Brocade Fabric OS v4.4.0c Release Notes_v1.0

April 7, 2005

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v4.4.0c Release Notes v1.0	First release.	April 7, 2005

TABLE OF CONTENTS

About This Release

Fabric OS v4.4.0c is a patch release containing fixes to a number of defects found since the release of Fabric OS v4.4.0b. Aside from these changes, this patch release includes the same feature set as the Fabric OS v4.4.0 release.

Overview

Fabric OS version 4.4.0c has the same features as Fabric OS v4.4.0, including significant enhancements in the areas of Fibre Channel long-distance support, scalability, and manageability. In addition, several improvements since the release of Fabric OS version 4.2.0 have been incorporated in this release. Major new features include:

- Support for the SilkWorm 4100 and the SilkWorm Multiprotocol Router Model AP7420
- Greater than two-fold increase in Brocade Extended Fabrics support:
    - SilkWorm 3250, 3850, and 24000 support distances up to 200 km at 1 Gbit/sec and 100 km at 2 Gbit/sec.
    - SilkWorm 4100 supports distances up to 500 km at 1Gbit/sec and 100 km at 4 Gbit/sec.
- Trunking over Brocade Extended Fabrics:
    - SilkWorm 3000-series, 12000, and 24000 support two links of up to 50 km at 2 Gbit/sec and four links of 10 km at 2Gbit/sec.
    - SilkWorm 4100 supports three links of up to 250 km at 2Gbit/sec or 100 km at 4 Gbit/sec.
- Increased scalability to 2560 ports and 50 domains
- Ports on Demand (POD) for instant scalability via license keys
- Fabric Watch improvements:
    - Improved notification
    - Switch health reports
- Standardized messaging: for example, including information such as time stamp, message number, severity, and switch name for all system messages
- Updated security enhancements:
    - SSH
    - RADIUS
    - DH-CHAP authentication
- Fabric Watch and Web Tools usability enhancements
- FICON®/CUP support for SilkWorm 3900, 12000, and 24000

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

Supported Switches

Fabric OS v4.4.0c supports SilkWorm 3016, 3250, 3850, 3900, and 4100 switches and SilkWorm 12000 and 24000 directors.

Standards Compliance

Brocade Fabric OS v4.4.0c conforms to the following Fibre Channel Standards in a manner consistent with accepted engineering practices and procedures. In certain cases, Brocade might add proprietary supplemental functions to

those specified in the standards. Brocade verifies conformance with Fibre Channels Standards by subjecting its switches to SANmark Conformance Tests developed by the Fibre Channel Industry Association. Brocade switches have earned the SANmark logo, indicating such conformance. SANmark is a limited testing program and does not test all standards or all aspects of standards. For a list of standards conformance, visit the following Brocade web site:

http://www.brocade.com/sanstandards

Important Notes

This section lists information you should be aware of when running Fabric OS v4.4.0c.

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.

OS Requirements

The following table summarizes the versions of Brocade software that are supported in conjunction with 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.

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

Effective September 2004, Fabric OS v2.6.0x and earlier, v3.0.2x and earlier, and v4.0.2x and earlier reached their end-of-life and are no longer supported.

	SilkWorm 2000 Series	**SilkWorm 3200 & 3800**	**SilkWorm 3016, 3250, 3850, 3900, 12000, & 24000** [1]	**SilkWorm 4100** [2]	**Fabric Manager**
General compatibility	v2.6.1 or later	v3.1.0 or later	v4.1.0 or later	v4.4.0b or later	3.0.2c or later
With Secure Fabric OS enabled	v2.6.1 or later	v3.1.2 or later	v4.2.0 or later	v4.4.0b or later	3.0.2c or later
Recommended software versions	v2.6.2	v3.2.0	v4.4.0	v4.4.0b or later	4.1.1 or later

1 SilkWorm 3016 is supported by Fabric OS v4.2.1x and v4.4.0b or later.
SilkWorm 3250, 3850, and 24000 are supported by Fabric OS v4.2.0 or later.
SilkWorm 3250, 3850, and 24000 are supported by Fabric Manager 4.1.1 or later.
SilkWorm 3900 is supported by Fabric OS v4.1.0 or later.

2 SilkWorm 4100 is supported by Fabric Manager 4.4.0 or later.

General

The major features incorporated in Fabric OS v4.4.0x are summarized in the following table.

Category	Feature	Release
SilkWorm 24000 Enhancements	Mixed-blade support for the SilkWorm 24000: ▪ Two-domain support ▪ Mixed SilkWorm 12000 and SilkWorm 24000 port blades	v4.4.0
SilkWorm 4100 Platform Support	Ports on Demand (16, 24, or 32 ports) Condor ASIC support: ▪ 1, 2 and 4 Gbit/sec automatic speed negotiation ▪ 4 Gbit/sec trunks ▪ 8-port trunk groups for up to 32 Gbit/sec trunks ▪ More distance options (see below) ▪ Dynamic path selection (DPS) with the exchange-based and device-based polices. The SilkWorm 4100 uses the frame information to determine the routing paths dynamically. Port-based policy is independent of the traffic pattern. ▪ Network boot using TFTP	v4.4.0
Reliability	Compact flash capacity monitoring	v4.4.0
Manageability	Advanced Performance Monitoring - ISL monitoring (CLI only) Fabric Watch enhancements Export performance data FDMI host name support	v3.2.0, v4.4.0 v3.2.0, v4.4.0 v3.2.0, v4.4.0 v4.4.0
RAS	New logging and tracing infrastructure Enhanced error message format **supportShow** command enhancements New **supportSave** command	v4.4.0 v4.4.0 v4.4.0 v4.4.0
Security-Related	RADIUS support Multiple user accounts SSL/HTTPS support SNMPv3 support DH-CHAP authentication (switch-switch) SAN gateway security	v3.2.0, v4.4.0 v3.2.0, v4.4.0 v4.4.0 v4.4.0 v3.2.0, v4.4.0 v3.2.0, v4.4.0

<table>
<tr><th>Category</th><th>Feature</th><th>Release</th></tr>
<tr><td>Long-Distance Enhancements</td><td>
200 km at 1 Gbit/sec or 100 km at 2 Gbit/sec (SilkWorm 3250, 3850, 24000, Bloom II ASIC-based switches)
500 km at 1 Gbit/sec, 250 km at 2 Gbit/sec, or 100 km at 4 Gbit/sec (SilkWorm 4100, Condor ASIC-based switches)
Trunking over Brocade Extended Fabrics (SilkWorm 3xxx, 12000, 24000, and all Bloom ASIC-based platforms, with v4.4.0) is only supported at 2 Gbit/sec, as follows:

four links at 10 km @ 2 Gbit/sec per trunk group
three links at 25 km @ 2 Gbit/sec per trunk group
two links at 50 km @ 2 Gbit/sec per trunk group

Buffer-limited ports
Enhanced trunking support with the Bloom ASIC is summarized below:
<table>
<tr><th>Distance</th><th>Number of 2-Gbit/sec ports (Bloom to Bloom)</th></tr>
<tr><td>LE 10 km</td><td>4 (one 4-port trunk)</td></tr>
<tr><td>L0.5 25 km</td><td>3 (one 3-port trunk)</td></tr>
<tr><td>L1 50 km</td><td>1 (one 2-port trunk)</td></tr>
<tr><td>L2 100 km</td><td>0</td></tr>
<tr><td>LD 200 km</td><td>0</td></tr>
<tr><td>LD 250 km</td><td>0</td></tr>
<tr><td>LD 500 km</td><td>0</td></tr>
</table>
Enhanced trunking support with the Condor ASIC is summarized below:
<table>
<tr><th>Distance</th><th>Number of 2-Gbit/sec ports or trunks (Condor to Condor)</th><th>Number of 4-Gbit/sec ports (Condor to Condor)</th></tr>
<tr><td>LE 10 km</td><td>32 (four 8-port trunks)</td><td>32 (four 8-port trunks)</td></tr>
<tr><td>L0.5 25 km</td><td>32 (four 8-port trunks)</td><td>15 (one 8-port trunk)</td></tr>
<tr><td>L1 50 km</td><td>15 (one 8-port trunk)</td><td>7 (one 7-port trunk)</td></tr>
<tr><td>L2 100 km</td><td>7 (one 7-port trunk)</td><td>3 (one 3-port trunk)</td></tr>
<tr><td>LD 200 km</td><td>3 (one 3-port trunk)</td><td>0</td></tr>
<tr><td>LD 250 km</td><td>3 (one 3-port trunk)</td><td>0</td></tr>
<tr><td>LD 500 km</td><td>0</td><td>0</td></tr>
</table>
</td><td>
v4.4.0
v4.4.0
v4.4.0
v4.4.0
v4.4.0
v4.4.0
</td></tr>
</table>

Category	Feature	Release
MPRS Enhancements	Max hop count (SilkWorm Multiprotocol Router Model AP7420) – CLI only	v3.2.0, v4.4.0
	WAN_TOV (FC Router) – CLI only	v3.2.0, v4.4.0
Scalability	Supports 1280 total ports and 34 domains with or without security enabled.	v3.2.0, v4.4.0
	Supports 2560 total ports and 50 domains in a fabric consisting of switches with 32 ports or more running Fabric OS v4.4.0.	v4.4.0
Usability Improvements + RFEs	Security Management – enables/merges secure fabrics (Fabric Manager only)	v3.2.0, v4.4.0
	Web Tools and Fabric Manager usability improvements	v3.2.0, v4.4.0
	Enhanced Fabric Watch support	v3.2.0, v4.4.0

Advanced Web Tools Updates

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

  http://ftp27f.newaol.com/pub/mozilla.org/mozilla/releases/mozilla1.6/README

- **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 additionally supported browsers, operating systems, and Java Plug-ins introduce the following limitations when using mixed OS versions in Advanced Web Tools v4.4.0.

Launch Switch Environment	Problems
Firmware: Fabric OS v3.1+ or v4.1+ **Operating System**: any supported operating system (with supported browser) **Browser**: any supported browser (on supported operating system)	**Issue**: When viewing the topology from Web Tools, if your initial login was a v3.1+ or v4.1+ 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+ and v4.1.0+ includes a Print button in the Fabric Topology window; earlier versions do not. **Workaround**: If the Fabric Topology window does not display a Print button, you can right-click anywhere inside the window and select Print from the popup menu.

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

Launch Switch Environment	Problems
Firmware: version *prior* to Fabric OS v4.4.0 **Operating System:** any supported operating system (with supported browser) **Browser**: any supported browser (on supported operating system)	**Issue:** When trying to perform end-to-end monitoring (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. **Workaround:** 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.
Firmware: version *prior* to Fabric OS v4.4.0 **Operating System:** any supported operating system (with supported browser) **Browser:** any supported browser (on supported operating system)	**Issue:** 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. **Workaround:** 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.
Firmware: version *prior* to Fabric OS v2.6.2, v3.1.2, or v4.2.0 **Operating System:** Solaris **Browser:** Netscape	**Issue**: Any switches running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later are unsupported through Netscape. **Workaround**: The Netscape browser is not supported by Web Tools for switches running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later. Use the Mozilla browser v1.6 to manage all of your switches from a Solaris operating system.
Firmware: version *prior* to Fabric OS v2.6.1, v3.0.x, or v4.0.x **Operating System:** Windows **Browser:** Internet Explorer	**Issue**: When you are trying to run Fabric View with a large fabric, the browser might crash. **Workaround**: 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 and later.

Other Notes

This table lists other important information you should be aware of regarding Fabric OS v4.4.0 and the SilkWorm 3016, 3250, 3850, 3900, 4100, 12000, and 24000 platforms.

<table>
<tr><th>SilkWorm 4100</th><th>Description</th></tr>
<tr><td>SWL and LWL SFP module release mechanism</td><td>
SilkWorm 4100 uses an octal-style SFP cage that places SFPs in close proximity. As a result of the physical space limitation between the SFPs, Brocade requires the use of approved SFP modules only.

Using an approved SFP module eliminates issues associated with the fit and removal of the module. Specifically, SFPs with wide bail latch mechanisms that are not flush with the body of the SFP or SFPs with “push-tab” removal mechanisms might prevent the proper insertion or removal of the SFP module. Consult the Brocade compatibility matrix for the appropriate SFPs.

At the time of release, the following SFPs were certified compatible with the SilkWorm 4100 switch.
<table>
<tr><th>2 Gbit/sec Media</th><th>Type</th><th>Manufacturer</th><th>Manufacturer’s Part Number</th></tr>
<tr><td>SWL</td><td>Digital Diagnostics</td><td>Finisar</td><td>FTRJ-8519P1BNL-B1</td></tr>
<tr><td>SWL</td><td>Digital Diagnostics</td><td>Infineon</td><td>V23848-M305-C56R</td></tr>
<tr><td>LWL</td><td>Digital Diagnostics</td><td>Finisar</td><td>FTRJ1319P1BTL-B1</td></tr>
<tr><td>ELWL (40 km)</td><td></td><td>Finisar</td><td>FTRJ-1419P1BCL</td></tr>
<tr><th>4 Gbit/sec Media</th><th>Type</th><th>Manufacturer</th><th>Manufacturer’s Part Number</th></tr>
<tr><td>SWL</td><td>Digital Diagnostics</td><td>Finisar</td><td>FTRJ-8524P2-BNV</td></tr>
<tr><td>SWL</td><td>Digital Diagnostics</td><td>Agilent</td><td>AFBR-57R5AP</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>SilkWorm 4100</th><th>Description</th></tr>
<tr><td>CWDM module and SFP</td><td>Course Wave Division Multiplexing (CWDM) media, providing up to 100 km distance support, has been qualified for use with SilkWorm 24000, 12000, 4100, 3900, 3800, 3850, and 3250.
<table>
<tr><th>2 Gbit/sec CWDM</th><th>Manufacturer</th><th>Manufacturer's Part Number</th></tr>
<tr><td>CWDM Mux/Demux Module - 8 port</td><td>Finisar</td><td>FWS-MUX-DEMUX-8</td></tr>
<tr><td>CWDM Mux/Demux Module - 4 port</td><td>Infineon</td><td>FWS-MUX-DEMUX-4</td></tr>
<tr><td>2G SFP 1470 nm (Gray)</td><td>Finisar</td><td>FWDM-1621-7D-47</td></tr>
<tr><td>2G SFP 1490 nm (Violet)</td><td>Finisar</td><td>FWDM-1621-7D-49</td></tr>
<tr><td>2G SFP 1510 nm (Blue)</td><td>Finisar</td><td>FWDM-1621-7D-51</td></tr>
<tr><td>2G SFP 1530 nm (Green)</td><td>Finisar</td><td>FWDM-1621-7D-53</td></tr>
<tr><td>2G SFP 1550 nm (Yellow)</td><td>Finisar</td><td>FWDM-1621-7D-55</td></tr>
<tr><td>2G SFP 1570 nm (Orange)</td><td>Finisar</td><td>FWDM-1621-7D-57</td></tr>
<tr><td>2G SFP 1590 nm (Red)</td><td>Finisar</td><td>FWDM-1621-7D-59</td></tr>
<tr><td>2G SFP 1610 nm (Brown)</td><td>Finisar</td><td>FWDM-1621-7D-61</td></tr>
</table></td></tr>
<tr><td>LED, system status</td><td>The system status LED blink behavior in the SilkWorm 4100 is different from that of legacy SilkWorm switches. Legacy products blink system status with amber/off, amber/off. The SilkWorm 4100 blinks amber/green, amber/green. Refer to the appropriate hardware specification.</td></tr>
<tr><td>LED, system power</td><td>The system power LED behaves differently in the SilkWorm 4100 than in SilkWorm 3250 and 3850 switches. In SilkWorm 3250 and 3850 switches, it is solid amber when a power supply FRU has failed. In SilkWorm 4100, the system power LED remains green, and the system status LED will blink, indicating an error.</td></tr>
<tr><td>Fan, RPM reading</td><td>The RPM range can differ by as much as 1000 RPM from fan to fan, which is within Brocade specifications. At the lowest RPM, the cooling specification is met, and at the highest RPM, the acoustic specification is met. In other words, during normal operation, both the lowest and the highest observed fan speeds are within adequate margin of the acoustic and cooling specifications.</td></tr>
</table>

SilkWorm 4100	Description
WWN	Brocade has consumed the majority of WWN numbers originally allocated by the IEEE. This is due to the rate of switch shipments and the preallocation of World Wide Name (WWN) blocks to current and past switch products. The SilkWorm 4100 products use a new block of WWN numbers. In response, in addition to the current WWN, Brocade uses the IEEE Organizationally Unique Identifier (OUI) that was formally owned by Rhapsody Networks (now a part of Brocade Communications Systems, Inc.) for the new block of WWNs. The official IEEE OUI database has been updated to reflect this ownership change. Network and fabric management applications that rely on the use of the original Brocade OUI (00:60:69) to identify Brocade network elements must be updated from the IEEE Web site database (location below) to also include the new Brocade OUI (00:05:1E). **IEEE OUI and Company_id Assignments:** NEW 00-05-1E (hex) **Brocade** Communications Systems, Inc. 00051E (base 16) **Brocade** Communications Systems, Inc. 1745 Technology Drive San Jose CA 95110 UNITED STATES OLD 00-60-69 (hex) **BROCADE** COMMUNICATIONS SYSTEMS, Inc. 006069 (base 16) **BROCADE** COMMUNICATIONS SYSTEMS, Inc. 1901 GUADALUPE PKWY SAN JOSE CA 95131 UNITED STATES **IEEE list of public OUI assignments:** *http://standards.ieee.org/regauth/oui/index.shtml* In a management application using a Fabric Access version earlier than v3.0.2, SilkWorm 3250 and 3850 switches are displayed as Rhapsody switches.

SilkWorm 12000	Description
Power supply requirements	Customers reconfiguring SilkWorm 24000-only configurations by adding SilkWorm 12000 blades must ensure that all three power supply FRUs are installed, because SilkWorm 12000 blades have greater power requirements.

Fabric OS Area	Description
Compatibility	Sometimes in a mixed fabric of Fabric OS v4.x/v3.x/v2.x, fabric reconfiguration is caused by link reset on v3.x/v2.x. This only happens in a fabric containing Fabric OS v3.x versions released prior to v3.1.0 or Fabric OS v2.x versions released prior to v2.6.1 that are under heavy traffic or CPU-intensive operations such as large (50 KB) zone database propagation. Use the latest revision of code across all releases in a mixed fabric.
Ethernet port IP addresses	When a SilkWorm 12000 or 24000 fails over to its standby CP for any reason, the IP addresses for the two logical switches move to that CP blade's Ethernet port. This might cause informational ARP address reassignment messages to appear on other switches in the fabric. This is normal behavior, because the association between the IP addresses and MAC addresses has changed.
FICON®	When deploying the SilkWorm 24000 director in FICON environments and planning to use CUP in-band management, port 126 should not be used for I/O. Due to the addressing of CUP management frames, I/O on an area 7E address is not supported simultaneously with CUP management. This constraint does not apply to the SilkWorm 3900 or 12000.
FICON®, mixed-blade support	SilkWorm 24000 two-domain and mixed-blade configurations are not supported for FICON. FICON is supported for SilkWorm 24000 single-domain environments only.
Firmware download	During a firmware download, rebooting or power cycling the CPs could corrupt the compact flash. **CAUTION:** Do not attempt to power off the CP board during firmware download, to avoid high risk of corrupting your flash**.**

Firmware download	Fabric OS v4.1.x, v4.2.x, and v4.4.x nondisruptive firmware download allows for firmware downgrades and upgrades; however, you might see warning messages such as the following:
	
	`0x239 (fabos): Switch: 0, Info PDM-NOTFOUND, 4, File not found`
	
	`(/etc/fabos/mii.0.cfg)`
	
	These warnings can be ignored.

Firmware download, boot ROM	The boot ROM in Fabric OS v4.4.0 is automatically upgraded, by firmware download, to version 4.5.0 in all v4.x switches. After it has upgraded, the boot ROM will not downgrade should a firmware downgrade be performed. This boot ROM version supports a redundant boot ROM capability and redundant boot environments in the SilkWorm 4100.

Fabric OS Area	Description
Firmware upgrade	Fabric OS v4.x firmware upgrades include the *release.plist* file. There is a separate *release.plist* file for each platform, and the correct one is automatically selected when the **firmwareDownload** command is executed. Provide the full path name; do not attempt to locate the *release.plist* file in the top-level directory.
HA switch reboot failure	When a switch reboot or a failover occurs before POST is complete, the HA resynchronization is disrupted. HA will not resynchronize until POST completes. **CAUTION:** Allow POST to complete before performing a switch reboot or failover, to avoid disruptive failover**.**

Invalid gateway IP address error message	The user will see the following message on the console during startup when the Ethernet IP and gateway IP addresses are set to the defaults:
	`SIOCADDRT: Invalid argument`
	`.....`
	`ip.c:311:Invalid gateway IP address 0.0.0.0`
	This is a display issue only and does not affect the functionality of the switch.

IP addresses	**CAUTION:** Do not set a switch or CP IP address for the Ethernet interface to 0.0.0.0.
Logging, *syslog.conf*	As a result of multiple requests for enhancements, in Fabric OS v4.x, the "kern" facility for syslog is no longer supported. You must update all *syslog.conf* files to support “local7” facilities. There is a new **syslogdFacility** command to set the facility level that will be used.
Logging, Solaris syslogd local7 users	When using the new **syslogdFacility** command to set the local7 level, if an even-numbered facility level is selected (for example, 0, 2, 4, or 6), all Brocade switch Critical system messages will appear in the *odd-numbered .emerg* facility level file on the target Solaris systems: for example, *local6.emerg* will appear in *local7.emerg* if syslogd facility level 6 is selected. This behavior is not observed when selecting an odd-numbered facility level initially on the Brocade switch. The problem also does not occur on Linux server systems and is currently under investigation with Sun. The immediate workaround is to select an odd-numbered syslogd facility level when using the **syslogdFacility** command.
Logging, **supportFTP** command	When setting the automatic FTP IP address, user ID, password, and associated directory path for use with the **supportFtp** command, the parameters are not checked immediately for validity. Generate a manual trace dump to confirm the FTP transfer immediately. First, use **supportFtp** to set up FTP parameters. Next, use **traceFtp -e** to enable automatic transfer of the trace dumps. Finally, use the **traceDump -n** command to create a dump. Confirm that the FTP transfer was successful.

Fabric OS Area	Description
Logging, **chassisName** command	Run the **chassisName** command before upgrading to Fabric OS v4.4.0 so that any subsequent error messages related to the chassis and switch services will be logged correctly to the system error log. For further information, refer to the *Brocade Fabric OS Procedures Guide.*
Logging, **errClea**r command	All error logs are persistent in Fabric OS v4.x, so the use of the **errClear** command must be carefully considered, as all persistent errors (all messages) will be erased on v4.4.0 switches, as opposed to just those in local memory.
Ports on Demand	SilkWorm 4100 with a 16-port factory configuration requires Ports on Demand licenses in order to enable and use switch ports 16 thru 31.
rsh and rlogin	For Fabric OS v4.2.0 or later, programs rsh and rlogin are not supported. If you try to use an rsh or rlogin client, Fabric OS rejects the login attempt; however, because most rsh or rlogin clients continue to retry the login for several seconds before timing out, your system appears to hang. Secure connections are available via a secure shell (SSH).
Security, default password length	The initial login prompt for a switch accepts a maximum password length of eight characters. Any characters beyond the eighth are ignored.
Security, error counter	Telnet security errors that arrive in quick succession are recorded as a single violation by the telnet error counter. For example, a login error from a host whose IP address is 192.168.44.247 is logged as follows: `"Security violation: Login failure attempt via TELNET/SSH/RSH. IP Addr: 192.168.44.247"` If another login violation occurs immediately, the message remains the same and only the error counter is incremented.
Security, fabric segment	When two secure fabrics are continuously joined and separated while the CPU is under heavy load, the fabric will segment after approximately 30 cycles.
Security, FCS list	Adding switches to the FCS list does not automatically join the switches in a secure fabric. Add the switches to the FCS list of the new switches and the target fabric. Reset the version stamp to 0 and either reset the E_Ports or perform a switch disable and enable for the switches to join.
Security, HTTP policy	If HTTP_Policy is empty, you will not be able to log in and will receive a "Page not found" error. This is expected behavior for this policy.
Security, invalid certficate	Web Tools and Fabric OS are not consistent in how they report switch certificate status. Web Tools reports a valid certificate with extra characters appended to it as invalid, whereas Fabric OS accepts the certificate and allows a **secModeEnable** command to complete successfully.

Fabric OS Area	Description
Security, PKICERT utility, CSR syntax	Before using the PKICERT utility to prepare a certificate signing request (CSR), ensure that there are no spaces in the switch names of any switches in the fabric. The Web site that processes the CSRs and generates the digital certificates does not accept switch names containing spaces; any CSRs that do not conform to this requirement are rejected.
Security, PKICERT utility, installing certificates	PKICERT version 1.0.6 is the most current version of the PKICERT utility. When running the PKICERT utility to install switch certificates in a fabric that did not previously contain switch certificates and now includes a SilkWorm 24000 director, select the option to specify that certificates are installed on only those switches that do not currently contain certificates. SilkWorm 24000 directors are delivered with switch certificates preinstalled. Switches that were originally shipped with Fabric OS versions 2.5/3.0/4.0 and have never installed and enabled Secure Fabric OS do not have certificates installed. Should you need to reinstall switch certificates in a SilkWorm 24000 director, follow these guidelines: • The host running PKICERT 1.0.6 must be connected to a proxy switch running Fabric OS versions 2.6.2/3.1.2/4.2.0 or later. • All other non-SilkWorm 24000 switches in the fabric can run v2.6.1/v3.1/v4.1 or newer firmware.
Security, sectelnet	If you try to log in to a switch through a sectelnet client while that switch is in the process of either booting or shutting down, you might see the message, "Random number generation failed." The message is printed by the sectelnet client because the switch telnet service is not running (the service has either already been shut down, if the switch is shutting down, or is not yet established, if the switch is booting). If the switch is booting, wait a few seconds and try again.
Security, secure mode	If an upgrade from Fabric OS version 4.0.x to version 4.1.x/4.2.x is performed, followed by a downgrade to Fabric OS version 4.0.x and upgrade back to Fabric OS version 4.1.x/4.2.x, the switch password state is reset and will prompt the user for new secure-mode passwords. This does *not* apply to upgrades from v4.2.0 to v4.4.0.
Security, secure mode, passwd telnet	**CAUTION**: Using the "passwd" telnet command in secure mode to change the password results in all sessions using that password being logged out, including the session that changed the password. This is expected behavior. The session will terminate if you change the password in secure mode.
Security, SLAP fail counter and two switches	The SLAP counter is designed to work when all the switches in the fabric are in secure mode. All the switches in the fabric must be in secure mode for accurate SLAP statistics.

Fabric OS Area	Description
Security, SSH login	To properly connect SSH login, wait for secure mode to complete before rebooting or performing HA failover on the SilkWorm 12000 or 24000 directors. If secure mode is enabled and a reboot occurs before secure mode completes, SSH login will not connect and will go to the wrong MAC address because the active CP changes after an HA failover.
SilkWorm 12000 large fabric constraints	Extreme stress-test conditions in a large fabric configuration (over 2000 ports) show that the SilkWorm 12000 platform might ASSERT or PANIC in extremely rare circumstances, due to memory or processor limitations. Other SilkWorm platforms do not have these limitations. The stress-test cases that reveal these limitations on SilkWorm 12000 require all switches in a large fabric configuration to go through reboot, fastboot, or switch disable and enable repeatedly in quick succession over long periods of time. Subjected to these stress-test cases, the SilkWorm 12000 fails only rarely and only after long hours of testing. Under normal operating conditions, customers should not encounter these failures. Related defects: 48168, 49254
Support	Fabric OS v4.4.0 users should run the **supportSave** command instead of, or in addition to, the **supportShow** command. Doing so gathers additional switch details and sends by FTP all files to a customer server. Refer to the *Brocade Fabric OS Procedures Guide* for instructions on setting up FTP services.
Trace dump	Fabric OS v4.4.0 users should set up automatic FTP trace dump transfers to customer FTP servers. Doing so will minimize trace dump overwrites. Refer to the *Brocade Fabric OS Procedures Guide* for instructions on setting up FTP services.
Trunking	The user can disable or enable trunking using the **switchCfgTrunk** or **portCfgTrunkPort** commands. When the command is executed to update the trunking configuration, the ports for which the configuration applies are disabled and reenabled with the new trunking configuration (as a result, traffic through those ports could be disrupted).
Upgrading to Fabric OS v4.4.0	Recommended upgrade procedures to Fabric OS v4.4.0 include the following: Before loading v4.4.0: • Run **configUpload.** Creates a backup configuration, should the user want to return to v4.2.0. • Run **supportShow.** Captures the previous error logs in v4.2.0. • Run **chassisName.** Changes the default factory configuration to a more meaningful name. After loading Fabric OS v4.4.0, refer to "Logging, **supportFTP**," earlier in this table.

Fabric OS Area	Description
WWN card FRU repair	If an HA failover or power cycle occurs during a FRU replacement on the WWN card, the SilkWorm 12000 or 24000 director becomes non-operational. **CAUTION**: When performing a FRU replacement on a WWN card, complete the FRU procedure before attempting an HA failover or power cycling the chassis.
Zoning	**Issue:** Domain 0 in a zoning configuration file is invalid but has not been previously enforced. **Workaround:** Prior to upgrading a switch to Fabric OS v4.2.0 or later, ensure that the fabric's zoning configuration does not contain domain ID 0, which is used for zoning. This is specific only to v4.x switches.
Zoning	When enabling a new zone configuration, you must ensure that the size of the configuration does not exceed the minimum size supported by all switches in the fabric. This is particularly important if and when you downgrade to a FOS that supports a smaller zone database than the current FOS. In this scenario, the zone database in the current FOS would have to be changed to the smaller zone database before the downgrade. You can use the **cfgSize** command to check both the maximum available size and the currently saved size on all switches. Refer to the *Fabric OS Command Reference Manual* for details on the **cfgSize** command. If you believe you are approaching the maximum, you can save a partially completed zoning configuration and use the **cfgSize** command to determine the remaining space."

Documentation Updates

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

The most recent Fabric OS v4.4.0 product manuals, which support all Fabric OS v4.4.x releases, are available on Brocade Connect:

http://www.brocadeconnect.com/

Fabric OS Command Reference Manual

(Publication number 53-0000519-09)

Under the **supportSave** command, in the "Description" section, replace this text:

"RASLOG *switchname-slot-YYYYMMDDHHMM-errDumpAll.ss*

TRACE *switchname-slot-YYYYMMDDHHMM-tracedump.dmp*

supportShow *switchname-slot-YYYYMMDDHHMM-supportShow* (saved in the specified remote directory)"

With this text:

"RASLOG *chassisname-slot-YYYYMMDDHHMM-errDumpAll.ss*

TRACE *chassisname-slot-YYYYMMDDHHMM-tracedump.dmp*

supportShow *chassisname-slot-YYYYMMDDHHMM-supportShow* (saved in the specified remote directory)"

The following commands have been added or modified in the documentation:

- **fportTest**
- **historyShow**
- **supportSave**

Each change is detailed next.

Under **fportTest**, within the "Operands" section, replace the –**seed** and –**width** operand descriptions as follows:

-seed *payload_pattern*

Specify the pattern of the test packets payload. Valid values are:

0 CSPAT (default)

1 BYTE_LFST

2 CHALF_SQ

3 QUAD_NOT

4 CQRT_SQ

5 CRPAT

6 RANDOM

-width *pattern_width*

Specify the width of the pattern that the user specified. When *payload_pattern* is set to 0x00, *pattern_width* is ignored. Valid values are:

1 byte (default)

2 word

4 quad

This operand is optional.

Under **historyShow**, within the "Description" section, add this text:

The SilkWorm 12000 and 24000 support 50 records. Other switch models, which contain field-replaceable units (FRUs), support 28 records.

Under **supportSave**, within the "Description" section, replace this text:

"Use this command to save RASLOG, TRACE, and **supportShow** information for the local CP to a remote FTP location."

With this text:

"Use this command to save RASLog, TRACE, and **supportShow** (active CP only) information for the local CP to a remote FTP location."

Fabric OS Features Guide

(Publication number 53-0000395-02)

On page 4-2, in the first paragraph, replace this text:

"Cable lengths for participating links should differ no more than 30 meters."

With this text:

"Cable lengths for participating links should differ no more than 550 meters. For optimal performance, no more than 30 meters difference is recommended."

Fabric OS Procedures Guide

(Publication number 53-0000518-06)

The following text should be added to Chapter 9, "Administering Advanced Zoning," in the section "Creating and Modifying Zoning Configurations" on page 9-14:

"When enabling a new zone configuration, you must ensure that the size of the configuration does not exceed the minimum size supported by all switches in the fabric. This is particularly important if and when you downgrade to a Fabric OS version that supports a smaller zone database than the current Fabric OS version. In this scenario, the zone database in the current Fabric OS version would have to be changed to the smaller zone database before the downgrade.

You can use the **cfgSize** command to check both the maximum available size and the currently saved size on all switches. Refer to the *Fabric OS Command Reference Manual* for details on the **cfgSize** command. If you believe you are approaching the maximum, you can save a partially completed zoning configuration and use the **cfgSize** command to determine the remaining space."

The following section should be added to Chapter 11, "Administering FICON Fabrics," in the section "Enabling and Disabling FICON Management Server Mode" on page 11-8:

Setting Up CUP When FICON Management Server Mode Is Enabled

Fmsmode may be enabled and in use on a switch without a CUP license. The transition from fmsmode disabled to fmsmode enabled with the CUP license installed triggers the notification to the host systems that the CUP feature is available. Without this notification, the host systems will never know the CUP

feature is available and consequently will never try to communicate with it. Hence, it is possible that fmsmode might already be enabled on the switch.

If FICON Management Server mode is already enabled, set up CUP as follows:

1. Verify that FICON Management Server mode is enabled by entering the **ficoncupshow fmsmode** command

   If FICON Management Server mode is not enabled, refer to "Enabling and Disabling FICON Management Server Mode" on page 11-9.

   Caution: If fmsmode is already enabled, disabling it might be disruptive to operation because ports that were previously prevented from communicating will now able to do so.

2. If FICON Management Server mode is enabled, then disable it by entering the **ficoncupset fmsmode disable** command.

   Install a CUP license key as described in "Adding and Removing FICON CUP Licenses" on page 11-14.

3. Enter the **ficoncupset fmsmode enable** command.

Fabric Watch User's Guide

(Publication number 53-0000524-05)

The following rows replace 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
Invalid CRC Count	Monitors the number of CRC errors	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
State Changes	Monitors state changes	Unit: Change(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

The following row replaces the existing row "State Changes" in Table A-7, "E_Port Class Threshold Defaults," on page A-9:

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
State Changes	Monitors state changes	Unit: Change(s) Time Base: minute Low:0	Changed: 0 Below: 0 Above: 0	Informative Informative Out_of_range

		High: 5 Buffer: 0	In-Between: 0	In_range

The following table replaces the existing Table A-8, "F/FL_Port Class Threshold Defaults," on page A-10:

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Loss of Synchronization Count	Monitors the number of loss of synchronization errors	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
Receive Performance	Monitors the receive rate, by percentage	Unit: Percentage (%) Time Base: minute Low: 0 High: 100 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative Informative
State Changes	Monitors state changes	Unit: Change(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
Transmit Performance	Monitors the transmit rate, by percentage	Unit: Percentage (%) Time Base: minute Low: 0 High: 100 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative Informative
Invalid CRC Count	Monitors the number of CRC errors	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
Invalid Transmission Word	Monitors the number of invalid words transmitted	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
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

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Loss of Signal Count	Monitors the number of signal loss errors	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
Primitive Sequence Protocol Error	Monitors the number of primitive sequence errors	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

The following row replaces the existing row “Flash” in Table A-9, “Resource Class Threshold Defaults,” on page A-11:

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Flash	Monitors the percentage of compact flash used	Unit: Percentage(s) Time Base: none Low:0 High: 85 Buffer: 0	Changed: 0 Below: 3 Above: 3 In-Between: 1	Informative Informative Out_of_range In_range

SilkWorm 3250/3850 Hardware Reference Manual

(Publication number 53-0000623-02)

On page 2-3, replace the following “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 *Brocade Fabric OS Procedures 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 reenable the switch to activate ports.
>
> For more information on activating ports on demand, refer to the *Brocade Fabric OS Procedures 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: 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"

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 reseat 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.

Closed Defects in Fabric OS v4.4.0c

Defects Closed in Fabric OS v4.4.0c		
Defect ID	**Severity**	**Description**
DEFECT000049044	High	Summary: Panic BLOOM-RAM_PAR_ERR, 0, S2,P19(12): epi1_status: 0x0010 R2T: 0x0000 TFR: 0x0000 STATS: 0x0000 SMI: 0x00000000 FLT: 0x0020 PHAN: 0x00 EFD: 0x0000 Symptom: In switches running Fabric OS 4.x (3250, 3850, 3900, 12000, 24000), the blade is faulted when hit bloom parity errors in following SRAMs: R2T, TFR, STATS, SMI, FLT, PHAN (Note: EFD is of a separate cause, and is not part of this defect topic) and would need manual intervention, such as slot power off/on blade or reboot switch, to recover. Solution: For soft FLT SRAM parity errors, software recovers by refreshing the SRAM. For unrecoverable hard FLTR SRAM parity errors and all other parity errors, software resets the blade for up to 5 times. If unrecoverable after 5 blade resets, blade is faulted and requires manual intervention to hot plug the blade. The change involves ASIC driver, Blade Driver, EM and RAS modules. The code path is exercised only when bloom parity is triggered and it is not invoked in normal code path. Customer Impact: Though both are rare, there are hard bloom parity errors and there are soft bloom parity errors. Hard bloom parity errors cannot be recovered and blade that are faulted due to hard bloom parity errors need to be replaced. However, majority of bloom parity error are soft bloom errors that are caused by alpha particles and they can be recovered by refresh of the SRAMs. Currently bloom based platform software treats all parity errors as hard error and force user to manual recover the faulted blade for both hard and soft parity errors. In this patch and future FOS release, soft parity errors will be recovered by software without manual intervention; only hard parity errors will need manual intervention. Service Request# RQST00000031866

Defects Closed in Fabric OS v4.4.0c		
Defect ID	**Severity**	**Description**
DEFECT000051056	High	Summary: In PID Format 2 configuration, host lost communication with device when another host reboot on a different port. Symptom: When port x is reset, traffic on port x +16 is lost Solution: Inside Asic driver code, filterCamRscnOffline used its unique macro which used PID Format conversion when checking DID. Consequently it removed the CAM entry for the wrong port (ie for port+16) when PID Format 2 is introduced in FOS 4.2. The fix is to use the right conversion before manipulate CAM table entries during offline RSCN. Customer Impact: The switch removes the CAM entry for the wrong port (ie for port+16). So if the port has devices connected, traffic will be interrupted unintentionally. Service Request# RQST00000033391
DEFECT000052337	High	Summary: Path lost during third party virtualization nodes reboot with Silkworm 4100 Symptom: The high level symptom is path loss during node reset; looking at finisar trace and internal trace log , multiple symptoms were identified: 1. many soft port fault due to the node did not cut off light during reboot. 2. PRLI drop by switch due to duplicate SID cam entries 3. Route on switch for a port did not setup correctly. Solution: Drop incoming FLOGIN when port is in port fault process to avoid race condition in route setup. FOS 4.4.0c also made enhancement to name server to remove duplicate SID in CAM entry setup and enhancement to port fault to reduce number of port fault when device did not cut off light during boot up for 14 minutes. Customer Impact: This defect mainly impacts Silkworm 4100 only. When there is a device/host/virtualization node that does not cut off light and takes a long time to boot up in the environment, it's very likely the port will soft fault many times due to excessive interrupt during speed negotiation etc. If one of the port fault window interferes with Flogin when port temperately reach AC, port route can not be setup. In overlap zoning, its also possible name serer will program duplicate SIDs into CAM entry which can potentially cause certain frame to drop on Silkworm 4100 only. Service Request# RQST00000034115

Defects Closed in Fabric OS v4.4.0c		
Defect ID	**Severity**	**Description**
DEFECT000052653	High	Summary: SW3900 slot-0 faulted and become "No ports found in the system!!!" during voltage variation. Also saw bogus fan messages. Symptom: The console message show " [HIL-1101], 107053,, ERROR, Term_113, Slot 0 faulted, 2.5V (3.30) is above threshold." and slot is faulted. Also observe console message: CRITICAL, Term_113, System fan(s) status Fan1=3276RPM Fan2=3443RPM Fan3=3245RPM Fan4=3443RPM Fan5=3276RPM Fan6=3443RPM Solution: When a voltage is detected as being out of range, messages are printed, which include readings of all sensors on the switch without disable the switch. Printed out the bogus fan message during switch in non-op state is also corrected. Workaround: To avoid the problem, none, except making sure that the input power to the switch is clean. To recover from a problem, reboot or power cycle the switch. Customer Impact: This low voltage setting is not expected to be seen on any normally running switch within the field. Issue was only caught in SQA due to forcing voltage levels that would only be observed on switches with faulty power supplies.
DEFECT000053533	High	Summary: NS does not response to many NS registration and discarded with timeout like 33170 ms. Symptom: This could only exists on the Condor ASIC driver based platform such as Silkworm 4100, when the condition is hit, port comes up very slow. Solution: NS processing was taking up to 200ms to complete on heavily loaded systems. Testing in large SANs on 256 port switches caused a backup of the NS queue as registrations were able to arrive faster then the processing speeds could handle. In this patch and future FOS release, the function is enhanced by use less expansive arithmetic. The new enhanced function takes less than 100ns to complete. Customer Impact: This issue only exists on the Condor ASIC driver, BLOOM based products did not have this processing delay. The SW4100 does not have enough ports, that this error condition should not ever be seen in the field, but under very large zone data base configurations, there is a chance that these time-outs could occur. Probability: Medium

Defects Closed in Fabric OS v4.4.0c		
Defect ID	**Severity**	**Description**
DEFECT000053901	High	Summary: Excessive interrupt may have triggered Fdet when pull cable from trunk port while traffic is running. Symptom: BL_1013 error message is observed on console, which indicate excessive interrupts during cable pull, switch reboot or host reboot. In very rare case if and when the double fault - fdet occurs, blade is faulted Solution: When RX_FIFO condition is detected by hardware due to short burst of invalid primitives, the interrupt is cleared, but port did not reset right away in FOS 4.4.0b (See FOS 4.4.0b release note for Defect 51111) compare to prior FOS due to a coding error. So if the condition persists, port eventually fault due to too many interrupts. The port will recover after a short period of time. The signature of this condition is BL1013 info message. The current fix is to make additional checks in code to determine only transient LOS interrupt or a short burst of invalid primitives on the link, which is shorted than the Loss of sync timeout period, are ignored as originally intended by Defect 51111. During the timing window of too many interrupt, if the port has another failure such as FDET, the blade is faulted. Code change is made to fix the Fdet by setting the blm_type correctly. In FOS 4.4.0c and later releases both excessive interrupt and Fdet are fixed. Customer Impact: Under normal conditions, even when the timing window is hit, the processing of the port will clear its interrupt signal. However, if the timing window is hit, and the port has another failure such as FDET, then in rare cases this error log may be generated. Testing has shown that repeated trunking pulls are required to recreate the timing window. This rare event combined with the need to see an FDET error at the same time should make this a very rare defect in a normal customer environment. Service Request# RQST00000035834
DEFECT000054602	High	Summary: configdownload fails with: ficuImport failed with rc=-2 Symptom: configdownload fails. Solution: Fixed a bug in FICON-CUP daemon library where Hex string to integer conversions routine had a nasty bug wherein any hex string without leading zero would not get converted correctly, thereby causing configdownload to fail. Customer Impact: A customer that uploads a configuration, performs a series of manual edits to the uploaded configuration file, forgets to place the □0x□ on the front of Hex numbers, and then downloads this configuration file back to the switch can cause this error to happen.

Defects Closed in Fabric OS v4.4.0c		
Defect ID	**Severity**	**Description**
DEFECT000053398	Medium	Summary: configupload does not save the FICON-CUP data Symptom: configupload does not save the FICON-CUP data on FOS 4.4.0x only. Solution: Change code such that FICU library reads the temporary file it created during configupload export phase. Customer Impact: The CUP configuration files can still be managed from the mainframe without any problems, but since the configuration files reside on the switch, there is no way to back them up on a server unless this problem is fixed (configupload/download is the only mechanism - which is currently broken with this defect).
DEFECT000053756	Medium	Summary: Got lot of message "Calling cal_CreateBladeObjectKeys on 43100000" on console when testing with a future release of code Symptom: After firmwaredownload -sf on sw12000, got lot of this message "Calling cal_CreateBladeObjectKeys on 43100000" Solution: Code path contained print statements. When remote switch enumerated blade instances in local switch, it caused print statements to appear on console. The print messages normally go to console if not redirected using fosrediout command. Removed the print messages. Customer Impact: These messages will not be seen by a customer running in a fabric containing FOS 4.4 or earlier versions of firmware. Only when the new advanced caching features activated in a future FOS firmware will cause the code to traverse this path containing the left over unit test message. These messages are harmless, but do make reading the console output very difficult. Probability: Low
DEFECT000055300	Medium	Summary: Silkworm3900 reports Fabric Watch error due to fabric watch is initialized before environment monitor daemon (emd) is fully ready. Symptom: Certain Fabric Watch CLI command will output: fabric watch daemon is not initialized Solution: Fabric Watch retry during the initialization sequence to wait for EMD to be ready. Workaround: Cold boot switch Customer Impact: Customer has to reboot the switch to re-initialize Fabric Watch. Service Request# RQST00000036626

Defects Closed in Fabric OS v4.4.0c		
Defect ID	**Severity**	**Description**
DEFECT000055736	Medium	Summary: systemverification fails under admin but passes under root due to sltest Symptom: systemverification command fails, which prevents admin user run diagnostics on a switch. Solution: Change sltest, a subtest under systemverification from factory to admin level. Workaround: Run at root level Service Request# RQST00000036938

Closed Defects in Fabric OS v4.4.0b

Defects Closed in Fabric OS v4.4.0b		
Defect ID	**Severity**	**Description**
DEFECT000050817	Critical	Summary: Web Tools will occasionally fail to provide a success indication, when adding a zone to an existing configuration. Symptom: Web Tools will occasionally display a time out message when updating a zoning configuration even though the operation completed successfully. Solution: The fix for this problem is to improve the callback mechanism from zoning to Web Tools. Customer Impact: Web Tools Zoning changes in some fabric configurations may timeout even though they completed successfully. Re-invoking the Web Tools panel will display the correct zoning configuration.

Defects Closed in Fabric OS v4.4.0b		
Defect ID	**Severity**	**Description**
DEFECT000051774	High	Summary: Using cfgEnable to enable a new zoning configuration that exceeds the CAM limit on a port group will cause traffic to be dropped. Symptom: Issuing a cfgEnable command will cause a port group to stop sending traffic if the new configuration causes the port group to exceed its CAM limit. Many devices will retry and cause traffic to resume after a short pause but some devices may require a port enable/disable to correct the behavior. Solution: When CAM entries are full (64 devices per quad on a BLOOM-based environment, and 2048 entries per chip on a CONDOR-environment), the port turned into session-based zoning. When add another entry into the zone, improper check of error return code puts the port into Hardware zoning temporarily, which caused class3 frame drop during the zoning transition. The fix is to check proper error return code to have the correct session-based zoning setup in the switch to eliminate the window. Customer Impact: This defect only affects systems where zones contain devices greater than the CAM entry limit (64 devices per quad on a BLOOM-based environment, and 2048 entries per chip on a CONDOR-environment). On these systems, a cfgEnable command would cause traffic to some devices to be dropped. If the devices re-login (PLOGI) as part of their error recovery process, zoning will be correctly re-configured and traffic would resume. Some devices may require manual intervention to correct the problem - for example - rebooting the host would clear the condition. However, because this problem is new for Fabric OS 4.4.x, then a configuration that worked correctly in Fabric OS 4.1.x or 4.2.x will now fail as a result of an upgrade. Service Request# RQST00000034503

Defects Closed in Fabric OS v4.4.0b		
Defect ID	**Severity**	**Description**
DEFECT000052731	High	Summary: A switch will failover or reboot as a result of an SNMP crash. Symptom: The software watchdog causes an unscheduled automatic failover or reboot on SilkWorm platforms running Fabric OS v4.4.x after a period of 49 days. Solution: Fabric OS includes a software watchdog (swd) that periodically verifies the operation of critical software components. As part of this process, each software daemon must check in on a regular basis to inform the watchdog that the process is alive. If the daemon doesn't check in, the swd will begin recovery procedures to restore operations. Some daemons can only be restarted by causing the switch to reboot or failover. In Fabric OS v4.4.x, the SNMP daemon incorrectly computes its refresh time due to a counter wraparound. As a result, the watchdog timer begins recovery procedures that cause a switch failover or reboot. This rollover will occur at approximately 49-day intervals. The only method to correct the situation is to activate a failover or reboot the switch prior to the 49-day interval. Customer Impact: Switches may have an unscheduled failover or reboot after 49 days or more of operation. Service Request# RQST00000035153
DEFECT000052786	High	Summary: Loss of Target one a host when another host is rebooted Solution: Resolves the problem where host on port+16 loses its target when host on port+0 reboots or port+0 is disabled, Service Request# RQST00000034804

Defects Closed in Fabric OS v4.4.0b		
Defect ID	**Severity**	**Description**
DEFECT000052973	High	Summary: Upgrading to FOS v4.4.x will result in a temporary Name Server/Zoning Service incompatibility. In large fabrics, this can also cause traffic to stop. Symptom: After upgrading from FOS v4.1.x/4.2.x to FOS v4.4.x, the Name Server loses all zoning information and leaves all devices zoned together. As devices go online/offline, a flood of PLOGI requests may be generated as the host driver re-synchronizes its information. In large fabrics, this PLOGI storm can cause the switch to disable interrupts and cause traffic to stop. Solution: Early update the Name Server cache but some installations may have additional problems as described in Defect000051774. Fabric OS 4.4.0b/4.4.1a will properly populate the Name Server cache after an upgrade. Workaround: The condition can be remedied by issuing a cfgEnable command. Customer Impact: There is no impact to the SilkWorm 3016. This issue would only impact the firmware upgrade of the older SilkWorm platforms from prior 4.x versions. Service Request# RQST00000035352
DEFECT000054591	High	Summary: Getting BL-1013 errors, port not resetting fast enough Service Request# RQST00000036168
DEFECT000051111	Medium	Summary: A single corrupted idle sent by a storage device despite subsequent good idles will cause the switch to take the port offline by sending a not operational primitive sequence (NOS). Symptom: The switch takes the port offline upon seeing a single bad idle frame, causing the host driver to lose connectivity to storage. Solution: We are making extra checks on rx_fifo_over, rx_fifo_under, current lli_status rx_fifo_under and current lli_status LOSYNC_TO to determine if we are going to process the transient LOS interrupt or not cause by a short burst of invalid primitives on the link. This way, any current ways of processing RX_FIFO, or LOSYNC_TO are not changed. Workaround: none. Customer Impact: A correctly operating storage system port may be taken offline due to single corrupted Idle primitive. Installing this fix will increase overall availability for some storage systems. Service Request# RQST00000033544

Defects Closed in Fabric OS v4.4.0b		
Defect ID	**Severity**	**Description**
DEFECT000051650	Medium	Summary: An edge condition could cause the software watchdog to incorrectly reboot a switch due to FSPF path change request storms. Symptom: The Software Watchdog (swd) could cause a failover or reboot due to an FSPF panic. Solution: As part of the software watchdog code review, an edge condition was discovered where a faulty routing driver could cause a condition where FSPF would be overloaded with a flood of path change requests. The fix was to properly handle this storm to avoid the possibility of the software watchdog error. Customer Impact: This condition should never occur in a real-life customer situation on FOS 4.4.x. This fix was created as part of continuing product quality improvements. Service Request# RQST00000034139
DEFECT000051911	Medium	Summary: Brocade 3250 with FOS v4.2.2a reboots continuously within two minutes if the switch gets into a severe over temperature condition. Symptom: SilkWorm 3250 and 3850 do not have the ability to shut down the switch via software. Currently Silkworm model 3250 would reboot if two or more of the three fans fail. Similarly, Silkworm model 3850s will issue a message and reboot when three or more of the fans fail. THERE IS NO HAZARD reaches the upper temperature threshold. While the switch has sufficient margin to operate without any operating fans, the condition would cause repeated fabric disruptions as the switch repeatedly exits and rejoins the fabric. Solution: In this fan fail condition, the software will permanently disable the switch. The switch will continue to reboot but will no longer disrupt the fabric. Customer Impact: The fan fail condition is not a safety issue as the SilkWorm 3250/3850 switches can safely operate without fans. By disabling the switch, the fix will ensure that the remaining fabric will not be affected by the switch rebooting. Service Request# RQST00000034581

Closed Defects in Fabric OS v4.4.0a

Defects Closed in Fabric OS v4.4.0a		
Defect ID	**Severity**	**Description**
DEFECT000034830	High	Summary: Switch reboot with CF Error: hda: status timeout .... Symptom: Watchdog Exception: current process c2c04000, r1=c2c059f0. Customer Impact: In extremely rare cases, the CF device will lock during a write action. The IDE driver will attempt to unlock the device through a soft reset of the device, but in some rare instances, that has failed. As a last resort we can perform a hard reset of the device and the system can proceed. This occurred because the software release in which this problem was found did not have the patch to perform the hard reset. In this case, the user would have to restart the CP to reset the CF and continue. Probability: Low Service Request# RQST00000025100
DEFECT000050483	High	Summary: Three switches rebooted nearly simultaneously after 497.1 days. Symptom: Switch reboot with daemon coredumps, uptime shows 497.1days Solution: Callers of clock_gettime() use a random time value passed back when jiffies wraps after 497.1 days. This causes indefinite waiting time on caller's thread, resulting in software watchdog kicks in and switch reboots. The fix is to have callers check return value of clock_gettime() rather than use the passed back random time value blindly. The callers will bail out and the high level code will retry gracefully after jiffies wraps. Also fixed libC times() call such that it will return correct jiffies within 5 seconds before jiffies overrun to counter measure syscall interface contamination of return code. Workaround: hareboot or hafailover when uptime is near 497.1 days Customer Impact: Switch most likely will reboot when switch uptime is at 497.1 days. Service Request# RQST00000033039

Defects Closed in Fabric OS v4.4.0a		
Defect ID	**Severity**	**Description**
DEFECT000050587	High	Summary: Edge switch panic in NS during switchreboot of core switches Symptom: Switch reboots because of Out of Memory after repeated queries of Symbolic Node Name by Node Name. Solution: Fix a memory leak in handling GSNN_NN(Get Symbolic Node Name by Node Name) request from a local device or API if the queried device is on a remote switch and has a symbolic node name. Customer Impact: Switch reboots because of out of memory. The leak is from handling GSNN_NN(Get Symbolic Node Name by Node Name) request from a local device or API if the queried device is on a remote switch and has a symbolic node name. The leak is small and it takes a long time to cause switch Out of Memory.
DEFECT000050909	High	Summary: MicroCode:Port with media (2G SFP) inserted reports no media when the switchshow command is run. Port status LED is amber. Symptom: when user is doing plugging/unplugging of SFPs, there is a possibility that the SFP will no longer be recognized as plugged in even though it is actually in. Customer Impact: The impact of this defect is that when user is doing plugging/unplugging of SFPs, there is a possibility that the SFP will no longer be recognized as plugged in even though it is actually in. Without the fix, the workaround is to do portdisable followed by portenable on the failure port. Service Request# RQST00000033549
DEFECT000051411	High	Summary: E-port connectivity is unavailable upon using the following: Finisar PN: FTRJ-1319-7D-2.5 Symptom: When using a specific DWDM equipment, the link b/w the switch and DWDM equipment does not come up. Customer Impact: A specific DWDM equipment needs 10B comma characters to gain sync and if SW4100 are connected to this requipment, the link will not come up. The SFP speed and type do not make a difference. There are other DWDM which work fine. A fix was to add the 10 comma character to the EMI transmit pattern when there is no light coming on the rx side. Service Request# RQST00000034128

Defects Closed in Fabric OS v4.4.0a		
Defect ID	**Severity**	**Description**
DEFECT000051461	High	Summary: About Defect of configRemoveAll Symptom: Use of ConfigRemoveAll command can panic the switch. Customer Impact: ConfigRemoveAll is a command that needs root access and is only used to restore the switch to it's default state in factory. When this command is issued, it is possible to leave the system state in a way where the systems keeps rebooting as it is using a zoning database file which should not be there and has one character in it. Service Request# RQST00000034166
DEFECT000051536	High	Summary: 'LR' does not restore login BB credits Symptom: After link reset the BB_Credits doe not get restored and stays at one. Customer Impact: Using Jammer to create a scenario of running out of BB_Credits leads to Link Reset after which the BB_Credits should have been restored to their initial value. But after Link reset the BB_credits are restored to 1. This could potentially slow the system down if the port had run out of BB_Credits. The fix is to restore the number correctly after Link Reset. Service Request# RQST00000034181
DEFECT000041567	Medium	Summary: SW3900 saw ENC_ERR when no cable plugged in on 4.0.2; SW3250/3850 saw same issue with 4.2 Symptom: Encoding errors denoted by Enc_out increasing on unused ports in some cases. Customer Impact: Port statistics display increasing ENC_ERR errors, even when the data link has no link partner (e.g. due to no SFP or cable). This gives the erroneous impression of faulty behavior. The fix qualifies the errors with the physical link state, asserting that errors pertain only when synchronization is achieved. Thus, when the fix is applied, ENC_ERR never increments when the data link has no link partner. Service Request# RQST00000027602

Defects Closed in Fabric OS v4.4.0a		
Defect ID	**Severity**	**Description**
DEFECT000048123	Medium	Summary: Run multiple third party applications using multiple proxy switches, some web page can no longer be retrieved with underlying MS timeout Symptom: When there are large numbers of management or third party applications running, Webtool can sometimes not retrieve nsinfo.htm and zoning information while underneath traffic is running fine. Solution: A chassis with two logical switches (switch A and switch B) has empty slots on each side. A request for a physical port number (GPNN) from application with a port wwn of zero is received on switch A. The empty slots have zero for the port wwn. Thus, when MS search it database of port wwn, it finds the switch B with the empty slots and send the request to it. Switch A and Switch B hence dead lock processing the 0 wwn request between each other. To fix, reject MS commands that have WWN of all zeros Workaround: This problem can be avoided with fully populate switch chassis. Also reduce the number of multiple applications running with multiple proxies seem to reduce the chance for it to happen. Customer Impact: This has been observed to happen if multiple concurrent applications run in the fabric with multiple proxy switches and there are switches in the fabric that are not fully populated with blades. When it happens, management applications do not function properly and fabric channel traffic continues to run fine. Service Request# RQST00000031531
DEFECT000049097	Medium	Summary: Intermittent Port init with a specific HBA connections on iSeries IO Symptom: Customer HBA keeps resetting the port by cutting off light after speed negotiation, after loop init failure, or in the middle of link init. Customer Impact: Without fix: customer HBA keeps resetting the port by cutting off light after speed negotiation, after loop init failure, or in the middle of link init. With fix, the link is cleaner (no echo/bypass of customer transmitted primitives) during port init which should eliminate the retries. Service Request# RQST00000032002

Defects Closed in Fabric OS v4.4.0a		
Defect ID	**Severity**	**Description**
DEFECT000049827	Medium	Summary: Port 26 fails to come up on multiple cable pull/insert Symptom: If the port is in AN mode, it doesn't come up if the cable is pulled and reinserted multiple times and is mainly seen with one of the third party arrays. Workaround: If the port is locked as G-port, then the problem doesn't happen. Customer Impact: When the config is set for AN, under some circumstances a newer version of a particular array type does not get recoganized when multiple cable pull/inserts are tried. This does not happen with the earlier version of the array. Service Request# RQST00000032580
DEFECT000050019	Medium	Summary: tempShow shows inconsistent data when Fabric Watch license is not present Symptom: The tempShow command can display somewhat different information for the "State" field, depending on whether Fabric Watch is installed or not. Workaround: Install Fabric Watch license Customer Impact: There is no impact on modular SilkWorms nor on single-board SilkWorms with Fabric Watch. The impact on single-board SilkWorms that do not have Fabric Watch is that a customer who runs the tempShow command (and the equivalent function in Web Tools) the "State" may not reflect over-temperature conditions for individual sensors. However, their systems will continue to monitor temperatures and if any system becomes too hot (as determined by platform-specific policies) it will take action and print one or more console logs to tell the customer what is happening. Service Request# RQST00000032852

Defects Closed in Fabric OS v4.4.0a		
Defect ID	**Severity**	**Description**
DEFECT000050199	Medium	Summary: In a fabric consisting of v2.6 switches, when trying to propagate a zone configuration whose size exceeds the supported v2.6 limit, the propagation fails, and no further zoning changes can be made in the fabric. Symptom: This problem occurs only in fabrics consisting of newer switches as well as v2.6 switches. When trying to propagate a zone configuration whose size exceeds the supported v2.6 limit, the zone propagation fails, and no further zoning changes can be made in the fabric. The customers would not be able to start another transaction. Solution: Added an error message to let the users know when they are attempting to create a zone config that exceeds the limit that can be supported in the fabric containing V2.6 switches. Workaround: If a fabric has 2.6 switches, then the customers should not create a zone cfg larger than 96 KB. Customer Impact: If the customers have v2.6 switches in their fabric, then they cannot create zone configurations larger than 96 KB. The issue is seen when zone DB is propagated from newer switches that support larger configuration sizes compared to the older versions of Fabric OS and the size of the new zone DB is larger than the size supported by older versions. Switches that do not support the larger zoning DB sizes will lose their zoning DBs when committing a larger zoning DB.
DEFECT000050554	Medium	Summary: After removing either Fan 2 or Fan 3 and running the fanshow command, the system reports a 4th nonexistent fan. Symptom: If the customer removes either fan 2 or fan 3 on a live switch and then runs the fanshow command, the command output will show a 4th non-existent fan. Solution: The solution is to do the associated check on the FRU state and not the hil sensor. The hil sensor is not updated properly whereas the FRU state one is. Workaround: none Customer Impact: If the customer removes either fan 2 or fan 3 on a live switch and then runs the fanshow command, the command output will show a 4th non-existent fan in some cases which can be confusing to the customer. The problem has been fixed and now the fanshow gives accurate information. Service Request# RQST00000033179

Defects Closed in Fabric OS v4.4.0a		
Defect ID	**Severity**	**Description**
DEFECT000050769	Medium	Summary: SNMP clients may break due to connUnitPortWwn response change Symptom: The connUnitPortWwn MIB variable has a syntax of OCTET STRING of size 8. Instead it was being incorrectly sent as a ASCII string (sequence of ASCII characters) with each octet of port WWN formatted as 2 hex characters separated by a ":". The size of the resulting OCTET STRING received by SNMP client will be thus 23 instead of 8. Customer Impact: SNMP client relying on the syntax of connUnitPortWwn MIB variable to parse the value returned by the SNMP agent will not be able to correctly interpret the port WWN value. Service Request# RQST00000033307
DEFECT000050774	Medium	Summary: Port type incorrect on web tools interface display Symptom: When a user locks a port as G_Port through the CLI, the current port type is shown as U_Port if the port is not connected yet. Workaround: The users should not worry about the port type until the port really connects to a switch/device. When the port is really connected to a switch/device, the current port type is accurate: F_Port, E_Port, or L_Port. Until then, the port state is actually transient. Web Tools does not show the configured value. It only shows the current value. The fact that a port is locked as a G_Port is not of much importance. If the user wants to see the configured value, the user should run the portcfgshow command in a telnet session. Customer Impact: It is confusing to the customer to see U port even though the port has been locked as G port. There is no impact to switch functionality. Service Request# RQST00000033373
DEFECT000050786	Medium	Summary: v4.4.0_rc1 "savesupport" command is present in help list, but does not exist. Symptom: Customer could see "savesupport" in help list which is not supported. Changed to "supportsave." Solution: remove savesupport item from help command. Add in new command - supportsave Workaround: ignore non-existent command Customer Impact: There is no customer impact of savesupport showing up in the help list. It has been removed to eliminate any confusion. Service Request# RQST00000033383

Defects Closed in Fabric OS v4.4.0a		
Defect ID	**Severity**	**Description**
DEFECT000050349	Low	Summary: SilkWorm 4100 segments E_Ports when "Fabric License" is not present Symptom: SilkWorm 4100 segments E_Ports when "Fabric License" is not present Customer Impact: SilkWorm 4100 is not a value-line switch. So it does not require explicit fabric license to participate in a multi-switch fabric. Without the fix for this defect SilkWorm 4100 will be isolated from the fabric with all the E-ports segmented. The workaround is to load full fabric license onto a SilkWorm 4100 for it to join the fabric.