



# Brocade Fabric OS v5.0.1a Release Notes v1.0

July 29, 2005

## *Document History*

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v5.0.1a Release Notes v1.0	First release.	July 29, 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.....	4
Overview .....	4
SilkWorm 48000.....	4
SilkWorm 200E .....	5
Supported Switches .....	5
Firmware Upgrades .....	5
Technical Support.....	6
Standards Compliance .....	6
OS Requirements .....	7
Important Notes .....	7
Upgrading and Installing FC4-16 and FC4-32 Blades.....	7
General .....	7
Merging Zones.....	10
Web Tools .....	10
Other Notes.....	12
Documentation Updates.....	15
Fabric OS Administrator’s Guide .....	15
Fabric OS Command Reference Manual .....	19
Fabric OS MIB Reference Manual .....	23
Fabric OS System Error Message Reference Manual.....	24
Fabric Watch User’s Guide .....	25
Secure Fabric OS Administrator’s Guide .....	25
SilkWorm 3250/3850 Hardware Reference Manual.....	26
SilkWorm 4100 Hardware Reference Manual.....	26
SilkWorm 12000 Hardware Reference Manual.....	27
SilkWorm 200E Hardware Reference Manual .....	28
SilkWorm 24000 Hardware Reference Manual.....	29
SilkWorm 48000 Hardware Reference Manual.....	30
SilkWorm Director Blade Support Notes .....	30
Web Tools Administrator’s Guide.....	31
Closed Defects in Fabric OS v5.0.1a.....	32

## About This Release

Fabric OS v5.0.1a is a patch release containing fixes to a number of defects found since the release of Fabric OS v5.0.1. Aside from these changes, this patch release includes the same feature set as Fabric OS v5.0.1.

## Overview

Brocade Fabric OS v5.0.1 supports two new 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 Advanced Zoning—Segments a fabric into virtual private 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.

**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 that 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 can stand up to any mission-critical test and offer significant business and performance advantages to small- to medium-size businesses as they develop and grow.

## **Supported Switches**

Fabric OS v5.0.1 adds support for the SilkWorm 48000 and SilkWorm 200E to existing support for the SilkWorm 3014, 3016, 4012, 3250, 3850, 3900, 4100, 12000, and 24000.

## **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 support 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 switch—Side of switch module
- SilkWorm 200E—Nonport side of the chassis
- SilkWorm 3250, 3850, and 3900 switches—Bottom of the chassis.
- SilkWorm 4100 switches—On the switch ID pull-out tab located on the port side and on the inside of the chassis, near the 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 v5.0.1 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 Website:

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

	General Compatibility	With Secure Fabric OS Enabled	Recommended Software Versions
SilkWorm 4012	v5.0.0 or later	v5.0.0 or later	v5.0.1 once released
SilkWorm 2000 Series	v2.6.1 or later	v2.6.1 or later	v2.6.2d
SilkWorm 3200 & 3800	v3.1.0 or later	v3.1.2 or later	v3.2.0a
SilkWorm 3016, 3250, 3850, 3900, 12000, 24000	v4.1.0 or later	v4.2.0 or later	v5.0.1 or later
SilkWorm 200E & 48000	v5.0.1 or later	v5.0.1 or later	v5.0.1 or later
SilkWorm 4100	v4.4.0b or later	v4.4.0b or later	v5.0.1 or later
Fabric Manager	3.0.2c or later	3.0.2c or later	5.0.0 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 on 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 will differ – largely to support the proper selection of platform-specific RPMs for the two different blades. When one issues **switchShow** from an active SilkWorm 24000 CP blade, and then issues the same command when the SilkWorm 48000 CP blade is the active CP blade, **switchShow** will show two different switchType values. The switch type, however, tracks with the active CP blade – just as it does for SilkWorm 24000 and SilkWorm 12000 switches.

Note that 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 won't be able to 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.
- Device-based path selection (paths are chosen based on SID and DID). FICON implementations require this policy on the SilkWorm 4100 and chassis containing FC4 blades (see Option 5 in the table below).
- Exchange-based path selection (paths are chosen based on SID, DID, and OXID).

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. If so, you can select:

- Device-based path selection (paths are chosen based on SID and DID). FICON implementations require this policy on the SilkWorm 4100 and chassis containing FC4 blades (see Option 5 in the table below).
- Exchange-based path selection (paths are chosen based on SID, DID, and OXID).

For all other modes, you must use the port-based path selection (paths are chosen based on ingress port and destination only). This also includes user-configured paths.

### SilkWorm Chassis Option Descriptions

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

## 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 = SW24000 CP blade

CP4 = SW48000 CP blade

FC2-16 = 2G, 16-port blade

FC4-16 = 4G, 16-port blade

FC4-32 = 4G, 32-port blade

12K = SW12000-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 SW200E ports-on-demand (POD) features, which delivers 8, 12, or 16 ports in a 1U form factor.

## Reliability

This release of the 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 (i.e. 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, 2650 ports with 50 domains.

## 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 **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 15](#) 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
<p><b>Firmware:</b> Fabric OS v3.1.0+, v4.1.0+, or v5.0.1+</p> <p><b>Operating System:</b> Any supported operating system (with supported browser)</p> <p><b>Browser:</b> Any supported browser (on supported operating system)</p>	<p><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.</p> <p>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.</p> <p><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.</p>

Launch Switch Environment	Problems
<p><b>Firmware:</b> Fabric OS v2.6.x</p> <p><b>Operating System:</b> Solaris</p> <p><b>Browser:</b> Mozilla</p>	<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>
<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</p> <p><b>Operating System:</b> Solaris</p> <p><b>Browser:</b> Mozilla</p>	<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>
<p><b>Firmware:</b> Version <i>prior</i> to Fabric OS v2.6.2, v3.1.2, or v4.2.0a</p> <p><b>Operating System:</b> Any supported operating system (with supported browser)</p> <p><b>Browser:</b> Any supported browser (on supported operating system)</p>	<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>
<p><b>Firmware:</b> Version <i>prior</i> to Fabric OS v4.4.0</p> <p><b>Operating System:</b> Any supported operating system (with supported browser)</p> <p><b>Browser:</b> Any supported browser (on supported operating system)</p>	<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
<p><b>Firmware:</b> Version <i>prior</i> to Fabric OS v4.4.0</p> <p><b>Operating System:</b> Any supported operating system (with supported browser)</p> <p><b>Browser:</b> Any supported browser (on supported operating system)</p>	<p><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.</p> <p><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.</p>
<p><b>Firmware:</b> Version <i>prior</i> to Fabric OS v2.6.2, v3.1.2, or v4.2.0</p> <p><b>Operating System:</b> Solaris</p> <p><b>Browser:</b> Netscape</p>	<p><b>Issue:</b> Any switches running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later are unsupported through Netscape.</p> <p><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.</p>
<p><b>Firmware:</b> Version <i>prior</i> to Fabric OS v2.6.1, v3.0.x, or v4.0.x</p> <p><b>Operating System:</b> Windows</p> <p><b>Browser:</b> Internet Explorer</p>	<p><b>Issue:</b> When you are trying to run Fabric View with a large fabric, the browser might crash.</p> <p><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).</p> <p>Use a launch switch with v.2.6.2, v3.1.x, or v4.1.x or later.</p>
<p><b>Firmware:</b> Fabric OS v5.0.1+</p> <p><b>Operating System:</b> Any supported operating system (with supported browser)</p> <p><b>Browser:</b> Internet Explorer and Mozilla</p>	<p><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.</p> <p><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.</p> <p>For Mozilla, follow the Mozilla Java plug-in installation instructions to install Java v1.4.2_06.</p>

## Other Notes

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

SilkWorm 4012	Description
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.

SilkWorm 48000	Description
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	<p>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</p>
PID 2 support for the SilkWorm 48000	<p>The additional ports (128-258) on a SW48000 require updates to certain Fabric OS releases in a special circumstance, that is, running PID-2 Format with a SW48000 in the fabric.</p> <p>Minimum Fabric OS version required: 2.6.2d, 3.2.0a, 4.4.0d</p>
Power cycling	<p>A minimum of 15 seconds between power cycles is required.</p>
Proxy switches	<p>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.</p>
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 a special circumstances, that is, Secure Fabric OS fabric with a SW48000 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 hardware updates	<p>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.</p>

Fabric OS Area	Description												
Advanced Performance Monitor	<p>Adding Advanced Performance Monitor (perfAddUserMonitor) 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 perfAddUserMonitor 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: backporttest	<p>Backport test will only pass in a) a pure SilkWorm 24000 system or b) a SilkWorm 24000 system with no Electron blades and under Option 5.</p> <p>For all other configurations, use the minicycle test instead.</p>												
Diagnostics: spinsilk	<table border="0"> <thead> <tr> <th data-bbox="488 636 1224 667"><b>Configuration</b></th> <th data-bbox="1224 636 1367 667"><b>spinsilk</b></th> </tr> </thead> <tbody> <tr> <td data-bbox="488 680 1224 714">Pure SilkWorm 24000 (only CP2 &amp; FC-16)</td> <td data-bbox="1224 680 1367 714">Pass</td> </tr> <tr> <td data-bbox="488 726 1224 760">Mixed SilkWorm 24000 (with either CP4 or FC4-16 blades inserted)</td> <td data-bbox="1224 726 1367 760">Fail</td> </tr> <tr> <td data-bbox="488 772 1224 806">Pure SilkWorm 48000, option 1</td> <td data-bbox="1224 772 1367 806">Fail</td> </tr> <tr> <td data-bbox="488 819 1224 852">Pure SilkWorm 48000, option 5 (w/o FC4-16)</td> <td data-bbox="1224 819 1367 852">Pass</td> </tr> <tr> <td data-bbox="488 865 1224 898">Pure SilkWorm 48000, option 5 (w/FC4-16)</td> <td data-bbox="1224 865 1367 898">Pass</td> </tr> </tbody> </table> <p>Pure SilkWorm 48000 is CP4 and FC4-16 only. The spinsilk command will fail in a mixed SilkWorm 24000 system and in a pure SilkWorm 48000system with configuration option 1.</p> <p>For all other configurations, use the minicycle test instead.</p>	<b>Configuration</b>	<b>spinsilk</b>	Pure SilkWorm 24000 (only CP2 & FC-16)	Pass	Mixed SilkWorm 24000 (with either CP4 or FC4-16 blades inserted)	Fail	Pure SilkWorm 48000, option 1	Fail	Pure SilkWorm 48000, option 5 (w/o FC4-16)	Pass	Pure SilkWorm 48000, option 5 (w/FC4-16)	Pass
<b>Configuration</b>	<b>spinsilk</b>												
Pure SilkWorm 24000 (only CP2 & FC-16)	Pass												
Mixed SilkWorm 24000 (with either CP4 or FC4-16 blades inserted)	Fail												
Pure SilkWorm 48000, option 1	Fail												
Pure SilkWorm 48000, option 5 (w/o FC4-16)	Pass												
Pure SilkWorm 48000, option 5 (w/FC4-16)	Pass												
Nondefault operands	<p><b>IMPORTANT:</b> The use of nondefault operands for diagnostic commands is recommended for advanced users and technical support only.</p>												
SNMP	<p>Starting with the FOS 4.4.0 release, Brocade added the ability to enable traps on a more granular level. After an upgrade, the snmpMibCapSet 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.</p>												
Upgrade	<p>Fabric OS v5.0.0 is superceeded by version v5.0.1, and you are strongly encouraged to upgrade to v5.0.1.</p> <p>Also, earlier releases of v5.0.0 might not support hot code activation. Therefore, when you upgrade to v5.0.1, you must reboot the switch for the new version to take affect.</p>												
Upgrading / downgrading	<p>When considering an upgrade to a later Fabric OS release the user should save the zone databse 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.</p>												

Fabric OS Area	Description
Upgrading to Fabric OS v4.2.0 to v5.0.1	<p>The SW and FA traps in pre-Fabric OS v4.4 code were turned on and off as a group; and it wasn't possible to set individual SW or FA traps. In v4.4 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 <code>snmpmibcapset</code> or the newer <code>snmpconfig</code> command to turn the desired traps on individually.</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>

## Documentation Updates

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

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 translative 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 translative 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 5.0.1 to 4.2.2 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 device-based path selection:

- Device-based path selection

SilkWorm 200E, 4012, 4100, and 48000 (using configuration option 5).

If there are devices in your fabric that cannot accommodate out-of-order exchanges, then you should use the device-based policy. Brocade recommends that you also use device-based routing for FICON environments.

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 FOS 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</b> <b>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</b> <b>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</b> <b>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

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

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>a</sup>	5 (26)	2.5 km	10 km	5 km	2 km	All	No
LE	11	16	10 km	n/a	10 km	5 km	v3.x, v4.x	No

a. 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)	2.5 km	10 km	5 km	2 km	All	No
LE	11	16	10 km	n/a	5 km	5 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:

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

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.

## Fabric OS Command Reference Manual

(Publication number 53-0000519-10)

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

- **diagEsdPorts**
- **itemList**
- **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.”

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 2-345, 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”.

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 **snmplibcapset** or **snmplibconfig** 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.

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.
FcpVersion	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 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)

The following messages were added after the document publication.

### 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

## 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 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 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 reenble 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:

“The left power connector provides power to the power supplies in power supply bays #1 and #3 (color-coded blue). The right power connector provides power to the power supplies in power supply bays #2 and #4 (color-coded yellow).”

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: xxxxx
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 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

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 2-8, “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 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"

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)

It should be replaced 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.

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.

## 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>