



Brocade Fabric OS v4.1.2e

Release Notes_v1.0

February 20, 2004

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v4.1.2e Release Notes_v1.0	First release	February 20, 2004

Copyright © 2004, Brocade Communications Systems, Incorporated.

ALL RIGHTS RESERVED.

BROCADE, the Brocade B weave logo, Brocade: the Intelligent Platform for Networking Storage, SilkWorm, and SilkWorm Express, are trademarks or registered trademarks of Brocade Communications Systems, Inc. or its subsidiaries in the United States and/or in other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

FICON® is a registered trademark of IBM Corporation in the US and other countries.

Notice: The information in this document is provided “AS IS,” without warranty of any kind, including, without limitation, any implied warranty of merchantability, noninfringement or fitness for a particular purpose. Disclosure of information in this material in no way grants a recipient any rights under Brocade's patents, copyrights, trade secrets or other intellectual property rights. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

Notice: The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find-out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

Export of technical data contained in this document may require an export license from the United States Government.

TABLE OF CONTENTS

Document History.....	1
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 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	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 SilkWorm 3900 Hot Code Activation.....	12
Microsoft Internet Explorer Issue	12
Interpreting Ambient and Internal Temperatures.....	12
Other Important Notes	13
Defects Closed in Fabric OS v4.1.2e.....	16
Defects Closed in Fabric OS v4.1.2d.....	17
Defects Closed in Fabric OS v4.1.2c	19
Defects Closed in Fabric OS v4.1.2b.....	20
Defects Closed in Fabric OS v4.1.2a.....	21

Overview

Fabric OS v4.1.2e 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 v4.1.2e is functionally identical to Fabric OS v4.1.2.

Fabric OS v4.1.2e is an upgrade and replacement for Fabric OS v4.0.2x, v4.1.0x, and v4.1.1x. Fabric OS v4.1.2 has completed IBM FICON¹ 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), is not 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 v3.0.1 (the Fabric Access API)
 - Fabric Manager v4.1.0 and later

About This Release

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

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

The serial number label is located as follows:

- *SilkWorm 2000 series (2109-S08/S16 and 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 bottom of chassis
- *SilkWorm 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 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 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 Manual*
- *Brocade Diagnostic and System Error Messages Reference Manual*

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 Message Manual*, 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 53-0000515-06)

The message text and severity level for the MSFICON-SWITCH_NID error message was updated for Fabric OS v4.1.2a. 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.”

Additionally 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 that the 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
D_ID	Destination ID (3 bytes)	Argument 1, next 3 bytes
S_ID	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 7effffffd,00502b00,00000000,00000000,00006103
13:15:57.159   msd    ficonq 43      005c7 7affffffa,00502b00,00000000,00000000,00060442
13:15:57.223   msd    ficonq 43      005d0 78ffffffd,00502b00,00100000,00000000,00063014
13:15:57.236   msd    ficonq 43      005cb 7affffffa,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)
D_ID	fffffd
S_ID	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

In Fabric OS v4.1.0 and v4.1.1 Release Notes, the “SilkWorm 2xxx Scalability Limits” 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 maximum number of devices supported in fabrics that include SilkWorm 2000-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

The documentation update for the v4.1.0 Release Notes also applies to the v4.1.1 notes.

Additionally, 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-Sxx 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 SW F32s 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 *Brocade Fabric OS Procedures Guide*.

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

Important Notes

This section includes the following topics:

- Security
- Cascaded Environment
- Maximizing Fabric Availability During SilkWorm 3900 (2109-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 SilkWorm 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 SilkWorm 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 *Brocade Fabric OS Procedures Guide*, v4.1.0, publication number 53-0000518-02.

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 a tree node causes the right panels to refresh to the currently selected switch. However, under NT 4.0 running IE 5.0/5.5, the right panel does *not* update for the second and subsequent instance of the Switch Explorer.

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&>.

There are two workarounds:

1. Always use a single instance of Switch Explorer on NT 4.0 running IE 5.0/5.5.
2. Install IE 6.0 SP1.

Alternatively, you might obtain a workaround for this problem directly from Microsoft. Contact Microsoft support and supply them the information in the defect as described in the previous URL.

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 optionally 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 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	When a SilkWorm 12000 (2109-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, because the association between the IP addresses and MAC addresses has changed.
Fabric Device Management Interface (FDMI)	An HBA will be allowed to register even though the originating port is not on the HBA's registered port list. This is intended behavior, included to test error cases.
Fabric OS CLI commands, failover, and port disable	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, wait for one command to finish before issuing another command.
Fabric OS switch beaconing	Problem: 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 (2109-M12) if there are faulty port blades. Verify that 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	Problem: Issuing a configdefault command followed by reboot or switch disable or enable can cause the fabric to segment due to possible domain overlap. Solution: Before rebooting the fabric, ensure that all switches are properly configured, to avoid domain overlap between the logical switches.
Firmware download	Review the "Firmware Download" section of the <i>Brocade Fabric OS Procedures Guide</i> before upgrading your firmware.
Firmware download	During a firmware download, rebooting or power cycling the CPs could corrupt the compact flash. 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	When a switch reboot or a failover occurs before POST is complete, the HA resynchronization is disrupted. HA will not resynchronize until POST completes. Allow POST to complete before performing a switch reboot or failover, to avoid disruptive failover.
IP addresses	Do not set a switch or CP IP address for the Ethernet interface to 0.0.0.0.
IP addresses	Supernetting IP addresses, also known as CIDR, is not supported in Fabric OS.
License removal	When a user removes a license from the switch, the feature is not disabled until the switch is rebooted or a switch disable or enable is performed.
LTO 2 tape drive support	When using the LTO 2 tape drive, the user must enter the following command on both Fabric OS 3.x and 4.x: switch> portcfggport port# where drive is plugged in This allows the tape drive to function in point-to-point mode rather than in loop mode.
OS hardware	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, bring up the port blade again after the failover on the SilkWorm 12000 (2109-M12).
Security	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	Adding switches to the FCC list does not automatically join the switches to 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	Before using the PKICERT utility to prepare a 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, and any CSRs that do not conform to this requirement will be rejected.
Security, SLAP fail counter and 2 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 (2109-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 changes after a HA failover.
Security: empty policies	If telnet, API, and serial port access policies are empty, the user will not be able to communicate with the switch. Contact your switch provider for the recovery procedure.
Security: error counter	The telnet security error counter will count each violation as 1 plus any autoretries the telnet software executes.
Security: secure mode	When in secure mode, if you upgrade from Fabric OS version 4.0 to 4.1, downgrade to Fabric OS version 4.0, and then upgrade back to Fabric OS version 4.1, the system prompt will ask you to reset the secure mode password.

Area	Description
Security: secure mode, passwd telnet	<p>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.</p> <p>This is expected behavior. The session will terminate if you change the password in secure mode.</p>
Advanced Web Tools and CLI commands	<p>If you use Advanced Web Tools to change the switch name, the SilkWorm 12000 (2109-M12) telnet console prompt will not update to the new name until a new telnet window is opened.</p>
Advanced Web Tools, Java bug	<p>Problem: If a dialog box is displayed from the switch admin window of Advanced Web Tools and the user selects another dialog box from Advanced Web Tools, a window display error occurs.</p> <p>Solution: 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.</p>
WWN card FRU repair	<p>If an HA failover or power cycle occurs during replacement of a FRU on the WWN card, the SilkWorm 12000 (2109-M12) becomes nonoperational.</p> <p>When performing replacement of a FRU replacement on a WWN card, complete the FRU procedure before attempting an HA failover or power cycling the chassis.</p>
Zoning	<p>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), make sure 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, 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 a Zoning license was missing.</p>
Zoning	<p>Problem: Domain 0 in a zoning configuration file is invalid but was not previously enforced.</p> <p>Solution: Prior to upgrading a switch to Fabric OS v4.1, ensure that the fabric’s zoning configuration does not contain domain ID 0, which is used for zoning. This is specific only to 4.x switches.</p>
FICON	<p>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. To avoid this situation, the ports on the SilkWorm 12000 (2109-M12) connected to the 1-GB channels should be configured for fixed 1-GB speed.</p>

Area	Description
FICON	<p>In FICON environments, dynamic load sharing (DLS) should be configured to “disabled” on the SilkWorm 12000 (2109-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.</p> <p>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 is 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.</p>
FICON	If the Manufacturer field in the switch node descriptor of the FRU header is programmed to "BRD", which is the default value, an informational message is displayed on the console, indicating that the switch NID is not programmed. This is only informational and does not impact the functionality of the switch.

Defects Closed in Fabric OS v4.1.2e

Defects Closed In Fabric OS v4.1.2e		
Defect ID	Severity	Description
DEFECT000037533	Critical	<p>Summary: Out Of Memory (OOM) panic on SW3900 (2109-F32)</p> <p>Symptom: Switch is rebooting almost every week, leaving behind the following signature in corefile Out of Memory: Killed process 4938 (xxxd). VM size = 6032 KB, Runtime = 1759 minutes, CPU time = 0 sec. kSWD:Detected unexpected termination of: "[14]secd:0'RfP=635,RgP=635,DfP=0,died=1,rt=14797098,dt=47777 to=50000,aJc 14745598,aJp=14728997,abiJc=-49185600,abiJp=-49202200,aSeq=889,kSeq=0,kJc=0,kJp=0,J=14749321,rs=2'^M</p> <p>Solution: Switch driver does not pass the free token IOCTL to the port driver to free the IU when did_port is MAX_PORT. Zoning will now pass did_port 0 instead of MAX_PORT, so port driver can free the IU in error path.</p>
DEFECT000034830	High	<p>Summary: Switch reboot with CF Error: hda: status timeout</p> <p>Symptom: Observed switch reboot with following message logged on switch console: hda: status timeout: status=0xd0 { Busy } hda: no DRQ after issuing WRITE ide0: reset timed-out, status=0x80 hda: status timeout: status=0x80 { Busy } hda: drive not ready for command ide0: reset timed-out, status=0x80] end_request: I/O error, dev 03:01 (hda), sector 75792 end_request: I/O error, dev 03:01 (hda), sector 75800 end_request: I/O error, dev 03:01 (hda), sector 71632</p>

Defects Closed In Fabric OS v4.1.2e		
Defect ID	Severity	Description
		<p>end_request: I/O error, dev 03:01 (hda), sector 71640 XFS: device 0x301- XFS write error in file system meta-data block 0x117d0 in ide0(3,1) end_request: I/O error, dev 03:01 (hda), sector 74128 end_request: I/O error, dev 03:01 (hda), sector 74136 end_request: I/O error, dev 03:01 (hda), sector 109020 I/O error in filesystem ("ide0(3,1)") meta-data dev 0x301 block 0x1a9dc ("xlog_iodone") error 5 buf count 3584 xfs_force_shutdown(ide0(3,1),0x2) called from line.... Watchdog Exception: current process c2c04000, r1=c2c059f0</p> <p>Solution: Once the write time-out occurs, instead of recover by issue two soft resets, the new recovery method is to wait for 1 second after software reset, then trigger IDE reset. This fix only applies to SW3900 (2109-F32) platform.</p> <p>SR #: RQST00000025100</p>
DEFECT000035936	High	<p>Summary: HBAs do not appear in zoning applet (Emulex Solaris driver 5.02b)</p> <p>Symptom: In webtool GUI, nodes attached to some ports are displayed and nodes attached to some ports are not displayed.</p> <p>Solution: Increase the size of the array used to store the symbolic names. Use the same constant as the NS.</p> <p>SR #: RQST00000025694</p>

Defects Closed in Fabric OS v4.1.2d

Defects Closed In Fabric OS v4.1.2d		
Defect ID	Severity	Description
DEFECT000037192	High	<p>Summary: SilkWorm 12000 (2109-M12) reboot when doing firmware download in an unstable fabric with a lots of device rscn.</p> <p>Customer Symptom: The SilkWorm 12000 (2109-M12) experiences a failover and reboots with Error RTWR-FAILED message in the panic dump trace and console log. An emd core dump is also generated by abort signal SIGABRT.</p> <p>Solution: During firmware download, port-detected RSCN delivery was timed out. After the failover, the Name Server tried to deliver all the timed out RSCNs, which took a lot of time and caused emd failing to refresh SWD. The fix is to increase RTWR timeout value so that the delivery would not timed out easily. Also only resend one RSCN in this case by removing duplicate pending RSCNs.</p> <p>Workaround: Perform firmware download in a stable fabric.</p>

Defects Closed In Fabric OS v4.1.2d		
Defect ID	Severity	Description
		SR #: RQST00000026703
DEFECT000036357	High	<p>Summary: SilkWorm 12000 (2109-M12) reboots with reason unknown caused by failover in the middle of processing Plogin frame</p> <p>Customer Symptom: Reboot of SilkWorm 12000 (2109-M12) after failover.</p> <p>Solution: Login flag is for local use only with login payload. The flag is synced up to standby CP but not the login payload. Panic occurs if login payload is accessed based on the flag after hafailover. The fix is to remove login flag from sync table and replace it with a reserved field.</p> <p>SR #: RQST00000026113</p>
DEFECT000035091	High	<p>Summary: zone stuck at commit operation, finally get ERROR RTWR-FAILED, 2, RTWR rtwrSend 2, fffce4, e4, 65, 0</p> <p>Customer Symptom: After removing and adding a member to quick loop as shown in the following steps, enable cfg process gets stuck.</p> <ol style="list-style-type: none"> 1. Remove a switch's WWN out of a dual quick loop 2. Add another switch's WWN to this dual quick loop 3. Enable the cfg <p>The control never get back until the RTWR error shows up.</p> <p>Solution: RCS could not check the return code of its IPC call fast enough. The subsequent IPC call overwrote the return code. RCS now uses a socket interface instead of IPC mechanism.</p>
DEFECT000036320	Medium	<p>Summary: If a watchdog interrupt is received during a printk (print to console), the back trace is not propagated into the panic dump logs</p> <p>Customer Symptom: In some cases, when hardware watchdog happens, panic dump logs do not contain back trace information</p> <p>Solution: Do not allow watchdog interrupt during an existing printk. Also put in a time delay for the last write before reboot to avoid potential CF corruption during reboot.</p>
DEFECT000037653	High	<p>Summary: CF sector write timeout on SilkWorm 12000 (2109-M12) and SilkWorm 3900 (2109-F32).</p> <p>Customer Symptom: Observed "hda: status timeout: status=0xd0 { Busy }" on console log and file system shutdown afterwards.</p> <p>Solution: Increased compact flash write timeout value to accommodate worst case CF internal re-mapping.</p> <p>SR #: RQST00000026990</p>

Defects Closed in Fabric OS v4.1.2c

Defects Closed In Fabric OS v4.1.2c		
Defect ID	Severity	Description
DEFECT000034966	High	<p>Summary: Standby CP may panic upon becoming active after a fail-over on a SW12000 (2109-M12) if SNMP query is in progress.</p> <p>Solution: Use mutex to prevent potential deadlock issue.</p>
DEFECT000036058	High	<p>Summary: Long I/O wait problem under FICON environment.</p> <p>Solution: Reject undeliverable frames.</p> <p>Service Request# RQST00000025865</p>
DEFECT000036520	High	<p>Summary: PCI DRAWBRIDGE: Failed secondary side test.</p> <p>Solution: NOTE: This problem will surface when downgrading to versions before 4.1.2c as the defect exists in those earlier versions.</p> <p>Following a fail-over, the standby CP performs a test of the drawbridges to ensure that they are operating correctly. The test involves issuing a "dummy" configuration read to non-existent device on the drawbridge's secondary bus. If the drawbridge is operating properly, the read should return all 1's or 0's. However, if the drawbridge is faulty, the read will hang and the PCI dead-man timer will expire causing an interrupt. The test currently is not targeting a non-existent device but the first blade slot instead. Therefore there is the potential for a conflict with the active CP when this test is run. Modified the configuration read to target a non-existent device (31). Also removed the check of the configuration read return code since as long as the read returns, this means the drawbridge is ok.</p> <p>Service Request# RQST00000026226</p>
DEFECT000036680	High	<p>Summary: FICON I/O delay when a port blade connected to the storage is pulled.</p> <p>Solution: The frames were being marked as timed out rather than undeliverable. Change status from the default IU_TIMED_OUT to IU_TX_UNAVAIL in order to send an F_RJT instead of F_BSY.</p> <p>Service Request# RQST00000026345</p>
DEFECT000036596	Medium	<p>Summary: SNMP community and trap recipient configuration are not retained after a switch reboot.</p> <p>Solution: Set the swEventTrapLevel value without writing to the FLASH.</p> <p>Service Request# RQST00000024677</p>

Defects Closed in Fabric OS v4.1.2b

Defects Closed In Fabric OS v4.1.2b		
Defect ID	Severity	Description
DEFECT000035187	High	<p>Summary: Add code to assist Hardware Watchdog debug.</p> <p>Customer Symptom: The symptom seen for the watchdog is an unscheduled automatic reboot on a SilkWorm 3900 (2109-F32) accompanied with the following error messages in the switch error log.</p> <p>Error 02 ----- 0x236 (fabos): Nov 05 16:26:43 Switch: 0, Info HAM-REBOOT_REASON, 4, Switch reboot, reason: Unknown</p> <p>Error 01 ----- 0x20c (fabos): Nov 05 16:26:05 Switch: 0, Info PD_TRACE-GENERIC, 4, Watchdog Register Contains: 0xf4000000</p> <p>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.</p> <p>Solution: Add instrumentation code to capture the CPU snapshot to assist with fault isolation when a hardware watchdog is encountered.</p> <p>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 get refreshed in a given time window, the switch is reset.</p> <p>Service Request #: RQST00000025100</p>

Defects Closed In Fabric OS v4.1.2b		
Defect ID	Severity	Description
DEFECT000035778	High	<p>Summary: Failure to de-link file descriptor and access log rotation caused compact flash full.</p> <p>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 (2109-M12), which may cause the switch to go down.</p> <p>Solution: Disable Web Tools access logging.</p> <p>Service Request #: RQST00000025348</p>

Defects Closed in Fabric OS v4.1.2a

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