



Brocade Fabric OS v4.4.2b Release Notes v1.0

June 14, 2006


Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v4.4.2b Release Notes v1.0	First release	June 14, 2006

Copyright © 2006, Brocade Communications Systems, Incorporated.

ALL RIGHTS RESERVED.

Brocade, the Brocade B weave logo, Fabric OS, File Lifecycle Manager, MyView, Secure Fabric OS, SilkWorm, and StorageX are registered trademarks and Tapestry is a trademark of Brocade Communications Systems, Inc., 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 and IBM  BladeCenter are registered trademarks of IBM Corporation in the U.S. and 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.

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.

CONTENTS

Document History.....	1
Overview	4
Supported Switches	4
Technical Support.....	5
Standards Compliance	5
Important Notes.....	6
OS Requirements.....	6
Features in Fabric OS v4.4.x	7
Advanced Web Tools Updates	9
Other Notes.....	12
Documentation Updates.....	20
Fabric OS Command Reference Manual	20
Fabric OS Features Guide.....	21
Fabric OS MIB Reference Manual	22
Fabric OS Procedures Guide	22
Fabric Watch User's Guide	23
SilkWorm 3250/3850 Hardware Reference Manual.....	25
SilkWorm 4100 Hardware Reference Manual.....	26
SilkWorm 12000 Hardware Reference Manual.....	27
SilkWorm 24000 Hardware Reference Manual.....	27
Closed Defects in Fabric OS v4.4.2b.....	30
Closed Defects in Fabric OS v4.4.2a.....	34

Overview

Fabric OS v4.4.2b is a patch release containing fixes to defects found since the release of Fabric OS v4.4.2a. It includes the same feature set as Fabric OS v4.4.2. Except where specified, Fabric OS v4.4.2 is functionally identical to earlier releases of Fabric OS v4.4.x. Fabric OS v4.4.0 provides the following enhancements and new features:

- Support for the SilkWorm 4100
- Greater than twofold 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 a maximum of 2560 ports and 50 domains
- Ports on Demand (POD) via license keys for instant scalability
- Fabric Watch improvements:
 - Improved notification
 - Switch health reports
- Standardized messaging for inclusion of 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

Supported Switches

This release supports SilkWorm 3016, 3250, 3850, 3900, and 4100 switches and SilkWorm 12000 and 24000 directors.

Technical Support

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

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: Side of switch module
- SilkWorm 3250, 3850, and 3900 switches: Back of chassis
- SilkWorm 4100 switches: On the switch ID pull-out tab located on the port side and on the inside of the chassis, near power supply 1 (on the right when looking at the nonport side)
- SilkWorm 12000 and 24000 directors: Inside front of chassis, on wall to left of 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 3016, 3250, 3850, 3900, and 4100 switches, and SilkWorm 12000 and 24000 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: Provides the switch WWN. Use the **wwn** command to display the switch WWN.

Standards Compliance

This release 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 that you should consider before you use this release

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

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

http://www.brocade.com/support/end_of_life.jsp

	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	v3.1.2 or later	v4.2.0 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

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, and 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.

Features in Fabric OS v4.4.x

The major features in Fabric OS v4.4.x are summarized in the following table.

Category	Feature	Release
SilkWorm 24000 Enhancements	Mixed-blade support for the SilkWorm 24000: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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

Category	Feature	Release																							
Long-Distance Enhancements	200 km at 1 Gbit/sec or 100 km at 2 Gbit/sec (SilkWorm 3250, 3850, 24000, Bloom II ASIC-based switches)	v4.4.0																							
	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)	v4.4.0																							
	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: <ul style="list-style-type: none">four links at 10 km @ 2 Gbit/sec per trunk groupthree links at 25 km @ 2 Gbit/sec per trunk grouptwo links at 50 km @ 2 Gbit/sec per trunk group	v4.4.0																							
	Buffer-limited ports	v4.4.0																							
	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>	Distance	Number of 2-Gbit/sec ports (Bloom to Bloom)	LE 10 km	4 (one 4-port trunk)	L0.5 25 km	3 (one 3-port trunk)	L1 50 km	1 (one 2-port trunk)	L2 100 km	0	LD 200 km	0	LD 250 km	0	LD 500 km	0	v4.4.0							
	Distance	Number of 2-Gbit/sec ports (Bloom to Bloom)																							
	LE 10 km	4 (one 4-port trunk)																							
	L0.5 25 km	3 (one 3-port trunk)																							
	L1 50 km	1 (one 2-port trunk)																							
	L2 100 km	0																							
LD 200 km	0																								
LD 250 km	0																								
LD 500 km	0																								
Enhanced trunking support 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>	Distance	Number of 2-Gbit/sec ports or trunks (Condor to Condor)	Number of 4-Gbit/sec ports (Condor to Condor)	LE 10 km	32 (four 8-port trunks)	32 (four 8-port trunks)	L0.5 25 km	32 (four 8-port trunks)	15 (one 8-port trunk)	L1 50 km	15 (one 8-port trunk)	7 (one 7-port trunk)	L2 100 km	7 (one 7-port trunk)	3 (one 3-port trunk)	LD 200 km	3 (one 3-port trunk)	0	LD 250 km	3 (one 3-port trunk)	0	LD 500 km	0	0	v4.4.0
Distance	Number of 2-Gbit/sec ports or trunks (Condor to Condor)	Number of 4-Gbit/sec ports (Condor to Condor)																							
LE 10 km	32 (four 8-port trunks)	32 (four 8-port trunks)																							
L0.5 25 km	32 (four 8-port trunks)	15 (one 8-port trunk)																							
L1 50 km	15 (one 8-port trunk)	7 (one 7-port trunk)																							
L2 100 km	7 (one 7-port trunk)	3 (one 3-port trunk)																							
LD 200 km	3 (one 3-port trunk)	0																							
LD 250 km	3 (one 3-port trunk)	0																							
LD 500 km	0	0																							

Category	Feature	Release
SNMP Support	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.	v4.4.0 or later
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://www.mozilla.org/releases/mozilla1.6/>

- 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)	<p>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.</p> <p>Web Tools v3.1.0+ and v4.1.0+ includes a Print button in the Fabric Topology window; earlier versions do not.</p> <p>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.</p>

Launch Switch Environment	Problems
<p>Firmware: Fabric OS v2.6.x</p> <p>Operating System: Solaris</p> <p>Browser: Mozilla</p>	<p>Issue: The Switch Admin does not launch correctly.</p> <p>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.</p> <p>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.</p> <p>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.</p>
<p>Firmware: version <i>prior</i> to Fabric OS v2.6.2, v3.1.2, or v4.2.0 with secure mode enabled</p> <p>Operating System: Solaris</p> <p>Browser: Mozilla</p>	<p>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.</p> <p>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.</p>
<p>Firmware: version <i>prior</i> to Fabric OS v2.6.2, v3.1.2, or v4.2.0</p> <p>Operating System: any supported operating system (with supported browser)</p> <p>Browser: any supported browser (on supported operating system)</p>	<p>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.</p> <p>Workaround: 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>Firmware: version <i>prior</i> to Fabric OS v4.4.0</p> <p>Operating System: any supported operating system (with supported browser)</p> <p>Browser: any supported browser (on supported operating system)</p>	<p>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.</p> <p>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.</p>

Launch Switch Environment	Problems
<p>Firmware: version <i>prior</i> to Fabric OS v4.4.0</p> <p>Operating System: any supported operating system (with supported browser)</p> <p>Browser: any supported browser (on supported operating system)</p>	<p>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.</p> <p>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.</p>
<p>Firmware: version <i>prior</i> to Fabric OS v2.6.2, v3.1.2, or v4.2.0</p> <p>Operating System: Solaris</p> <p>Browser: Netscape</p>	<p>Issue: Any switches running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later are unsupported through Netscape.</p> <p>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.</p>
<p>Firmware: version <i>prior</i> to Fabric OS v2.6.1, v3.0.x, or v4.0.x</p> <p>Operating System: Windows</p> <p>Browser: Internet Explorer</p>	<p>Issue: When you are trying to run Fabric View with a large fabric, the browser might crash.</p> <p>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).</p> <p>Use a launch switch with v.2.6.2, v3.1.x, or v4.1.x and later.</p>

Other Notes

The following are known issues in this release of Fabric OS.

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

SilkWorm 4100	Description																																	
CWDM module and SFP	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>	2 Gbit/sec CWDM	Manufacturer	Manufacturer's Part Number	CWDM Mux/Demux Module - 8 port	Finisar	FWS-MUX-DEMUX-8	CWDM Mux/Demux Module - 4 port	Infineon	FWS-MUX-DEMUX-4	2G SFP 1470 nm (Gray)	Finisar	FWDM-1621-7D-47	2G SFP 1490 nm (Violet)	Finisar	FWDM-1621-7D-49	2G SFP 1510 nm (Blue)	Finisar	FWDM-1621-7D-51	2G SFP 1530 nm (Green)	Finisar	FWDM-1621-7D-53	2G SFP 1550 nm (Yellow)	Finisar	FWDM-1621-7D-55	2G SFP 1570 nm (Orange)	Finisar	FWDM-1621-7D-57	2G SFP 1590 nm (Red)	Finisar	FWDM-1621-7D-59	2G SFP 1610 nm (Brown)	Finisar	FWDM-1621-7D-61
	2 Gbit/sec CWDM	Manufacturer	Manufacturer's Part Number																															
	CWDM Mux/Demux Module - 8 port	Finisar	FWS-MUX-DEMUX-8																															
	CWDM Mux/Demux Module - 4 port	Infineon	FWS-MUX-DEMUX-4																															
	2G SFP 1470 nm (Gray)	Finisar	FWDM-1621-7D-47																															
	2G SFP 1490 nm (Violet)	Finisar	FWDM-1621-7D-49																															
	2G SFP 1510 nm (Blue)	Finisar	FWDM-1621-7D-51																															
	2G SFP 1530 nm (Green)	Finisar	FWDM-1621-7D-53																															
	2G SFP 1550 nm (Yellow)	Finisar	FWDM-1621-7D-55																															
	2G SFP 1570 nm (Orange)	Finisar	FWDM-1621-7D-57																															
	2G SFP 1590 nm (Red)	Finisar	FWDM-1621-7D-59																															
2G SFP 1610 nm (Brown)	Finisar	FWDM-1621-7D-61																																
LED, system status	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.																																	
LED, system power	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.																																	
Fan, RPM reading	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.																																	

SilkWorm 4100	Description
WWN	<p>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.</p> <p>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.</p> <p>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).</p> <p>IEEE OUI and Company_id Assignments:</p> <p>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</p> <p>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</p> <p>IEEE list of public OUI assignments:</p> <p>http://standards.ieee.org/regauth/oui/index.shtml</p> <p>In a management application using a Fabric Access version earlier than v3.0.2, SilkWorm 3250 and 3850 switches are displayed as Rhapsody switches.</p>

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.
Firmware upgrade	Fabric OS v4.x firmware upgrades include the <i>release.plist</i> file. There is a separate <i>release.plist</i> 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 <i>release.plist</i> 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.

Fabric OS Area	Description
Invalid gateway IP address error message	<p>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:</p> <pre>SIOCADDRT: Invalid argument ip.c:311:Invalid gateway IP address 0.0.0.0</pre> <p>This is a display issue only and does not affect the functionality of the switch.</p>
IP addresses	CAUTION: Do not set a switch or CP IP address for the Ethernet interface to 0.0.0.0.
Logging, <i>syslog.conf</i>	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 <i>syslog.conf</i> 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	<p>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 <i>odd-numbered .emerg</i> facility level file on the target Solaris systems: for example, <i>local6.emerg</i> will appear in <i>local7.emerg</i> if syslogd facility level 6 is selected.</p> <p>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.</p>
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.
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 <i>Brocade Fabric OS Procedures Guide</i> .
Logging, errClear 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).

Fabric OS Area	Description
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	<p>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:</p> <pre>"Security violation: Login failure attempt via TELNET/SSH/RSN. IP Addr: 192.168.44.247"</pre> <p>If another login violation occurs immediately, the message remains the same and only the error counter is incremented.</p>
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 certificate	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.
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	<p>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.</p> <p>Should you need to reinstall switch certificates in a SilkWorm 24000 director, follow these guidelines:</p> <ul style="list-style-type: none"> • 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.

Fabric OS Area	Description
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 <i>not</i> apply to upgrades from v4.2.0 to v4.4.0.
Security, secure mode, passwd telnet	<p>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.</p> <p>This is expected behavior. The session will terminate if you change the password in secure mode.</p>
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.
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	<p>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.</p> <p>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.</p> <p>Related defects: 48168, 49254</p>
Support	<p>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.</p> <p>Refer to the <i>Brocade Fabric OS Procedures Guide</i> for instructions on setting up FTP services.</p>
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 <i>Brocade Fabric OS Procedures Guide</i> for instructions on setting up FTP services.

Fabric OS Area	Description
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	<p>Recommended upgrade procedures to Fabric OS v4.4.0 include the following:</p> <p>Before loading v4.4.0:</p> <ul style="list-style-type: none"> 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. <p>After loading Fabric OS v4.4.0, refer to “Logging, supportFTP,” earlier in this table.</p>
WWN card FRU repair	<p>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.</p> <p>CAUTION: When performing a FRU replacement on a WWN card, complete the FRU procedure before attempting an HA failover or power cycling the chassis.</p>
Zoning	<p>Issue: Domain 0 in a zoning configuration file is invalid but has not been previously enforced.</p> <p>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.</p>
Zoning	<p>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.</p> <p>You can use the cfgSize command to check both the maximum available size and the currently saved size on all switches. Refer to the <i>Fabric OS Command Reference Manual</i> 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.”</p>
Loss of sync between Emulex HBA and Brocade 4Gb/sec switch	<p>Issue: If there is a loss of sync forcing a link to be re-established, it is possible that links between Emulex HBAs and 4Gb Brocade switches may not automatically be re-established. This issue could occur after an error that has forced the switch and HBA to re-establish link initialization such as a cold switch reboot.</p> <p>Workaround: Use the command portCfgGPort to configure the switch port in point-to-point only mode, also known as G port mode. To configure the HBA to point-to-point mode, please refer to Emulex HBAnyware™ documentation. To re-establish the link on the affected port without traffic disruption on other ports, issue the commands portDisable and portEnable on the affected port.</p>

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)

On page 2-75, remove the reference to “fabric.ops.mode.vcEncode: 0” from the **configShow** output in the Example section.

The following commands are not supported in Fabric OS v4.4.x:

- **diagEsdPorts**
- **diagModePr**
- **diagSilkworm**
- **numSwitchSet**
- **numSwitchShow**
- **portCfgMcastLoopback**
- **tsHelp**

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

RASLOG	<i>switchname-slot-YYYYMMDDHHMM-errDumpAll.ss</i>
TRACE	<i>switchname-slot-YYYYMMDDHHMM-tracedump.dmp</i>
supportShow	<i>switchname-slot-YYYYMMDDHHMM-supportShow</i> (saved in the specified remote directory)”

With this text:

RASLOG	<i>chassisname-slot-YYYYMMDDHHMM-errDumpAll.ss</i>
TRACE	<i>chassisname-slot-YYYYMMDDHHMM-tracedump.dmp</i>
supportShow	<i>chassisname-slot-YYYYMMDDHHMM-supportShow</i> (saved in the specified remote directory)”

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

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

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.”

Under **portLoopbackTest**, within the “Operands” section, replace this text:

“Specify a list of user ports to test. By default, all of the user ports in the current switch are tested. This option can be used to restrict testing to the specified ports.”

With this text:

“Specify a list of blade ports to test. By default, all the blade ports in the specified slot (using **–slot**) are used. Refer to **itemlist** for further details.”

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 MIB Reference Manual

(Publication number 53_0000521_08)

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 turn on and off traps individually within a trap group. The individual traps need to be enabled explicitly after the corresponding trap group is enabled.

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

Fabric OS Procedures Guide

(Publication number 53-0000518-06)

On page 3-14, 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 4-11, at the end of the section “Upgrading SilkWorm 12000 and 24000 Directors,” add the following:

Caution

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

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 be 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.

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

- Brocade translatable mode

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

Note: Switches with a Condor ASIC do not support translatable mode.

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 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range 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
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
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

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
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
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)

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”.
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.

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).”

SilkWorm 24000 Hardware Reference Manual (Publication number 53-0000619-01)

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.”

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

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

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

Replace Step 1 with this information:

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

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

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

The system is coming up, please wait...
Checking system RAM - press any key to stop test
00b00000
System RAM check terminated by keyboard
System RAM check complete
```

Press escape within 4 seconds to enter boot interface.

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

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

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

On page 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"

Closed Defects in Fabric OS v4.4.2b

This table lists defects that have been newly closed in Fabric OS v4.4.2b.

Defects Closed in Fabric OS v4.4.2b		
Defect ID	Severity	Description
DEFECT000062068	High	<p>Summary: Power failure in a port blade caused SilkWorm 24000 to panic on both CP's.</p> <p>Symptom: A power failure was most likely due to an improperly seated blade. It affected both the active and standby CP's.</p> <p>Solution: Sets the slot parameter to the correct value before calling the interrupt validation routine.</p> <p>Risk of Fix: Low</p> <p>Service Request# RQST00000042166</p> <p>Reported in Release: V4.4.0</p>
DEFECT000063030	High	<p>Summary: Frame drop might occur in session-based zoning in NPIV testing environment on 4Gig switch.</p> <p>Symptom: This might impact a 4Gig switch with multiple devices attached to a single port or a single host talking to multiple targets in session-based zoning.</p> <p>Solution: Corrects an ASIC hardware programming race condition.</p> <p>Workaround: Use hard-based instead of session-based zoning.</p> <p>Probability: Medium</p> <p>Risk of Fix: Medium</p> <p>Reported in Release: V5.0.1</p>

Defects Closed in Fabric OS v4.4.2b		
Defect ID	Severity	Description
DEFECT000063089	High	<p>Summary: N_port login and acceptance (PLOGIN/PLOGIN ACC) frames might be delayed or dropped for all Fabric OS v4.x and v5.0.1 on SilkWorm 3x50, 301x, 3900, 12000, and 24000 platforms.</p> <p>Symptom: Host loses connection to target. Most likely to occur when the host does not retry PLOGIN, and for session-based zoning where a substantial volume of PLOGIN occurs on the switch. HBAs or hosts that re-send their PLOGI requests self-correct as the interrupt from the re-send frees the stuck filter frame.</p> <p>Solution: Fixes a rescheduling issue in the filter task during chip lock contention for a quad (4 ports). The filter task rescheduling issue could cause PLOGI and PLOGI ACC to delay or to drop after a timeout in the switch.</p> <p>Probability: Medium</p> <p>Risk of Fix: Medium</p> <p>Service Request# RQST00000042896</p> <p>Reported in Release: V5.0.1</p>
DEFECT000063582	High	<p>Summary: Under some rare conditions, on a SilkWorm 4020 or other 4Gig platforms, the host cannot see a device after a switch reboot or if a frame drop occurs during a device reboot.</p> <p>Symptom: If the blade enclosure is repeatedly power-cycled, one of the server ports might lose connectivity (1 in 3000 times) to the switch. The server OS will not be able to see the storage drives attached through the SilkWorm 4020.</p> <p>Solution: Covers a small timing window to guarantee the route to the device is set properly when an F_Port login (FLOGI) comes in very fast before the port online process is complete.</p> <p>Workaround: Run portdisable and portenable.</p> <p>Probability: Low</p> <p>Risk of Fix: Low</p> <p>Reported in Release: V5.0.2</p>

Defects Closed in Fabric OS v4.4.2b		
Defect ID	Severity	Description
DEFECT000064156	High	<p>Summary: Frame drop between two ports when other ports in the same zone go offline/online .</p> <p>Symptom: When configuration changed to CHPOFF/ON, ICC occurred on the other paths. This issue only affects 4Gig switches and exists in both 4.4.x and 5.0.x firmware versions. A small timing window exists when a new zoning configuration is installed. When zone groups are being merged, older zone groups are removed from the ASIC tables before new merged zone groups are added. If the switch is under heavy traffic loads, some frames can be dropped during this window between the zone group updates.</p> <p>Solution: Ensures any zone groups that are still valid are not removed: only deleted zone groups will be removed. The timing window is also removed.</p> <p>Probability: Low</p> <p>Risk of Fix: Medium</p> <p>Service Request# RQST00000043608</p> <p>Reported in Release: V5.0.1</p>
DEFECT000065808	High	<p>Summary: Running out of shared segment memory causes switch to panic.</p> <p>Symptom: Memory condition ["Failed to allocate memory: (Shared Memory)"] halts one of the secure shell daemons (sshd). The software watchdog daemon in turn reboots the switch.</p> <p>Solution: Ensures there are no stray sshd threads.</p> <p>Workaround: Create and execute a script to kill the sshd stray threads.</p> <p>Risk of Fix: Low</p> <p>Service Request# RQST00000045222</p> <p>Reported in Release: V4.4.2</p>

Defects Closed in Fabric OS v4.4.2b		
Defect ID	Severity	Description
DEFECT000068720	High	<p>Summary: Some hosts lost traffic to targets during zone configuration change testing on 4Gig platforms.</p> <p>Symptom: During zone configuration testing, some hosts received error messages [CDR-5460] and lost traffic to targets on 4Gig platforms. This was found during internal new platform testing only, but there may be a small window of vulnerability on previously GA'd platforms as well.</p> <p>Solution: Fixes a small window introduced when adding an ASIC content addressable memory (CAM) entry.</p> <p>Workaround: Run configdisable and configenable on the port.</p> <p>Probability: Low</p> <p>Risk of Fix: Medium</p> <p>Reported in Release: FVT_V5.2.0 FOS V4.x</p>
DEFECT000065897	Medium	<p>Summary: Management server daemon (msd) crashes while performing a memcpy() and causes switch to panic.</p> <p>Symptom: Msd crash (SIGSEGV).</p> <p>Solution: Fixes the user space buffer corruption in msd.</p> <p>Risk of Fix: Low</p> <p>Service Request# RQST00000045310</p> <p>Reported in Release: V4.4.0</p>

Closed Defects in Fabric OS v4.4.2a

This table lists defects that have been newly closed in Fabric OS v4.4.2a.

Defects Closed in Fabric OS v4.4.2a		
Defect ID	Severity	Description
DEFECT000063350	High	<p>Summary: After firmware upgrade/downgrade, hosts lost device on SilkWorm 3900 and SilkWorm 12000.</p> <p>Symptom: After firmware upgrade/downgrade on a SilkWorm 3900 and SilkWorm 12000, a host reboot/shutdown might cause the other host sharing the same internal route to lose the device connection. When the down host comes back up, all is recovered.</p> <p>Solution: The problem is caused by miscalculating shared routes when the internal trunk master used for routing is an odd port on a SilkWorm 3900 and SilkWorm 12000. It may only happen on switches with multiple E or F source ports connected to the same target F port on the same switch, but with different mini-switches. The code has been fixed to respond in these situations with the appropriate route reconstruction during HAreboot.</p> <p>Workaround: portdisable/portenable the shared port that lost the shared internal route and/or reboot the switch.</p> <p>Customer Impact: The problem exists since Fabric OS v4.2 on SilkWorm 3900 and SilkWorm 12000. It is more likely after HAreboot or firmware download and may be exposed when F/E ports go down.</p> <p>Probability: Medium</p> <p>Service Request# RQST00000041351</p> <p>Reported in Release: V4.4.0</p>