Brocade Fabric OS v4.4.1a Release Notes_v1.1

March 30, 2005

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v4.4.1a Release Notes v1.0	First release.	February 22, 2005
Brocade Fabric OS v4.4.1a Release Notes v1.1	SilkWorm 4100 table listing certified SFPs has been updated.	March 30, 2005

TABLE OF CONTENTS

About This Release

Fabric OS v4.4.1a is a patch release containing fixes to a number of defects found since the release of Fabric OS v4.4.1. Aside from these changes, this patch release includes the same feature set as Fabric OS v4.4.1.

Due to a specific fix implemented in Fabric OS v4.4.1a, in which an unexpected reboot occurs as a result of an SNMP crash when running Fabric OS v4.4.1 (see Defect 52731), as well as other issues fixed in this patch, Brocade strongly urges all customers to take the following action:

- Upgrade existing switches running Fabric OS v4.4.1 to Fabric OS v4.4.1a as soon as possible.

Overview

Fabric OS v4.4.1a has the same features included in Fabric OS v4.4.1. Fabric OS v4.4.1 is functionally identical to Fabric OS v4.4.0, except for the following enhancements and new features:

- Brocade Fabric OS v4.4.1 is a maintenance release that supports the IBM @server BladeCenter™ enterprise chassis and introduces support for the IBM @server BladeCenter™ T chassis. The SilkWorm 3016 has been certified as NEBs compliant and the associated Fabric OS changes will allow the same SilkWorm 3016 embedded switch to be inserted into either a IBM @server BladeCenter™ enterprise or T chassis.
- New command: **enclosureShow**

  The **enclosureShow** command displays the identifier of the enclosure interface to which the switch is attached. For more information, refer to the section *Commands Added in Fabric* OS v4.4.1.

For a list of the new features introduced in Fabric OS v4.4.0, refer to the section *New Features in Fabric OS v4.4.0*.

Supported Switches

Fabric OS v4.4.1 supports the SilkWorm 3016, 3250, 3850, 3900, and 4100 switches and the SilkWorm 12000 and 24000 directors.

OS Requirements

Table 1 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 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.

Table 1: OS Requirements

	SilkWorm 2000 Series	SilkWorm 3200 & 3800	SilkWorm 3250, 3850, 3900, 12000, & 24000	SilkWorm 3016	SilkWorm 4100	Fabric Manager
General compatibility[1]	v2.6.1 or later	v3.1.0 or later	v4.1.0 or later	v4.2.1 or v4.4.0b 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	v4.2.1 or later	v4.4.0b	3.0.2c or later
Recommended software versions	v2.6.2	v3.2.0	v4.4.0b	v4.2.1a or later	v4.4.0b	4.4.0 or later[2]

1 SilkWorm 3016 is supported by Fabric OS v4.2.1x (v4.4.1b or later in a IBM @server BladeCenter™ T chasis)
SilkWorm 3250, 3850, and 24000 are supported by Fabric OS v4.2.0 or later.
SilkWorm 3900 is supported by Fabric OS v4.1.0 or later.

2 SilkWorm 3016, 3250, 3850, and 24000 are supported by Fabric Manager 4.1.1 or later.
SilkWorm 4100 is supported by Fabric Manager 4.4.0 or later.

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 three sets of information immediately available when you call:

1. **General Information**

   - Technical Support contract number, if applicable
   - Switch model
   - Switch operating system version
   - Error 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: Provide the switch WWN. Use the **wwn** command to display the switch WWN.

Standards Compliance

Brocade Fabric OS v4.4.1 conforms to the following Fibre Channel Standards in a manner consistent with accepted engineering practices and procedures. In certain cases, Brocade might add proprietary supplemental functions to those specified in the standards. Brocade verifies conformance with Fibre Channels Standards by subjecting its switches to SANmark Conformance Tests developed by the Fibre Channel Industry Association. Brocade switches have earned the SANmark logo, indicating such conformance. SANmark is a limited testing program and does not test all standards or all aspects of standards. For a list of standards conformance, please visit the following Brocade web site:

- *http://www.brocade.com/sanstandards*

New Features in Fabric OS v4.4.0

Brocade Fabric OS version 4.4.0 contains 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 3016, 3250, 3850, and 24000 distance support up to 200 km at 1 Gbit/sec and 100 km at 2 Gbit/sec
    - SilkWorm 4100 distance support 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 supports two links up to 50 km at 2 Gbit/sec and four links at 10 km at 2 Gbit/sec
    - SilkWorm 4100 supports three links up to 250 km at 2 Gbit/sec and 100 km at 4 Gbit/sec
- Increased scalability to 2560 ports and 56 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.

The major features incorporated in Fabric OS v4.4.0 are summarized in Table 2.

Table 2: Major Features Incorporated in Fabric OS v4.4.0

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 ▪ Eight-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 3016, 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, all Bloom ASIC-based platforms, with v4.4.0) is only supported at 2 Gbit/sec speed, as follows:
4 links at 10 km @ 2 Gbit/sec per trunk group
3 links at 25 km @ 2 Gbit/sec per trunk group
2 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>
<tr><td>MPRS Enhancements</td><td>Max hop count (SilkWorm Multiprotocol Router Model AP7420) – CLI only
WAN_TOV (FC Router) – CLI only</td><td>v3.2.0, v4.4.0
v3.2.0, v4.4.0</td></tr>
</table>

Category	Feature	Release
Scalability	Supports 1280 total ports and 34 domains with or without security enabled.	v3.2.0, v4.4.0
	Supports 2560 total ports and 56 domains in a fabric consisting of switches 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

Important Notes for Fabric OS v4.4.1

In addition to the Important Notes for Fabric OS v4.4.0, you should be aware of the following information when running Fabric OS v4.4.1:

Firmware Upgrade

Fabric OS v4.x firmware upgrades include the *release.plist* file. There is a separate *release.plist file* for each platform; the correct one is automatically selected when the **firmwareDownload** command is executed. Provide the full path name to the top-level directory; do not attempt to locate the *release.plist* file in the top-level directory. For more information, refer to the *Fabric OS Command Reference Manual*.

Important Notes for Fabric OS v4.4.0

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

Advanced Web Tools

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, as identified in Table 3.

Table 3: Advanced Web Tools Compatibility Limitations

Launch Switch Environment	Problems
Firmware: Fabric OS v3.1.0+ or v4.1.0+ **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 v3.1.0+ or v4.1.0+ 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.
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.

Launch Switch Environment	Problems
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.
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 (Brocade Advanced Performance Monitoring) on a local switch with a Fabric OS prior to v4.4.0, the SilkWorm 4100 is displayed as a 16-port switch. **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.

SilkWorm 3016

Table 4 lists other important information you should be aware of specific to the SilkWorm 3016.

Table 4: SilkWorm 3016 Important Notes

Problem Area	Description
ifModeSet command unsupported	**Issue:** Use of the **ifModeSet** command is unsupported. Do not use the **ifModeSet** command to change the operating mode of the "eth0" interface to the Brocade SilkWorm 3016 for **IBM @server®BladeCenter™**. The internal Ethernet in the **IBM @server® BladeCenter™** chassis operates exclusively in fixed 100-Mbit full-duplex mode. Using **ifModeSet** could disconnect your Ethernet connection to the SilkWorm 3016. **Workaround:** The "eth0" interface operating mode is correctly set (to 100-Mbit full-duplex) each time the Silkworm 3016 is rebooted. If Ethernet connectivity is lost due to a mode change, the switch can be reset using the management module's chassis-management application.
Trunking and long-distance mode unsupported	The SilkWorm 3016 switch does not support trunking mode or long-distance mode on internal ports (ports 1 through 14). If you try to enable trunking or long-distance mode on ports 1 through 14, the command line interface and Advanced Web Tools return an error message.
Diagnostic commands	The diagnostic commands **fportTest** and **portTest** are not supported on the internal ports 1 through 14. The commands **spinSilk** and **spinJitter** must be run with the additional argument *-lb_mode 2* on the SilkWorm 3016 switch's internal ports. If these commands are run without this argument, they fail on all internal ports, because they default to external loopback mode, which requires a loopback plug or cable.

Problem Area	Description
Extended links	The user must be very careful when using the Brocade Extended Fabrics optionally licensed feature with the SilkWorm 3016 switch. The Extended Fabrics feature allows the user to configure external ports (0 and 15) for long-distance performance; however, certain long-distance configurations can disable the other external (and possibly some internal) ports, as well as possibly causing a disruption in traffic. When considering configuring external ports for long distance, both the port speed (1 or 2 Gbit/sec) and distance setting (L0.5, L1, L2, and LD) must be considered. The two internal ports 9 and 10 might be disabled due to long-distance configuration of the external ports. For external ports operating at 2 Gbit/sec, the following restrictions should be observed: • Setting two ports to L2 (100 km) is not allowed. • Setting one external port to L2 (100 km) and the other external port to L0.5 (25 km) will disable two internal ports. • If you set one external port to L2 (100 km) and the other external port is an E_Port, then one internal port will be disabled. • Setting both external ports to L1 (50 km) will disable two internal ports. • Setting one external port to L1 (50 km) and the other external port to L0.5 (25 km) will disable one internal port. • If you set one external port to L1 (50 km) and the other external port is an E_Port, then one internal port will be disabled. • Setting both external ports to L0.5 (25 km) will disable one internal port. Using the LD setting for the external ports will create uncertain results. LD mode autosenses the actual cable lengths and, depending on their distances, might disable internal and/or external ports, as described earlier. For example, if the two external ports are set to LD and the cable lengths are both 50 km, then internal ports 9 and 10 will be disabled. For more information regarding extended fabric setup and usage, refer to *Brocade Distributed Fabrics User's Guide* v3.1.0/4.1.0.
IP address configuration	The Ethernet IP address, Ethernet subnet mask, and gateway IP address should not be configured using local mechanisms on the switch, such as the **ipAddrSet** CLI command or Advanced Web Tools. On the SilkWorm 3016, the values must be configured using the **IBM @server® BladeCenter** Management Module's chassis-management GUI, because all IP Ethernet access to the switch module itself is forwarded through the Management Module. If the switch IP address information is changed without changing the Management Module configuration, then telnet access to the switch will very likely be lost. Note that this restriction does not apply to the Fibre Channel IP address and the Fibre Channel subnetmask (also referred to as the "in-band IP address" and "subnetmask"). These can still be configured using any of the standard switch-management mechanisms.

Problem Area	Description
Management using IP over FC	To manage the Brocade SilkWorm 3016 switch using IP over FC, both the IP address and subnet need to be set to 0.0.0.0. As a result of an error message from the IBM @server® BladeCenter Management Module on these changes, the implementation of single Ethernet connection (SEC) on the SilkWorm 3016 can be deployed only as the Ethernet-to-FC router, not as a switch using IP-over-FC addressing only.
switchShow command	The **switchShow** command indicates the CU port state as No_Light when no Fibre Channel signal is received from an internal port on the SilkWorm 3016.

Security Enablement	Use the userRename command to change the user-level ID to "user" and the admin-level ID to "admin" on the local switch if the following error message displays after you issue the secModeEnable command:
	`Switch does not have all default account names.`
	Use the **userRename** command to change the user IDs on the specified domain if the following error message displays:
	`Error from domain <domain ID>: Switch does not have all default account names.`
	Refer to the *Fabric OS Command Reference Manual* for **userRename** command details.

Fabric Watch	An additional Fabric Watch element, the F/FL Port Class, has been added to allow the monitoring of the 14 internal copper ports. Refer to the *Brocade Fabric Watch User's Guide,* for more detailed information.

SilkWorm 4100

Table 5 **Error! Reference source not found.**lists other important information you should be aware of regarding the SilkWorm 4100.

Table 5: SilkWorm 4100 Important Notes

<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>FTRJ-1319P1BTL-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>
<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 blinks, indicating an error.</td></tr>
</table>

SilkWorm 4100	Description
Fan, RPM reading	The RPM range can differ by as much as 1000 RPM from fan to fan, which is within Brocade's specification. 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.
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

Table 6 lists other important information you should be aware of regarding the SilkWorm 12000.

Table 6: SilkWorm 12000 Important Notes

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

Fabric OS

Table 7 lists other important information you should be aware of regarding Fabric OS.

Table 7: Fabric OS Important Notes

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 trunk configuration (as a result, for a period of time, traffic through those ports could be disrupted).
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**.**

Fabric OS Area	Description

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.
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.
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 by Sun. The immediate workaround is to select an odd-numbered syslogd facility level when using the **syslogdFacility** command.

Fabric OS Area	Description
Logging, **supportFTP** command	When setting the automatic FTP IP address, userid, 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 *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: all persistent errors (all messages) will be erased on v4.4 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.

Fabric OS Area	Description
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.
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 sectelnet client prints the message 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 to v4.4.
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.

Fabric OS Area	Description
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.
Support	Fabric OS v4.4.0 (and later) users should run the **supportSave** command instead of, or in addition to, the **supportShow** command. Doing so will gather additional switch details and 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 (and later) 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.
SilkWorm 12000 large fabric constraints	Extreme stress-test conditions in a large fabric configuration (over 2000 ports) show that the SilkWorm 12000 platform could 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/enable repeatedly in quick succession over long periods of time. Subjected to these stress-test conditions, 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
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. • 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 nonoperational. **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, the user must ensure that the size of the zone configuration does not exceed the minimum size supported by all the switches in the fabric. Zone configuration sizes can be determined by executing **cfgSize** on all the switches in the fabric.

Changes in Fabric OS v4.4.1 Unique to the SilkWorm 3016

- The SilkWorm 3016 switch can now be inserted into either the **IBM @server® BladeCenter™** Enterprise or **IBM @server® BladeCenter™** T blade server chassis. It can also be removed from one and installed in the other. Fabric OS v4.4.1 adds functionality that will detect in which chassis the Silkworm 3016 has been installed and will set parameters accordingly.

The **IBM @server® BladeCenter™** T chassis has only eight internal server bays compared to the **IBM @server® BladeCenter™** Enterprise chassis, which has fourteen. The six unused internal ports (ports 9-14) on the SilkWorm 3016 are displayed in GUIs but always with dark LEDs. In addition, for all CLI commands (such as **switchShow** or **portShow**), ports 9-14 report as "disabled (persistent)" ports. These ports cannot be enabled using Web Tools or the CLI when the SilkWorm 3016 is installed in the **IBM @server® BladeCenter™** T chassis. If the SilkWorm 3016 is moved from the **IBM @server® BladeCenter™** T chassis, then ports 9-14 can be enabled and used.

Commands Added in Fabric OS v4.4.1

enclosureShow

A command for embedded Fibre Channel switches that identifies the blade server in which the switch is installed.

SYNOPSIS

enclosureShow *attribute*

AVAILABILITY

all users

DESCRIPTION

Use this command to display attributes of the blade server chassis. Currently, supported attributes are the vendor-specific blade server chassis identifier, vendor-specific blade server chassis model name, and the identifier of the blade server chassis interface to which the switch is attached.

OPERANDS

attribute	Attribute of the enclosure to display.
id	Display the vendor-specific blade server chassis identifier.
modelname	Display the vendor-specific blade server chassis model-name.
slotid	Display the identifier of the blade server chassis interface to which the switch is attached.

EXAMPLE

Display the identifier of the enclosure interface to which the switch is attached.

```
switch: admin> enclosureShow modelname
    Enterprise T
```

Documentation Updates

Table 8 lists the documents that support Fabric OS v4.4.1.

Table 8: Documentation Supporting Fabric OS v4.4.1

Title	Part Number
Advanced Web Tools Administrator's Guide	53-0000522-07
Fabric OS Command Reference Manual	53-0000519-09
Fabric OS Features Guide	53-0000395-02
Fabric OS MIB Reference Manual	53-0000521-08
Fabric OS Procedures Guide	53-0000518-06
Fabric OS System Error Message Reference Manual	53-0000515-09
Fabric Watch User's Guide	53-0000524-05
Secure Fabric OS QuickStart Guide	53-0000352-04
Secure Fabric OS User's Guide	53-0000526-04

The most recent documentation is available on Brocade Connect:

http://www.brocadeconnect.com/

This section provides information on last-minute additions or corrections to the documentation listed in Table 8.

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 with the following text:

-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 Watch User's Guide

(Publication number 53-0000524-05)

The following rows replace the existing rows "Link Failure Count," "Invalid CRC 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 Informative

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
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
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 "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.

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-numbered group of inactive ports 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-5), 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 or 2 Gbit/sec 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 1through5). 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 (1through 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;verify that the command has completed and displayed the message "Cleaning up kernel modules.....Done".

   b. From the active CP card session, log in to Switch 0 by entering the **login** command, logging in as admin, and then entering **0** to log in to Switch 0.

   c. Enter the **switchShutdown** command to ensure a graceful shutdown of Switch 0; verify that 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)

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 v4.4.1a

Defects Closed in Fabric OS v4.4.1a		
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 v4.4.1a		
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 does not 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

Defects Closed in Fabric OS v4.4.1a		
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: Fabric OS v4.4.x introduced a name server zone cache as a scalability enhancement. During the firmware upgrade to 4.4.x, the previous code base (v4.1x/4.2.x) did not generate the name server□s copy in the standby, as this was not a feature in previous versions of the OS. When Fabric OS v4.4.x does a warm recovery, it has an empty zone database in the Name Server which results in the wrong zone member list cached in the name server (NS) database. Any RSCN will cause the host driver to resynchronize its information with the Name Server, which currently holds incorrect information. As a result, the host driver logs into every device in the fabric (PLOGI). Even though the Zone Server correctly enforces zoning, the fabric is stressed as devices flood the fabric with PLOGIs requests. Large fabric configurations may cause the switch to disable interrupts and cause the traffic to stop. An installation could mitigate the impact by doing a cfgEnable command immediately after a firmware upgrade. The cfgEnable would properly 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

Defects Closed in Fabric OS v4.4.1a		
Defect ID	**Severity**	**Description**
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: The current detection of bad idles is too sensitive, causing unnecessary link resets. The software change is made to accommodate temporary loss of sync condition per FC standards. However, FOS 4.4.0b will ignore spurious invalid primitives, it relies on port fault mechanism to reset the link. FOS 4.4.1a and later will not rely on port fault mechanism but will reset link based on loss of signal detection. 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
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

Defects Closed in Fabric OS v4.4.1a		
Defect ID	**Severity**	**Description**
DEFECT000051911	Medium	Summary: SilkWorm 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