



Brocade Fabric OS v4.1.1e

Release Notes_v1.0

March 9, 2004

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v4.1.1e Release Notes_v1.0	First release	March 9, 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	5
Documentation Updates.....	6
Brocade Fabric OS Procedures Guide v4.1.0	6
Requirements and Compatibility	6
Important Notes	7
Security	7
Maximizing Fabric Availability During SW 3900 Hot Code Activation	7
Microsoft Internet Explorer Issue	7
Interpreting Ambient and Internal Temperatures.....	7
Other Important Notes	8
Defects Closed in Fabric OS v4.1.1e	11
Defects Closed in Fabric OS v4.1.1d.....	13
Defects Closed in Fabric OS v4.1.1c	14
Defects Closed in Fabric OS v4.1.1b.....	15
Defects Closed in Fabric OS v4.1.1a.....	16

Overview

Brocade Fabric OS v4.1.1e is a patch release that contains fixes to a small number of additional issues detected. 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, v4.1.1e is functionally identical to the last patch release, Fabric OS v4.1.1d. These Release Notes will refer to “Fabric OS 4.1” when making statements that apply to Fabric OS 4.1.0 and 4.1.1x.

About This Release

Fabric OS v4.1 represents the first major feature revision to the Fabric OS v4.0 firmware. It should be considered an upgrade and replacement for Fabric OS v4.0, which shipped initially with the launch of the Brocade SilkWorm 12000 (2109-M12) director in the first half of 2002 and then later with Fabric OS v4.0.2, which shipped initially in the second half of 2002, supporting the SilkWorm 3900 (2109-F32) switch and SilkWorm 12000 (2109-M12) director.

Fabric OS v4.1.1e includes the following changes:

- Fixes to defects, as detailed in the section “Defects Closed in Fabric OS v4.1.1e.”
- Starting in November 2003, Brocade is adding versioning to all Release Notes. This is a documentation format change and does not affect the actual code.

Supported Switches

This release supports the Brocade SilkWorm 3900 (2109-F32) switch and the SilkWorm 12000 (2109-M12) director.

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

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 (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 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 Manual*
- *Brocade Diagnostic and System Error Messages Reference Manual*

Standards Compliance

Brocade Fabric OS v4.1 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 Fabric OS Procedures Guide v4.1.0

(Publication number 53-0000518-02)

The following information should be added to Step 7 of the procedure “Upgrading the Firmware on the SilkWorm 12000,” in Chapter 4.

“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*.

For the User prompt, enter a user ID that has an account on the FTP server.”

Requirements and Compatibility

Brocade Fabric OS v4.1.0 and v4.1.1 can be installed and run on the SilkWorm 3900 (2109-F32) and SilkWorm 12000 (2109-M12).

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 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

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) or 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
- Maximizing Fabric Availability During SW 3900 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.)

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 SilkWorm 3900 (F32 directly connected via an ISL) are running Fabric OS v2.6.1 or later, v3.1.0 or later, or v4.1.0 or later. More information is available in the “Firmware Download” section of the *Brocade Fabric OS Procedures Guide*.

Microsoft Internet Explorer Issue

There is an issue 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 and IE 5.0/5.5, the right panel does *not* update the second and subsequent instances of Switch Explorer.

Microsoft addresses the issue at: <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 and IE 5.0/5.5.
2. Install IE 6.0 SP1.

Alternatively, you could obtain a workaround 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 Brocade Fabric Watch optionally licensed firmware product.

Sensor	Minimum	Maximum	Comments
SilkWorm 12000 (2109-M12)			
Blowers	0° C	40° C	Sensor on each blower measures inlet (ambient) air temperature.
Port blades	0° C	74° C	Each port blade has its own temperature sensor. Warning at 75° C.; blade shutdown at 80° C.
CP blades	0° C	74° C	Each CP blade has its own temperature sensor.

			Warning at 75° C.; CP faulted at 80° C.
SilkWorm 3900 (2109-F32)			
Switch	0° C	69° C	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 (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 in 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 disable ports. Reissue the command after the failover is complete to bring ports back online.
Fabric OS commands	<p>Issue: Under the root account, issuing Fabric OS commands in parallel through scripts could cause the kernel task to consume excessive memory.</p> <p>Solution: When using scripts to issue Fabric OS commands, it is always a good practice to wait for one command to finish before issuing another command.</p>
Fabric OS switch beaconing	<p>Issue: Switch beaconing is not preserved across a failover. If you start beaconing, a failover will cause all lights to stop flashing.</p> <p>Solution: If this occurs, reissue the command to resume switch beaconing.</p>
Fabric OS, switch reboot, and blade repair	<p>Issue: Switch reboot will fail in the SilkWorm 12000 (M12) if there are faulty port blades.</p> <p>CAUTION: 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 perform a switch reboot and find a faulty blade, remove the blade and reboot will continue.</p> <p>Solution: To reboot successfully identify and remove the faulty blade using the slotshow command. .</p>
Fabric routing, Fabric Manager: domain overlap	<p>Issue: Issuing a configdefault command followed by reboot or switch disable or enable will cause the fabric to segment due to possible domain overlap.</p> <p>Solution: Before rebooting the fabric, ensure that all switches are properly configured to avoid domain overlap between the logical switches.</p>
Firmware download	Review the "Firmware Download" section of the <i>Brocade Fabric OS Procedures Guide</i> before upgrading your firmware.

Area	Description
Firmware download	<p>Issue: During a firmware download, rebooting or power cycling the CPs could corrupt the compact flash.</p> <p>CAUTION: Do not attempt to power off the CP board during firmware download, to avoid high risk of corrupting your flash.</p>
HA switch reboot failure	<p>When a switch reboot or a failover occurs before POST is complete, the HA resynchronization is disrupted. HA will not resynchronize until POST completes.</p> <p>CAUTION: Allow POST to complete before performing a switch reboot or failover, to avoid disruptive failover.</p>
IP addresses	CAUTION: 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 a switch, the licensed feature is not disabled until the switch is rebooted or a switch disable or enable is performed.
LTO 2 tape drive support	<p>When using the LTO 2 tape drive, the user must issue the following command for both Fabric OS v3.x and v4.x:</p> <p style="text-align: center;">switch> portcfggport port# where drive is plugged into</p> <p>This allows the tape drive to function in point-to-point mode rather than loop mode.</p>
OS, hardware	Bringing up port blades during a failover could cause the port cards to come up disabled. This is a rare occurrence; when this happens, bring the port blade back up after the failover on the SilkWorm 12000 (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, empty policies	<p>CAUTION: If telnet, API, and serial port access policies are empty, the user will not be able to communicate with the switch.</p> <p>Solution: Contact your switch provider for the recovery procedure.</p>
Security, error counter	The telnet security error counter will count each violation as 1 and will add 1 for each autoretry that the telnet software executes.
Security, FCC list	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 to join the switches.
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.
Security, secure mode, passwd telnet	<p>CAUTION: Using the "passwd" telnet command in secure mode to change the password results in all sessions using that password being logged out, including the session that changed the password.</p> <p>This is expected behavior. The session will terminate if you change the password in secure mode.</p>
Security, 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.

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.
Security, SSH login	To properly connect SSH login, wait for secure mode to complete before rebooting or performing 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 changes after an HA failover.
Web Tools and CLI commands	If you use Brocade Advanced 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	<p>Issue: 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.</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>Issue: If an HA failover or power cycle occurs during a FRU replacement on the WWN card, the SilkWorm 12000 (M12) will become nonoperational.</p> <p>CAUTION: When performing a FRU replacement on a WWN card, complete the FRU procedure before attempting an HA failover or power cycling the chassis.</p>
Zoning, non-RCS fabric	<p>To use zoning in a non-RCS (Reliable Commit Service) mode fabric (that is, in a fabric containing switches with firmware versions 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, you must make sure it is reinstalled properly on the affected switch before attempting the cfgenable zoning operation.</p> <p>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 (or can also be seen by issuing errShow, errDump), indicating that the zoning license is missing.</p>
Zoning, domain ID 0	<p>Issue: Domain 0 in a zoning configuration file is invalid but has not been enforced.</p> <p>Solution: Prior to upgrading a switch to v4.1, ensure that the fabric's zoning configuration does not contain the domain ID 0 for zoning. This is specific only to v4.0.x switches.</p>

Defects Closed in Fabric OS v4.1.1e

Defects Closed In Fabric OS v4.1.1e		
Defect ID	Severity	Description
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 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 SilkWorm 3900 (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 Web Tools 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 v4.1.1e		
Defect ID	Severity	Description
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>
DEFECT000036786	Medium	<p>Summary: After "fastboot" was issued on the SilkWorm 12000 (M12), with following error messages are displayed: Switch: 0, Error EM-INIT_FAIL, 2, EM Init Error: hillInitLED failed, err=-28, 0x35d (fabos): set_i2c_mux_local(): Failed to get exclusive access</p> <p>Solution: Active CP resets itself when it wants to be reset, rather than depending upon other CP.</p>
DEFECT000037192	High	<p>Summary: SilkWorm 12000 (M12) reboot when doing firmware download in an unstable fabric with a lots of device rscn.</p> <p>Customer Symptom: The SilkWorm 12000 (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> <p>SR #: RQST00000026703</p>
DEFECT000037533	Critical	<p>Summary: Out Of Memory (OOM) panic on SW3900 (F32)</p> <p>Symptom: The SilkWorm 3900 (F32) reboots 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>

Defects Closed In Fabric OS v4.1.1e		
Defect ID	Severity	Description
DEFECT000037653	High	<p>Summary: CF sector write timeout on SilkWorm 12000 (M12) and SilkWorm 3900 (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 v4.1.1d

Defects Closed In Fabric OS v4.1.1d		
Defect ID	Severity	Description
DEFECT000034465	Critical	<p>Summary: Cannot disable trunking without trunking license.</p> <p>Solution: Allow user to disable trunking without trunking license, but user cannot enable trunking without trunking license.</p> <p>Service Request# RQST00000024874</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>Symptom: After removing and adding a member to quickloop, enable cfg process gets stuck.</p> <p>Solution: RCS was not able to 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> <p>Service Request# None</p>
DEFECT000036357	High	<p>Summary: SilkWorm 12000 (M12) reboots with reason unknown caused by fail over in the middle of processing Plogin.</p> <p>Symptom: Reboot of SilkWorm 12000 (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>Service Request# RQST00000026113</p>
DEFECT000034767	Medium	<p>Summary: Debug messages left enabled on Fabric OS v4.1.x</p> <p>Symptom: Within the portlogdump, the event "debug" was left enabled.</p>

Defects Closed In Fabric OS v4.1.1d		
Defect ID	Severity	Description
		<p>Also, the application level debug modules have been left enabled.</p> <p>Solution: Disable all debugging message.</p> <p>Service Request# None</p>

Defects Closed in Fabric OS v4.1.1c

Defects Closed In Fabric OS v4.1.1c		
Defect ID	Severity	Description
DEFECT000034298	High	<p>Summary: ADISC/PLOGI is dropped by switch under certain zone configurations, which cause zoned ports to not talk to each other.</p> <p>Solution: Fix code to have the zoning internal hash table set up correctly after reboot</p> <p>Workaround: If port level zoning is used, the problem can be worked around by:</p> <ol style="list-style-type: none"> 1. Use an empty dummy zone before reboot 2. Enable the appropriate zone after reboot <p>Service Request# RQST00000024778</p>
DEFECT000034966	High	<p>Summary: Standby CP may panic upon becoming active after a fail-over on a SW12000 (M12) if SNMP query is in progress.</p> <p>Solution: Use mutex to prevent potential deadlock issue.</p>
DEFECT000036520	High	<p>Summary: PCI DRAWBRIDGE: Failed secondary side test.</p> <p>Solution: NOTE: This problem will surface when downgrading to versions before 4.1.1c/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</p>

Defects Closed In Fabric OS v4.1.1c		
Defect ID	Severity	Description
		(31). Also removed the check of the configuration read return code since as long as the read returns, this means the drawbridge is ok. Service Request# RQST00000026226
DEFECT000036596	Medium	Summary: SNMP community and trap recipient configuration are not retained after a switch reboot. Solution: Set the swEventTrapLevel value without writing to the FLASH. Service Request# RQST00000024677

Defects Closed in Fabric OS v4.1.1b

Defects Closed In Fabric OS v4.1.1b		
Defect ID	Severity	Description
DEFECT000035172	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. SR ID: RQST00000025348
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 -----

Defects Closed In Fabric OS v4.1.1b		
Defect ID	Severity	Description
		<p>0x20c (fabos): Nov 05 16:26:05</p> <p>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>SR ID: RQST00000025100</p>

Defects Closed in Fabric OS v4.1.1a

Defects Closed In Fabric OS v4.1.1a		
Defect ID	Severity	Description
DEFECT000026554	Critical	<p>Summary: 3800 switch port is left INSYNC after a reboot of the array</p> <p>Symptom: When a loop capable device negotiates to the F-port briefly, and NOS happens, the switch port does not complete port initialization at LIP phase. The port is left in the IN_SYNC state.</p> <p>Solution: Enable the LPSM_OPEN_INIT_RCVD interrupt when appropriate, to prevent the port from hanging during port initialization.</p>
DEFECT000026397	High	<p>Summary: Incorrect behavior in FOS 4.0.2c after ABTS is sent to the Name Server</p> <p>Symptom: When HBA accepts first RSCN, and then communicates to the name server to get new information. Another RSCN is sent, which the HBA accepts and sends ABTS to the name server for the previous query. The name server accepts but then sends the reply to the query that's not needed.</p> <p>Solution: Drop the iu if the sequence has been aborted.</p>

Defects Closed In Fabric OS v4.1.1a		
Defect ID	Severity	Description
DEFECT000026431	High	<p>Summary: The servers in the SAN failed to recover any drives when many drivers are power up at the same time.</p> <p>Symptom: In a fabric with zoning turned on, the LTO tape subsystem was powered down. After the SAN stabilized, the LTO was powered up. After 8 to 10 minutes, the servers that connected to the switch (Fabric OS v4.0.0x) with the tape subsystem successfully recovered all drives. However, the servers that connected to other switches in the SAN failed to recover any drives.</p> <p>Solution: From the traces, it shows that many PLOGIs were sent from the server after receiving the RSCNs, but only three of the PLOGI ACC were received back, other ACC to the PLOGI were dropped. The PLOGI and ACC were trapped by different filters. The solution is to update and synchronize the different filters to avoid this issue.</p>
DEFECT000026615	High	<p>Summary: CP timeout during firmware upgrade</p> <p>Symptom: During the firmware upgrade from Fabric OS 4.0.x to 4.1.1, the active control processor (CP) with 4.1.1 resets the other CP while the other CP is in the middle of upgrading firmware. This reset either corrupts the other CP's PROM or causes failure to the other CP's upgrade process.</p> <p>Solution: Use the same time window for detecting heartbeat as Fabric OS 4.0.x.</p>
DEFECT000033165	High	<p>Summary: Firmware download failed on Silkworm3900 (F32) when using Webtools to upgrade firmware from v4.0.2c to v4.1.1</p> <p>Symptom: Using Web Tools to upgrade firmware from v4.0.2c to v4.1.1 causes ASSERT panic. Web Tools cannot abort the firmware download after the switch reboots. Subsequently, the user cannot restart another firmware download.</p> <p>Solution: In single CP case, ASSERT is not needed. Removed the ASSERT.</p>