the WWN of the new disk drive.</p> <p>Service Request# RQST00000038373</p> <p>Reported in Release: V4.4.0</p>
DEFECT000058011	High	<p>Summary: Switch does not pass traffic in interop mode with Windows host when a zone change is performed without switch reboot</p> <p>Symptom: FC trace showed FOS 4.4 switch rejecting a GPN_ID with the error port ID not in register.</p> <p>Solution: The fix is to change zoning to set the proper zone type before pushing down the new zone configuration to the Name Server.</p> <p>Workaround: Reboot the switch.</p> <p>Customer Impact: Switch must be rebooted after the zone change.</p> <p>Probability: High</p> <p>Service Request# RQST00000038307</p> <p>Reported in Release: V4.4.1</p>

Defects Closed in Fabric OS v5.0.1b		
Defect ID	Severity	Description
DEFECT000058281	High	<p>Summary: SW48000: False RLIRs on 1Gig channels on system resets</p> <p>Symptom: When a System Reset Clear is issued to the mainframe operators console the SW48000 detects false link incidents on the 1Gig channels.</p> <p>Solution: Primitive is now read in top half and saved. Later, if there is rx_fifo, the saved primitive will be checked to see if OLS was received.</p> <p>Probability: High</p> <p>Reported in Release: V5.0.1</p>
DEFECT000058396	High	<p>Summary: Switch panic on FOS4.4.x with zoned assert on invalid interface identifier.</p> <p>Symptom: Zone panic with assert at merge/zn_merge_dbg.c:453, with call from zoneDomain_portsIfld.</p> <p>Solution: The fix is to recover if_id for all online ports during failover.</p> <p>Customer Impact: The problem is only likely to happen during upgrade from 4.2.x to 4.4.x when the switch is in interop mode. The switch may also assert when there is no effective CFG enabled in non-interopmode. Once the switch is upgraded to 4.4 and rebooted, the problem should not recur.</p> <p>Probability: Medium</p> <p>Service Request# RQST00000038732</p> <p>Reported in Release: V4.4.0</p>
DEFECT000058556	High	<p>Summary: SW200E Firmwaredownload problems</p> <p>Symptom: Firmwaredownload problems while performing multiple downloads with Fabric Manager and 2 of the 4 SW200Es failed with "unable to download ROM".</p> <p>Solution: This issue is caused by firmwaredownload not being able to install a RPM package after the package is downloaded from the network. The solution is to retry the install command for maximum of 4 times when the install command fails. If the install still fails after 4 retries, display a message "Fails to install RPM package".</p> <p>Service Request# RQST00000038947</p> <p>Reported in Release: V5.0.1</p>

Defects Closed in Fabric OS v5.0.1b		
Defect ID	Severity	Description
DEFECT000058745	High	<p>Summary: FICON CUP overnight test run stopped with ABTs</p> <p>Symptom: Unable to bring FICON CUP Port back online</p> <p>Solution: Fix the overflow condition by making sure that the reference count for FICON CUP field descriptor is recovered after HA. Remove FICON CUP filter when port is offline. And only update the reference count if it's none zero.</p> <p>Customer Impact: Loss of access to CUP Port</p> <p>Probability: High</p> <p>Reported in Release: V5.0.1</p>
DEFECT000058836	High	<p>Summary: SW24000 panic when multiple changes take place without Reliable Commit Service (RCS)</p> <p>Symptom: Zone daemon causes switch panic (zoned ASSERT when trans_in_progress is detected) .</p> <p>Solution: Avoid the ASSERT in case multiple transactions are initiated at the same time when RCS is disabled in the fabric.</p> <p>Workaround: Enable RCS, avoid multiple transactions initiated in parallel.</p> <p>Customer Impact: In a fabric not running RCS, multiple transactions can occur in the fabric. The Zone daemon can process only one transaction at a time and could hit a race condition and cause a switch panic. The probability of this actually happening is low due to the small race condition window.</p> <p>Probability: Low</p> <p>Service Request# RQST00000039208</p> <p>Reported in Release: V4.2.2</p>

Defects Closed in Fabric OS v5.0.1b		
Defect ID	Severity	Description
DEFECT000059048	High	<p>Summary: Multiple hosts lose IO, fcping to storage drops frames on certain switches in fabric</p> <p>Symptom: While running tests that disabled ISL between a SW200E and a SW48000, and on the SW48000 running a slotpoweroff / slotpoweron script, caused multiple hosts to be unable to query their respective storage volumes even though the name server and zone database looked OK.</p> <p>When performing an fcping between a host and storage port, frames were dropped on multiple switches in the fabric. Hafilovers on dual CP switches did not solve the problem. A reboot of two affected switches allowed the host to query its storage volumes even though an fcping between the two continues to drop frames on multiple switches in the fabric. A switchdisable/switchenable seemed to clear unstable fabric.</p> <p>Solution: This issue happens only when POST is run on a CP/port blade. The solution is to suppress the rebalance operations when diagnostics are running.</p> <p>Workaround: Disable POST temporarily while removing or inserting a port or CP blade.</p> <p>Customer Impact: There may be some missing internal routes due to this defect.</p> <p>Service Request# RQST00000039426</p> <p>Reported in Release: V5.0.0</p>
DEFECT000059285	High	<p>Summary: Firmware v5.0.1 - switch does not display status "MARGINAL" when the fan is disabled. Setting for SwitchStatusPolicy - Fans: Down 2, Marginal 1.</p> <p>Symptom: Switch does not display status "MARGINAL" when the fan is disabled using the fandisable command. Setting for SwitchStatusPolicy - Fans: Down 2, Marginal 1.</p> <p>Solution: Changing switch status even when the fan FRU state is OFF due to disabling the fan.</p> <p>Customer Impact: Disabled Fan did not contribute to the switch status due to this the customer would not see the switch status change; i.e., from HEALTHY to MARGINAL.</p> <p>Service Request# RQST00000039509</p> <p>Reported in Release: V5.0.1</p>

Defects Closed in Fabric OS v5.0.1b		
Defect ID	Severity	Description
DEFECT000059393	High	<p>Summary: No way for a customer to change if webtools.basicuser.enabled other than as root</p> <p>Symptom: If a user uses the Web Tools EZ on a SW200E that had been set for standard webtools, the webtools.basicuser.enabled will be set and will not allow the user to return to the use of the standard webtools interface. To undo this problem requires root access to the switch. This may be an issue as most OEM-provided switches are not provided with a root password.</p> <p>Solution: In the "configure" command, add a new field for basic user mode. User can telnet to switch and login as admin, disable the Basic User Mode through the "configure" command</p> <p>Service Request# RQST00000039684</p> <p>Reported in Release: V5.0.1</p>
DEFECT000059437	High	<p>Summary: Switch blade insertion causes FICON I/O disruption.</p> <p>Symptom: In a fully populated switch, inserting a switch blade causes numerous Interface Control Checks (IFCC) on mainframe channels. Mainframe will try to recover from these errors. These will also cause CALL HOME to support.</p> <p>Solution: The fix is to not do the rebalance operation when a new blade is inserted while running in a FICON environment.</p> <p>Customer Impact: There could be disruption to the existing traffic flows.</p> <p>Reported in Release: V5.0.1</p>
DEFECT000059443	High	<p>Summary: MVS System reports Interface control checks on CP removal</p> <p>Symptom: Interface errors during repair action involving removal of a CP in a FICON Environment</p> <p>Solution: Closed as a duplicate of 59048.</p> <p>Customer Impact: There may be some missing internal routes due to this defect.</p> <p>Probability: High</p> <p>Reported in Release: V5.0.1</p>

Defects Closed in Fabric OS v5.0.1b		
Defect ID	Severity	Description
DEFECT000059454	High	<p>Summary: In the FICON CUP tab in Webtools the "Device Based Routing" option needs to be changed to "Port Based Routing".</p> <p>Symptom: Enhancement request to change Device Based Routing to Port Based Routing in FICON environments.</p> <p>Solution: Changed behavior of button to enable Port Based Routing.</p> <p>Reported in Release: V5.0.1</p>
DEFECT000059533	High	<p>Summary: FSPF segment fault in de-reference a NULL Isdbe during sending RTE domain unreachable update</p> <p>Symptom: In a disruptive fabric environment, where domain is added and removed from the fabric, segment fault in FSPFd may occur which will trigger an HA failover.</p> <p>Solution: check for null pointer before de-reference link-state record in domain unreachable update to RTE.</p> <p>Reported in Release: V5.0.1</p>
DEFECT000059539	High	<p>Summary: SW4012 becomes unresponsive to enclosure requests to arbitrate loop through the I2C bus controller</p> <p>Symptom: If diagnostic post is enabled, SW4012 will stop responding to arbitration requests for the enclosure-to-switch communication path after the first diagnostic step is executed.</p> <p>Solution: Correct the algorithm designed to handle the case where the I2C device has been reset by the POST diagnostics.</p> <p>Workaround: Disabling diagnostic POST will allow the arbitration logic to function without disruption.</p> <p>Reported in Release: V5.0.1</p>
DEFECT000059616	High	<p>Summary: SW48000 displayed ASSERT - Failed expression: rg-&gt;rg_paths[snode-&gt;n_id.n_inst][dnode-&gt;n_id.n_inst] == 0 and OOPs after slotpoweroff either a port blade(either C16 or C32)</p> <p>Symptom: Upon execution of a number of actions on SW48000 with traffic running, like remove/reinsert standby CP, turn on/off trunking, disable/enable switch, hafailover, and finally when slotpower off on a port blade(either C16 or C32), get ASSERT error on RTE. Following the ASSERT failure, the switch rebooted and Oops occurs constantly.</p> <p>Solution: To ensure iod remains set through rapid multiple failovers.</p> <p>Reported in Release: V5.0.1</p>

Defects Closed in Fabric OS v5.0.1b		
Defect ID	Severity	Description
DEFECT000059649	High	<p>Summary: Model Number in Sense ID data not correct</p> <p>Symptom: MVS errors with I/O Ops. commands</p> <p>Solution: Modified the code which was computing the Model Number to handle switches with more than 128 ports</p> <p>Probability: High</p> <p>Reported in Release: V5.0.1</p>
DEFECT000059694	High	<p>Summary: Read Port Descriptors command (FICON) does not return bit zero set to "1" on all unimplemented ports</p> <p>Symptom: Unit checks from CUP Device on MVS System IPL</p> <p>Solution: Fixed the code so that all unimplemented ports, starting from the port number above the maximum to port number 256, will have bit zero set to "1".</p> <p>Customer Impact: Some MVS I/O Ops commands on the CUP Port fail</p> <p>Probability: Low</p> <p>Reported in Release: V5.0.1</p>
DEFECT000058928	Medium	<p>Summary: Port 23 on slot 10 shows non-trunking config on "portcfgshow"</p> <p>Symptom: Port 23 on slot 10 shows up as non-trunking when running "portcfgshow". Running a "configshow" shows duplicate ports for 246 (slot 10/port 22) and no entry for port 247 (slot 10/port 23). After setting trunk on port using "portcfgtrunkport 1", the correct port (247) will show up again under "configshow"</p> <p>Solution: There was a typo in default table which missed port 247 and instead contains two entries for 246. Fix is to just correct this one. The default values do not affect any changes to the values to port 247, which will be written as a correct entry.</p> <p>Service Request# RQST00000039284</p> <p>Reported in Release: V5.0.1</p>

Defects Closed in Fabric OS v5.0.1b		
Defect ID	Severity	Description
DEFECT000059561	Medium	<p>Summary: DLS change is not synced over to standby CP. This causes reroute and frame drop on existing ports when adding a new host with DLS turned off.</p> <p>Symptom: The "new" setting of DLS/IOD is not synced over to the standby CP. So, when there is a failover (due to "hafailover" or active CP plug-out), the new active CP would NOT have the new setting change that was made earlier. The result is that even DLS is set as OFF, disable/enable an F port still causes traffic reroute for all ports in the switch.</p> <p>Solution: Process IOD and DLS change management preparation on the standby CP even if there is no change to the routing policy.</p> <p>Reported in Release: V5.0.1</p>
DEFECT000059618	Medium	<p>Summary: WT EZ does not recognize the factory default zoning for SW 200E switch.</p> <p>Symptom: EZSwitchSetup states it is not configured for default zoning after it has just been instructed to restore defaults.</p> <p>Solution: Changed the warning message that pops up when user clicks on restore to factory default zoning to inform the user that this action will restore factory default zoning and that it will overwrite any previous zoning modifications done.</p> <p>The new message is          "You have chosen to restore default Fixed zoning, which means that current zoning will be overwritten.          Do you want to continue?"</p> <p>Reported in Release: V5.0.1</p>

## Closed Defects in Fabric OS v5.0.1a

Defects Closed in Fabric OS v5.0.1a		
Defect ID	Severity	Description
DEFECT000057565	Critical	<p>Summary: Oops: kernel access of bad area, sig: 11</p> <p>Symptom: With a SW4012 running 5.0.0_beta code and ISLs connected to an embedded storage switch, run ACU for SSP and then run traffic. Run ACU again to make more LUN allocation, the SW4012 may panic.</p> <p>Solution: A null function pointer was called when an unexpected error happened during autonegotiation. The null pointer has been replaced with valid function call which does nothing and the error is handled properly.</p> <p>Customer Impact: This problem has a greater chance of occurrence only in SW 4012 because its internal ports constantly do autonegotiation until a server is attached. On other switches, this is not the case.</p> <p>Probability: Low</p> <p>Service Request# RQST00000038087</p> <p>Reported in Release: V5.0.0</p>
DEFECT000058603	Critical	<p>Summary: When a PDCM matrix save fails no indication of location of error</p> <p>Symptom: If a port address name is invalid there is no indication of which port has an invalid name and must be corrected before the PDCM matrix maybe saved.</p> <p>Solution: When there is no change in name of a port, the FABOS returns a positive error code which should be ignored.</p> <p>Workaround: Manually clear all port address names and replace with valid names.</p> <p>Customer Impact: Could result in customer re-entering port address names.</p> <p>Probability: Medium</p> <p>Reported in Release: V5.0.1</p>

Defects Closed in Fabric OS v5.0.1a		
Defect ID	Severity	Description
DEFECT000057037	High	<p>Summary: Memory corruption when management software sends fabric slot information request through msd, which causes a switch panic.</p> <p>Symptom: kSWD kill of msd, portlogdump has following entry earlier: msd msRemQ 255 f004 00ffc7b,00ffc2c,10000060,69805fe1 &lt;-- GSLOTD</p> <p>Solution: The response payload is larger than the allocated memory space, causing memory corruption when data is copied. The fix is to allow the correct length during copy of the response.</p> <p>Customer Impact: This problem occurs when FM is in the fabric with multiple switch views open and a fabric slot information request is performed.</p> <p>Probability: Low</p> <p>Service Request# RQST00000037753</p> <p>Reported in Release: V4.2.2</p>
DEFECT000057631	High	<p>Summary: DCC policy is not enforced properly after failover/reboot/fastboot.</p> <p>Symptom: DCC_POLICY is not enforced if only 1 CP is rebooted or fastbooted during either cold or warm recovery. Rebooting or fastbooting both CPs does not show any error.</p> <p>Solution: DCC policies were not being converted from file to shared memory on standby. The solution is to update the shared memory after the failover before attempting to push the DCC policies down to the kernel, such that the policies are converted from file to shared memory again when the switch becomes active.</p> <p>Workaround: Issue a subsequent secpolicyactivate after the reboot/fastboot completes to reestablish the DCC policy.</p> <p>Customer Impact: The DCC policy is incorrect, and the user will have to establish the correct one by issuing a subsequent secpolicyactivate after the reboot/fastboot completes.</p> <p>Probability: High</p> <p>Reported in Release: V4.4.0</p>

Defects Closed in Fabric OS v5.0.1a		
Defect ID	Severity	Description
DEFECT000057675	High	<p>Summary: CUP Port returns F-Reject not available to PLOGI</p> <p>Symptom: CUP Port goes offline and not able to vary back online</p> <p>Solution: Fix is to cache the 'ficu_licensed' during warm recovery instead of relying on SW_ONLINE SCN.</p> <p>Probability: Medium</p> <p>Reported in Release: V5.0.1</p>
DEFECT000058208	High	<p>Summary: A memory leak causes out of memory (OOM) kill of evmd if Fabric Manager opens sessions with event listener through API during end-to-end performance monitoring.</p> <p>Symptom: Observe [EVMD-5000] when FM open event listener and switch panic with Out of Memory: Killed process 653 (evmd0). VM size = 86684 KB, Runtime = 84379 minutes, CPU time = 1 sec.</p> <p>Solution: When Fabric Manager (FM) performs end-to-end performance monitoring through a FOS 4.4 switch, an event session is being opened by the API library every time a new API session is created by FM. There is a 1/2 k byte leak for every session opened.</p> <p>Workaround: Do not enable any periodically scheduled API based operations from Fabric Manager (for example: PM/APM, Change Management snapshots). Turn off APM in Fabric Manager by simply selecting "Off" radio button and "Save." Turn off change management by clicking "Manage Profiles" menu item (Tools -&gt; Change Management -&gt; Manage Profiles menu in Fabric Manager) and edit profiles.</p> <p>Customer Impact: With FM opening event session through API, a small amount of memory leak occurs for that session. This happens between FM4.2/4.4 and FOS4.4 when FM pulls end-to-end performance data or performs change management periodically. This defect does not apply to releases prior to FOS4.4.0.</p> <p>Service Request# RQST00000038385</p> <p>Reported in Release: V4.4.0</p>

Defects Closed in Fabric OS v5.0.1a		
Defect ID	Severity	Description
DEFECT000058340	High	<p>Summary: Channel errors on FICON Channels during concurrent firmware install.</p> <p>Symptom: Many channel errors during firmware upgrade</p> <p>Solution: "Inconsistent FICON CUP filter setup" problem was encountered. This is one of the two known Zoning/Filtering problems. The fixes for these two zoning/filtering problems are in some common code areas and should be fixed together: 1) hafailover generates "Inconsistent FICON CUP filter setup" messages for all the offline ports. 2) I/O stops when a perfAddUserMonitor command is set up.</p> <p>Workaround: Don't do a firmware install while traffic is running through the switch.</p> <p>Customer Impact: High volume of error messages and possible job appends.</p> <p>Probability: High</p> <p>Reported in Release: V5.0.1</p>
DEFECT000058587	High	<p>Summary: SW3016 "configsave -restore" function no longer works because "configsave -factory" is broken</p> <p>Symptom: The SW3016 Restore Factory Configuration operation will not work properly because of a problem in the algorithm that is used to save the factory configuration at the time the unit is manufactured.</p> <p>Solution: The function responsible for saving the factory defaults has been updated to handle a new format of the control file.</p> <p>Customer Impact: This defect does not affect SW3016 units already in the field. This defect only affects future units that would have been manufactured using 5.0.1 as the base software release. SW3016 units manufactured with 5.0.1 do not successfully save the factory values for the configuration files.</p> <p>Probability: High</p> <p>Reported in Release: V5.0.1</p>

Defects Closed in Fabric OS v5.0.1a		
Defect ID	Severity	Description
DEFECT000058824	High	<p>Summary: Found memory leak in proxy switch ARR when target switch does not have IP connectivity.</p> <p>Symptom: the arr process virtual memory usage will slowly increase and eventually take up memory and eventually cause the switch to reboot</p> <p>Solution: The fix was to free memory that previously had not been freed</p> <p>Probability: Low</p> <p>Reported in Release: V4.4.0</p>
DEFECT000058864	High	<p>Summary: Interface Control Checks when the PCDM Matrix is changed with traffic running</p> <p>Symptom: Interface Control Checks running I/O Ops. program to modify the PCDM Matrix.</p> <p>Solution: When PDCM is changed, NS or Zoning would reprogram the affected port's CAM. The current code misses disable zoning before reprogramming. This would cause IO traffic disruption when CAM is reprogrammed. The fix is to disable zoning before reprogramming ports and after all the affected ports are reprogrammed enable the zoning. Fix is done in both Zoning and NS areas.</p> <p>Customer Impact: Intermittent loss of frames giving Interface Control Checks in FICON environment.</p> <p>Probability: High</p> <p>Reported in Release: V5.0.1</p>
DEFECT000059324	High	<p>Summary: SW4012 returns wrong value for SNMP cpqRackNetConnectorModel field</p> <p>Symptom: SNMP request for cpqRackNetConnectorModel will see value "BRD0000CA" instead of "Brocade 4Gb SAN Switch."</p> <p>Solution: Change string value to "Brocade 4Gb SAN Switch."</p> <p>Customer Impact: Without this change, customer will see "BRD0000CA" instead of "Brocade 4Gb SAN Switch for HP p-Class BladeSystem;" however, system will function correctly in all other respects</p> <p>Reported in Release: V5.0.1</p>

Defects Closed in Fabric OS v5.0.1a		
Defect ID	Severity	Description
DEFECT000057932	Medium	<p>Summary: Refresh operations in Web Tools Switch View, Name Server, Switch Events, and Fabric Events not reflected in "Last Updated" status messages</p> <p>Symptom: The timestamp updates automatically at 60-second intervals, irrespective of user- or system-generated refresh events, when every invocation of a refresh operation, either manual or timed auto-refresh, should update the timestamp displayed in the "Last Updated" status message.</p> <p>Solution: Correct a merge error.</p> <p>Customer Impact: Inaccurate or misleading information about the last refresh time is displayed for Name Server, Switch Events, and Fabric Events.</p> <p>Probability: High</p> <p>Reported in Release: V5.0.1</p>
DEFECT000058419	Medium	<p>Summary: Firmware upgrade from 5.0.1 'main' to GA build fails, Standby CP not accessible for upgrade</p> <p>Symptom: Customer cannot upgrade the firmware to GA release v5.0.1 without doing a "firmwareupgrade -s" on each CP which upgrades the primary partition first not the secondary or backup partition. Also, when using the "-s" option, the remote CP will upgrade the primary partition first.</p> <p>Solution: Modify standby CP logic to update our packet filter when IP address is changed.</p> <p>Customer Impact: After changing the IP address of the standby CP, the CP will lose external IP access until it's rebooted or becomes the active CP due to HA failover.</p> <p>Service Request# RQST00000038765</p> <p>Reported in Release: V5.0.1</p>
DEFECT000059227	Low	<p>Summary: RNIDS vanish on display</p> <p>Symptom: Missing RNIDS on Ports display if FMSMode is disabled on the switch</p> <p>Solution: FOS must return the RNIDS when the FMSMODE is disabled on the switch.</p> <p>Customer Impact: FOS will fail to return RNID information after the FMSMODE is disabled, but FICON devices continue to operate on the switch.</p> <p>Reported in Release: V5.0.0</p>