Brocade Fabric OS v4.1.2b

Release Notes_v1.0

November 13, 2003

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v4.1.2b Release Notes_v1.0	First release	November 13, 2003

TABLE OF CONTENTS

Document History....1
Overview....4
About This Release....4
Supported Switches....4
Technical Support....4
Information About Secure Fabric OS....5
Supporting Documentation....5
Standards Compliance....6
Documentation Updates....6
Brocade SilkWorm 3900 Hardware Reference Manual....6
Brocade Diagnostic and System Error Messages Manual, v4.1.2....7
Brocade Fabric OS Procedures Guide, v4.1....8
Brocade Fabric OS Procedures Guide, v4.1....8
Brocade ISL Trunking User's Guide, v3.1.0/4.1.0....10
Brocade Fabric OS Reference, v4.1.2....10
Brocade Fabric OS, v4.1.0 Release Notes Brocade Fabric OS, v4.1.1 Release Notes....10
Brocade Fabric OS, v4.1.1 Release Notes....10
Requirements and Compatibility....11
Important Notes....11
Security....11
Cascaded Environment....11
Maximizing Fabric Availability During SW 3900 (2109-F32) Hot Code Activation....12
Microsoft Internet Explorer Issue....12
Interpreting Ambient and Internal Temperatures....12
Other Important Notes....13
Defects Closed in Fabric OS v4.1.2b....16
Defects Closed in Fabric OS v4.1.2a....17

Overview

Fabric OS v4.1.2b is a patch release that contains fixes to a small number of additional issues found since the release of Fabric OS v4.1.2. Brocade software release policy is to carry forward all fixes in patches to subsequent maintenance and feature releases of Fabric OS. Aside from these changes, Fabric OS v4.1.2b is functionally identical to Fabric OS v4.1.2.

Fabric OS v4.1.2b is an upgrade and replacement for the Fabric OS v4.0.2, v4.1.0, and 4.1.1. Fabric OS v4.1.2b has completed IBM FICON certification and qualification.

Note the following:

- Starting with Fabric OS v4.1.2, FICON mode has been eliminated, implementing a new requirement from IBM during the certification process.
- The in-band FICON management server, also known as CUP (Control Unit Port), will not be a supported feature of Fabric OS v4.1.2. Brocade intends to support it in a future Fabric OS version.
- Fabric OS v4.1.2 is supported by the following releases of the Fabric Access API and Fabric Manager:
  - Fabric Access Layer 3.0.1 (the Fabric Access API)
  - Fabric Manager 4.1.0 and later

About This Release

Fabric OS v4.1.2b includes fixes to defects as detailed in the section "Defects Closed in Fabric OS v4.1.2b."

Supported Switches

This release supports SilkWorm 3900 (2109-F32) and SilkWorm 12000 (2109-M12) switches.

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 to 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 messages received
- **supportshow** command output
- Detailed description of the problem and specific questions
- Description of any troubleshooting steps already performed and results

[1] FICON is a registered trademark of IBM Corporation in the U.S. and other countries.

2. Switch Serial Number

The switch serial number is provided on the serial number label, as shown here.

Type 2109-M12	**Type 2109-F32**
S/N PPSSSSS	**S/N PPSSSSS**

The serial number label is located as follows:

- *SilkWorm 2000 series (3534-1RU) switches:* Bottom of chassis
- *SilkWorm 3200 (3534-F08) and 3800(2109-F16) switches: Front and bottom* of chassis
- *SilkWorm 3900 (2109-F32) switches: Front and b*ottom of chassis
- *SilkWorm 6400 and 12000 (2109-M12) switches:* Inside front of chassis, on wall to left of ports

3. Worldwide Name (WWN)

- *SilkWorm 3900 (2109-F32) and 12000(2109-M12) switches:* Provide the license ID. Use the **licenseidshow** command to display the license ID.
- *All other SilkWorm (1RU/S08/S16/F08/F16) switches:* Provide the switch WWN. Use the **wwn** command to display the switch WWN.

Information About Secure Fabric OS

Brocade Secure Fabric OS® is a comprehensive security product that requires some planning and specific steps to set up. For this purpose, the following document should be reviewed as a minimum of preparation prior to starting:

- *Brocade Secure Fabric OS QuickStart Guide*

More detailed product information can be obtained from the *Brocade Secure Fabric OS User's Guide*.

Supporting Documentation

SilkWorm switch hardware documentation:

- *SilkWorm 3900 QuickStart Guide (provided as hardcopy with the switch)*
- *SilkWorm 3900 Hardware Reference Manual*
- *SilkWorm 12000 Hardware Reference Manual*
- *SilkWorm 12000 QuickStart Guide*

Brocade Fabric OS v4.1 software documentation:

- *Brocade Fabric OS Reference*
- *Brocade Fabric OS Procedures Guide*
- *Brocade Advanced Zoning User's Guide*
- *Brocade Advanced Web Tools User's Guide*
- *Brocade Advanced Performance Monitoring User's Guide*
- *Brocade Distributed Fabrics User's Guide*
- *Brocade Fabric Watch User's Guide*
- *Brocade ISL Trunking User's Guide*
- *Brocade Secure Fabric OS User's Guide*
- *Brocade MIB Reference*

- *Brocade Diagnostic and System Error Message Reference*

The primary documentation for this release is the Fabric OS 4.1.0 documentation set as described above. In addition, updates were made to the following manuals for FICON environments:

- *Brocade Advanced Web Tools User's Guide, v4.1.2*
- *Brocade Diagnostic and System Error Messages, v4.1.2*
- *Brocade Fabric OS Reference, v4.1.2*
- *Brocade Glossary, v4.1.2*
- *Brocade MIB Reference Manual, v4.1.2 (also supports v4.1.0, 4.0.2x, 3.1.0, 3.0.x, 2.6.x)*
- *Brocade Support for FICON® Reference Guide, v4.1.2*

Standards Compliance

Brocade Fabric OS v4.1.2 is compliant with the following Fibre Channel Standards:

- FC-AL ANSI X3.272: 1996
- FC-AL-2 NCIT S 332: 1999
- FC-FLA NCIT S TR-20: 1998
- FC-GS-3 NCITS 348-2000 Rev 7.01
- FC-FG ANSI X3.289: 1996
- FC-PH ANSI X3.230: 1994
- FC-PH-2 ANSI X3.297: 1997
- FC-PH-3 ANSI X3.303: 1998
- FC-PLDA NCIT S TR-19: 1998
- FC-SW-2 Rev 5.3
- FC-VI Rev 1.61
- FC-MI Rev 1.92
- FC-SB-2 Rev 2.1 (FICON support)
- FC-BB Rev 4.7
- FC-FS Rev 1.7 (still in draft)
- FC-BB-2 Rev 5.3 (still in draft)
- IPFC RFC 2625
- FCP ANSI X3.269: 1996
- FCP-2 Rev 7

Documentation Updates

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

Brocade SilkWorm 3900 Hardware Reference Manual

(Publication number 53-0001595-02)

The following statement should be added to the Port Status LED information for when the port status is offline in Table 3-1, “Port-Side LED Patterns During Normal Operation,” on page 3-2:

> “When a Port Status LED indicator light is off, it is possible that another hardware status is offline.”

Brocade Diagnostic and System Error Messages Manual, v4.1.2

(Publication number 53-0000516-06)

The message text and severity level for the MSFICON-SWITCH_NID error message has been updated for Fabric OS v4.1.2a (since Fabric OS v4.1.2). The Probable Cause and Recommended Action are the same for the error message in both releases.

The error message was not documented in the *Brocade Diagnostic and System Error Messages Manual*, *v4.1.2*. The updated error message should be added to the documentation.

MSFICON-SWITCH_NID *(in Fabric OS v4.1.2a)*

Message

```
<switch number> Info MSFICON-SWITCH_NID, 4, Chassis FRU header not programmed for
switch NID, using defaults (applies only to FICON environments).
```

Probable Cause

Custom switch node descriptor (NID) fields have not been programmed in nonvolatile storage. Therefore, the default Brocade values are used. Note that the Switch Node Descriptor is used only in the SB-3 ELS frames: Request Node Identification Data (RNID) and Registered Link Incident Record (RLIR). The use of SB-3 link incident registration and reporting is typically limited to FICON environments.

Recommended Action

No action is required if SB-3 link incident registration and reporting is not used by the host or if default values are desired for the switch-node-descriptor fields. If custom values are required, then these fields can be set using the root-level command **fruInfoSet**.

Severity

Information

MSFICON-SWITCH_NID *(in Fabric OS v4.1.2)*

Message

```
<switch number> Warning MSFICON-SWITCH_NID, 3, Chassis FRU header unusable for
switch NID using defaults
```

Severity

Warning

Brocade Fabric OS Procedures Guide, v4.1

(Publication number 53-0000518-02)

The following information should be added to Step 7 of the procedure on page 4-11 of Chapter 4, "Firmware Downloads," section "Performing Firmware Upgrades," subsection "Upgrading the Firmware on the SilkWorm 12000":

> "When the v4.1.0 firmware is unzipped, it creates a folder and a set of firmware files. Use the following directory and file name when downloading this firmware to the switch:
>
> /v4.1.0/release.plist.
>
> "At the User prompt, enter a User ID that has an account on the FTP server."

Brocade Fabric OS Procedures Guide, v4.1

(Publication number 53-0000518-02)

The following section should be added to Chapter 16, "Guide to Port Logs":

Decoding FICON Events

FICON uses the **portlogDump** command output to measure task-execution performance and to obtain queue statistics. Use this event information to analyze the management server ELS processing during the Fibre Connection link initialization.

PortlogDump logs the following ELS entries:

- ELS RNID: 78
- ELS LIRR: 7A
- ELS QSA: 7E

Refer to the *Brocade Fabric OS Reference Manual* for more information regarding the different port log commands.

Entry Descriptions

Each FICON entry in the port log contains the following information.

Name	Description	Location in Argument
Entry log time	Time that the entry was created in the port log	
Process	msd (Management Server Daemon) – Confirms FICON thread executes FICON requests	
Event	Ficonq (FICON queue statistics)	
Port	Physical port number	
Exchange ID	Exchanged ID number	Argument 0
ELS	ELS code (1 byte)	Argument 1, first byte
DID	Destination ID (3 bytes)	Argument 1, 3 bytes
SID	Source ID	Argument 2

Queue age	Number of milliseconds the message was in the queue before FICON processed it (2 bytes)	Argument 3, first 2 bytes
Queue size	Number of messages still in the queue at the time FICON starts to process the current message (2 bytes)	Argument 3, second 2 bytes
Error code	Absolute value of return code from the processing of the ELS request (2 bytes)	Argument 4, first 2 bytes
Wall time in seconds	Number of seconds that the current task took (2 bytes)	Argument 4, second 2 bytes
Wall time in microseconds	Number of microseconds that the current task took (2 bytes)	Argument 5

FICON Port Log Examples

To display FICON port logs of port 43:

```
switch:admin> portlogdumpport 43 | grep ficonq
13:15:57.093   msd     ficonq  43      005c8 7effffd,00502b00,00000000,00000000,00006103
13:15:57.159   msd     ficonq  43      005c7 7affffa,00502b00,00000000,00000000,00060442
13:15:57.223   msd     ficonq  43      005d0 78fffffd,00502b00,00100000,00000000,00063014
13:15:57.236   msd     ficonq  43      005cb 7affffa,00502b00,00200000,00000000,00012720
```

Use the following table to interpret the FICON port log information.

Name	Value
Entry log time	13:15:57.093
Process	msd
Event	ficonq
Port	43
Exchange ID	005c8
ELS	`7e` (ELS QSA)
DID	fffffd
SID	00502b00
Queue age	0000
Queue size	0000
Error code	0000
Wall time in seconds	0000
Wall time in microseconds	`00006103`

Brocade ISL Trunking User's Guide, v3.1.0/4.1.0

(Publication number 53-0000520-02)

Page 1-3 of the *Brocade ISL Trunking User's Guide*, v3.1.0/4.1.0, contains the following statement:

> "... ISL Trunking does not support the "LE", "L1", or "L2" **portcfglongdistance** modes. For information about these modes and Extended Fabrics in general, refer to the *Distributed Fabrics User's Guide*."

This statement should be modified to say the following:

> "...Trunking is supported for normal E_Ports (referred to as L0 in the **portcfglongdistance** command) with LWL media up to 5 km at the full speed permitted by the link. With LWL media, the throughput begins to fall off beyond 5 km, due to normal latency effects. ISL Trunking does not support the LE, L1, or L2 **portcfglongdistance** modes. For information about these modes and Extended Fabrics in general, refer to the *Distributed Fabrics User's Guide*."

Brocade Fabric OS Reference, v4.1.2

(Publication number 53-0000519-06)

There are changes to the **supportshow** command not documented in the *Brocade Fabric OS Reference*. The command has been modified to include the following information under the services group:

```
ficonDbg dump rnid
ficonDbg rnid
ficonShow ilir
ficonShow lirr
ficonShow rlir
ficonShow rnid
ficonShow switchrnid
```

Brocade Fabric OS, v4.1.0 Release Notes
Brocade Fabric OS, v4.1.1 Release Notes

In Fabric OS v4.1.0 and v4.1.1 Release Notes, the SilkWorm 2*xxx* (S08/S16/1RU) Scalability Limit section specifies that fabrics containing Fabric OS v2.6.1 or later should not exceed 500 user (non-ISL) ports or devices. Brocade has increased to 728 devices the maximum number of devices supported in fabrics that include SilkWorm 2000 (S08/S16/1RU) series switches running Fabric OS v2.6.1 or later. This is only a change to the documentation; there is no change to the Fabric OS.

Brocade Fabric OS, v4.1.1 Release Notes

In the Fabric OS v4.1.1 Release Notes, the "Important Notes" section stated that the commands **moredisable** and **moreenable** were added to the Fabric OS. This should read, "The commands **moredisable** and **moreenable** are not available for Fabric OS v4.x."

Requirements and Compatibility

Brocade Fabric OS v4.1.2 can be installed and run on SilkWorm 3900 (2109-F32) and SilkWorm 12000 (2109-M12) switches.

The following table summarizes the versions of Brocade firmware and software that are supported in conjunction with these releases:

	2109-S08/S16 & 3534-1RU	2109-F16 3534-F08	2109-F32	2109-M12	Fabric Manager
General compatibility	2.6.0c or later	3.0.2c or later	4.0.2 or later	4.0.0c or later	3.0.2c or later
With Secure Fabric OS enabled	2.6.1 or later	3.1.0 or later	4.1.0 or later	4.1.0 or later	3.0.2c or later
Recommended adjacent to 2109-F32 running 4.1.0 or later	2.6.1 or later	3.1.0 or later	4.1.0 or later	4.1.0 or later	3.0.2c or later
FICON environment	n.a	n.a	n.a,	4.1.2 or later	4.1.0 or later

Note: For Fabric OS v2.x or v3.x switches, the Core Switch PID Format must be enabled (that is, set to 1) using the **configure** command before it can interconnect with the SilkWorm 3900 (2109-F32) and SilkWorm 12000 (2109-M12). For more information regarding the Core Switch PID Format, refer to "Updating the Core PID Format" in the *Fabric OS Procedures Guide*.

For more information about configuring SilkWorm 2000 (S08/S16/1RU)- or 3000 (F08/F16) - series switches or the SilkWorm 6400 integrated fabric to interoperate in the same fabric with the SilkWorm 3900 (2109-F32) and SilkWorm 12000 (2109-M12) switches, contact your switch provider.

Important Notes

This section includes the following topics:

- Security
- Cascaded Environment
- Maximizing Fabric Availability During SW 3900 (F32) Hot Code Activation
- Microsoft Internet Explorer Issue
- Interpreting Ambient and Internal Temperatures
- Other Important Notes

Security

A security problem was observed in which an invalid certificate was not detected and the **secmodeenable** command completed successfully. (Copying the certificate file into itself created the invalid certificate.)

Cascaded Environment

Secure Fabric OS is required in a cascaded environment or a noncascaded environment using 2-byte addressing to ensure the presence of a high-integrity fabric. Secure Fabric OS provides a FICON environment with integrity checking to confirm whether a switch in a cascaded environment is allowed to join the fabric by determining if the

WWN and domain IDs are acceptable. The fabric maintains a list (domain IDs and WWNs) of switches and ports that are allowed to join. If the integrity check fails, the switch or port attempting to join is prevented from establishing a connection.

Additionally, at link initialization, the FICON host queries the attached F_Port for its security attributes (Security Enabled, Fabric Wide Insistent Domain ID (IDID) mode set and SCC_Policy Activated) If any of the conditions are not met, the attached F_Port is placed in the Invalid Attachment state by the host, which prevents any frame transmission over that link.

Maximizing Fabric Availability During SW 3900 (F32) Hot Code Activation

During code activation on a SilkWorm 3900 (2109-F32) running Fabric OS 4.1.0 or later, data keeps flowing between hosts and storage devices. However, fabric services are unavailable for a period of approximately 50-55 seconds. Possible disruption of the fabric can be minimized by ensuring that switches logically adjacent to the SW 3900 (2109-F32 directly connected via an ISL) are running Fabric OS 2.6.1 or later, 3.1.0 or later, or 4.1.0 or later. More information is available in the "Firmware Download" section of the *Fabric OS Procedures Guide*.

Microsoft Internet Explorer Issue

An issue has been identified with Microsoft Internet Explorer 5.0 and 5.5 running on Windows NT 4.0. Normally, when you launch a copy of the Switch Explorer applet, the left panel displays a tree of switches in your fabric. Clicking on a tree node will cause the right panels to refresh to the currently selected switch. However, under NT 4.0 and IE 5.0/5.5, the right panel will *not* update for the second and subsequent instance of the Switch Explorer. Only the first instance works.

This issue has been identified and confirmed by Microsoft. For details, see the URL http://support.microsoft.com/default.aspx?scid=KB;en-us;242167&.

Workaround: There are twoworkarounds for this:

1. Always use a single instance of SwitchExplorer on NT 4.0 and IE 5.0/5.5
2. Install IE 6.0 SP1

Alternatively, you might obtain a workaround directly from Microsoft for this problem. Please contact Microsoft support and supply them the information in the defect as described in the URL http://support.microsoft.com/default.aspx?scid=KB;en-us;242167&.

Interpreting Ambient and Internal Temperatures

Brocade SilkWorm fabric switches are instrumented with temperature sensors to monitor the operating characteristics of the products and their environment. The following table explains how to interpret the various temperature readings that might be reported via Fabric OS v4.1.x and monitored via the Fabric Watch optional licensed firmware product. All temperatures are degrees C.

Sensor	Minimum	Maximum	Comments
SilkWorm 12000 (2109-M12)			
Blowers	0	40	Sensor on each blower measures inlet (ambient) air temperature.
Port Blades	0	74	Each port blade has its own temperature sensor. Warning at 75° C.; blade shutdown at 80° C.
CP Blades	0	74	Each CP blade has its own temperature sensor. Warning at 75° C.; CP will be faulted at 80° C.
SilkWorm 3900 (2109-F32)			
Switch	0	69	Switch sends warning at internal temperature of 67° C. Switch begins 2-minute controlled shutdown at 69° C.

Other Important Notes

This table lists important information you should be aware of regarding Fabric OS v4.1.x.

Area	Description
Ethernet port IP addresses	**NOTE:** When a SilkWorm 12000 (M12) 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, since the association between the IP addresses and MAC addresses has changed.
Fabric OS CLI commands, failover and port disable	**NOTE:** Changing port configurations during a failover might cause ports to be in a disabled state. Reissue the command after the failover is complete to bring the port online.
Fabric OS commands	**Problem:** Under the root account, issuing Fabric OS commands in parallel through scripts could cause the Kernel task to consume excessive memory. **Solution:** When using scripts to issue Fabric OS commands, it is always a good practice to wait for the command to finish before issuing another command.
Fabric OS switch beaconing	**NOTE:** Switch beaconing is not preserved across a failover. If you start beaconing, a failover will cause all lights to stop flashing. **Solution:** If this occurs, reissue the command to resume switch beaconing.
Fabric OS, switch reboot and blade repair	**Problem:** Switch reboot will fail in the SilkWorm 12000 (M12) if there are faulty port blades. **CAUTION: Verify all blades are in working order before performing a switch reboot. Switch reboot is meant to be issued after all repairs are complete. If you do a switch reboot and find a faulty blade, remove the blade and reboot will continue.** **Solution:** Identify and remove the faulty blade using the **slotshow** command to reboot successfully.
Fabric routing, Fabric Manager: domain overlap	**NOTE:** Issuing a **configdefault** command followed by reboot or switch disable/enable will cause the fabric to segment due to possible domain overlap. **Solution:** Before rebooting the fabric, ensure all switches are properly configured to avoid domain overlap between the logical switches.
Fabric Device Management Interface (FDMI)	**NOTE**: An HBA will be allowed to register even though the originating port is not in the HBA's registered port list. This is intended behavior included in order to test error cases.
Firmware download	**NOTE:** Please review the "Firmware Download" section of the *Fabric OS Procedures Guide* before upgrading your firmware.
Firmware download	**Problem:** During a firmware download, rebooting or power cycling the CPs could cause the compact flash to be corrupted. **CAUTION: Do not attempt to power off the CP board during firmware download to avoid high risk of corrupting your flash.**

Area	Description
HA switch reboot failure	**NOTE:** When a switch reboot or a failover occurs before POST is complete, the HA resynchronization will be disrupted. HA will not resynchronize until POST completes. **CAUTION: Allow POST to complete before performing a switch reboot or failover to avoid disruptive failover.**
IP addresses	**CAUTION:** Do not set a switch or CP IP address for the Ethernet interface to 0.0.0.0.
IP addresses	**NOTE:** Supernetting of IP addresses, also known as CIDR, is not supported in Fabric OS.
License removal	**NOTE:** When a user removes a license from the switch, the feature is not disabled until the switch is rebooted or a switch disable/enable is performed.
LTO 2 tape drive support	When using the LTO 2 Tape Drive, the user must perform the following command on both Fabric OS 3.x and 4.x: switch> portcfggport *port# where drive is plugged into* This will allow the tape drive to function in point-to-point mode rather than in loop.
OS - hardware	**NOTE:** Bringing up port blades during a failover could cause the port cards to come up in a disabled state. This is a rare occurrence; when this happens, redo the port blade bringup after the failover on the SilkWorm 12000 (M12).
Security	**NOTE:** 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, FCC list	**NOTE:** Adding switches to the FCC list does not automatically join the switches in a secure fabric. Add the switches to the FCC list and either reset the E_Ports or perform a switch disable and enable for the switches to join.
Security, PKICERT utility	**NOTE:** Before using the PKICERT utility to prepare a CSR, please 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, and any CSRs that do not conform to this requirement will be rejected.
Security, SLAP fail counter and 2 switches	**NOTE:** 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	**NOTE:** To properly connect SSH login, wait for Secure Mode to complete before rebooting or doing HA failover on the SilkWorm 12000 (M12). 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 would change after a HA failover.
Security: empty policies	**CAUTION: If telnet, API, and serial port access policies are empty, the user will not be able to talk to the switch.** **Solution:** Contact switch provider for the recovery procedure.
Security: error counter	**NOTE:** The telnet security error counter will count each violation as 1 plus any auto retries the telnet software executes.

Area	Description
Security: secure mode	**NOTE:** When in Secure Mode, if you upgrade from Fabric OS version 4.0 to 4.1, then downgrade to Fabric OS version 4.0, and upgrade back to Fabric OS version 4.1, the system prompt will ask the user to reset the Secure Mode password.
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 session.** **This is expected behavior. The session will terminate if you change the password in Secure Mode.**
Web Tools and CLI commands	**NOTE:** If you use Web Tools to change the switch name, the SilkWorm 12000 (M12) telnet console prompt will not update to the new name until a new telnet window is opened.
Web tools, java bug	**Problem:** If a dialog box is displayed from the switch admin window of Web Tools and the user selects another dialog box from Web Tools, this causes a window display error. **NOTE:** This is a known defect in Java 1.3 documented at www.java.sun.com, bug ID 4763605. To avoid the display error, open only one dialog box at a time or launch another switch admin session in a separate window.
WWN card FRU repair	**Problem:** If an HA failover or power cycle occurs during a FRU on the WWN card, the SilkWorm 12000 (M12) will become nonoperational. **CAUTION: When performing a FRU on a WWN card, complete the FRU procedure before attempting an HA failover or power cycling the chassis.**
Zoning	**NOTE:** To use Zoning in a non-RCS (Reliable Commit Service) mode fabric (that is, in a fabric containing switches with firmware version other than v2.6.x, v3.1 and v4.1), it is recommended that all appropriate Zoning licenses are installed on all the switches in the fabric before attempting to bring a switch in to the fabric. Furthermore, if the Zoning license is to be removed, the user must make sure it is reinstalled properly on the affected switch before attempting the **cfgenable** zoning operation. Failure to follow these steps can cause inconsistency of Zoning configuration on the affected switches should a zoning operation be attempted from a remote switch in the fabric. On the affected switches, an error message will appear on the console or telnet session (can also be seen by doing **errShow**, **errDump,**) indicating that zoning license was missing.
Zoning	**Problem:** Domain 0 in a zoning configuration file is illegal but was not previously enforced. **NOTE:** Prior to upgrading a switch to 4.1, please ensure that the fabric's zoning configuration does not contain the Domain ID 0 used for zoning. This is specific only to 4.x switches.
FICON	When using fixed 1-GB channels (both G5 and FICON Express), there might occasionally be erroneous link incidents generated by the FICON host when the channels are coming online. These link incidents will result in a call home. Other than the generated link incident, the channel will come online and function normally. In order to avoid this situation, the ports on the SilkWorm 12000 (M12) connected to the 1-GB channels should be configured for fixed 1-GB speed.

Area	Description
FICON	In FICON environments, it is recommended that Dynamic Load Sharing (DLS) be configured to "disabled" on the SilkWorm12000 (M12). With DLS "enabled," traffic on existing ISL ports might be affected when one or more new ISLs is added between the same two switches. Specifically, adding the new ISL might result in dropped frames as routes are adjusted to take advantage of the bandwidth provided by the new ISL. By disabling DLS, there will be no dropped frames. A similar situation occurs when an ISL port is taken offline and then brought back online. When the ISL port goes offline, the traffic on that port will be rerouted to another ISL with a common destination. When the ISL port comes back online and DLS is enabled, the rerouting of traffic back to the ISL port might result in dropped frames. If DLS is not enabled, traffic will not be rerouted back.

Defects Closed in Fabric OS v4.1.2b

Defects Closed In Fabric OS v4.1.2b		
Defect ID	**Severity**	**Description**
DEFECT000035187	High	Summary: Add code to assist Hardware Watchdog debug. Customer Symptom: The symptom seen for the watchdog is an unscheduled automatic reboot on a SilkWorm 3900 (F32) accompanied with the following error messages in the switch error log. Error 02 -------- 0x236 (fabos): Nov 05 16:26:43 Switch: 0, Info HAM-REBOOT_REASON, 4, Switch reboot, reason: Unknown Error 01 -------- 0x20c (fabos): Nov 05 16:26:05 Switch: 0, Info PD_TRACE-GENERIC, 4, Watchdog Register Contains: 0xf4000000 Note: The switch error log with watchdog register value should be ignored in the case when the user initiates a power cycle of the switch rather than the switch reboots on its own. Such error log should not be interpreted as a watchdog condition. Solution: Add instrumentation code to capture the CPU snapshot to assist with fault isolation when a hardware watchdog is encountered. Note: A hardware watchdog is a feature on the central processing unit (CPU) to monitor the state of the software and/or hardware. The hardware watchdog checks in, or refreshes a certain register at a regular interval. When the hardware watchdog timer register did not

Defects Closed In Fabric OS v4.1.2b		
Defect ID	**Severity**	**Description**
		get refreshed in a given time window, the switch is reset. Service Request #: RQST00000025100
DEFECT000035778	High	Summary: Failure to de-link file descriptor and access log rotation caused compact flash full. Customer Symptom: Under the Fabric OS v4.1.x code stream there is a possibility for the compact flash to become full as a result of the Apache web server implementation. If the compact flash does become full, any process that attempts to write to the compact flash has a high probability of corrupting an open file. Compact flash full can cause a fail over. If a fail over does occur, the same risk is present in the new active CP in the SilkWorm 12000 (M12), which may cause the switch to go down. Solution: Disable Web Tools access logging. Service Request #: RQST00000025348

Defects Closed in Fabric OS v4.1.2a

Defects Closed In Fabric OS v4.1.2a		
Defect ID	**Severity**	**Description**
DEFECT000034465	Critical	Summary: Cannot disable trunking without trunking license Solution: The fix is to allow user to disable trunking without Trunking License, but user can not enable trunking without trunking license.
DEFECT000035138	Critical	Summary: Device lost Peer-to-Peer connectivity across fabric if the device does NS registration 1 second later after FLOGI. Solution: Send Name Server correct updated device bitmap such that Name Server can generate RSCN if device has updated registrations.
DEFECT000035137	Medium	Summary: Debug Messages left enabled on Fabric OS v4.1.x Solution: Disabled all debugging messages.
DEFECT000035021	Low	Summary: When switch has not been configured with FRU header, will see " Warning MSFICON-SWITCH_NID, 3, Chassis FRU header unusable for switch NID, using defaults". Solution: Change log level to 'info' from 'warning' if default switch NID values are used
DEFECT000035029	Low	Summary: Add 'ficonshow' command output to the supportShow Solution: Add 'ficonshow' command output to the supportShow