Fabric OS 4.1.1

Release Notes

June 19, 2003

TABLE OF CONTENTS

General Information

Fabric OS 4.1.0 represents the second major feature release of firmware for the SilkWorm 3900 (2109-F32) and SilkWorm 12000 (2109-M12) switches. This release adds a large number of significant new features to an already robust and comprehensive firmware platform.

Fabric OS 4.1.1 is a maintenance release that contains fixes to a small number of additional issues detected during the latter part of the OEM qualification cycle. Aside from these fixes, it is functionally identical to Fabric OS 4.1.0. These Release Notes will refer to "Fabric OS 4.1" when making statements that apply to both Fabric OS 4.1.0 and 4.1.1.

Overview

About This Release

Fabric OS 4.1 represents the first major feature revision to the Fabric OS v4.0 firmware. It should be considered an upgrade and replacement for Fabric OS 4.0.0, which shipped initially with the launch of the SilkWorm 12000 (2109-M12) in the first half of 2002, and for Fabric OS 4.0.2, which shipped initially in the second half of 2002, supporting the SilkWorm 3900 (2109-F32) and SilkWorm 12000 (2109-M12).

Fabric OS 4.1 has been developed in close coordination with Fabric OS 3.1, and great pains have been taken to keep the feature sets of the two releases as similar as possible.

Supported Switches

Like Fabric OS 4.1.0, Fabric OS 4.1.1 supports both the SilkWorm 12000 (2109-M12) and the SilkWorm 3900 (2109-F32).

Technical Support

Contact IBM 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

- 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 and corresponding bar code are provided on the serial number label, as shown below.

Type 2109-M12 **S/N PPSSSSS**	**Type 2109-F32** **S/N PPSSSSS**	**Type 2109-F16** **S/N PPSSSSS**	**Type 3534-F08** **S/N PPSSSSS**

The serial number label is located as follows:

- *SilkWorm 3200(3534-F08) and 3800(2109-F16) switches:* Front of chassis
- *SilkWorm 3900(2109-F32) switches:* Front 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 switches:* Provide the switch WWN. Use the **wwn** command to display the switch WWN.

Documentation

Supporting Documentation

Fabric OS 4.1.1 uses the same documentation as Fabric OS 4.1.0.

In addition to these release notes, this release is supported by the following documentation:

Switch documentation:

• IBM TotalStorage SAN Cabinet 2109 Model C36 with Model M12 Installation and Service Guide (GC26-7467-03).

• IBM TotalStorage SAN Switch 2109 Model M12 User's Guide (GC26-7468-02).

• IBM TotalStorage SAN Switch 2109-M12 World Wide Name Card Replacement Procedure.

• IBM TotalStorage SAN Switch 2109 Model F32 Installation and Service Guide (GC26-7496-02).

• IBM TotalStorage SAN Switch 2109 Model F32 User's Guide (GC26-7517-01).

Fabric OS v4.1 software documentation:

• Fabric OS Reference

• Fabric OS Procedures Guide

• Advanced Zoning User’s Guide

• Advanced Web Tools User’s Guide

• Advanced Performance Monitoring User’s Guide

• Distributed Fabrics User’s Guide

• Fabric Watch User’s Guide

• ISL Trunking User’s Guide

• Secure Fabric OS User’s Guide

• MIB Reference

• Diagnostic and System Error Message Reference

These documents can be fount at:

http://www.storage.ibm.com/ibmsan/products/2109/library.html

Standards Compliance

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

New Features and Enhancements

Fabric OS v4.1 will provide the following enhancements and new features relative to Fabric OS 4.0.2:

- Additional High Availability features:
    - Non-disruptive code activation on SilkWorm 12000 (2109-M12) and SilkWorm 3900 (2109-F32) switches
    - Non-disruptive failover between CPs (Control Processors) on the SilkWorm 12000 (2109-M12)
    - Additional background health monitoring of the Standby CP on the SilkWorm 12000 (2109-M12)
    - Managed hot swap procedure for the SilkWorm 12000 (2109-M12) WWN / status card
- Support for the optionally licensed Secure Fabric OS product. Secure Fabric OS includes the following features:
    - A new, centralized fabric management model, in which all fabric-wide management operations must originate from the Fabric Configuration Server, or “trusted switch”
    - Management Access Controls to secure and limit all means of switch and fabric management
    - Switch Connection Controls and Device Connection Controls, which strictly control what switches and devices may participate in the fabric.
    - Standards-based authentication (using digital certificates and PKI, or Public Key Infrastructure) of all switches in the fabric, to prevent unauthorized switches from joining the fabric.
    - A workstation-based utility, PKICERT, to acquire and install digital certificates for all switches in the fabric which do not already have them. The digital certificates are required to enable secure mode.

- Support for the Fabric Device Management Interface, allowing centralized management of some Host Bus Adapters via the fabric, including the download of new HBA firmware to the HBAs via the fabric.
- Zoning enhancements:
    - New commands for searching the Zoning data base
    - Improved performance
    - More selective SCNs – they are now sent only to devices in zones where there has been a status change among the online members of those zones.
- WebTools enhancements:
    - Replacement of the Fabric View panel with a "switch explorer" tree – an approach which allows WebTools to handle larger fabrics more efficiently
- Disabling and enabling of ports and of entire switches may now be made persistent across reboots and power cycles.
- Fabric Time Service
    - Synchronizes time among switches in the fabric
    - Fabric time may be set from a CLI session or obtained from an external NTP server
- A new fabricPrincipal command allows the administrator to give a switch preference in negotiating to become principal switch in a fabric. This can be useful in optimizing the efficiency of fabric configurations and management operations.
- Fabric Watch enhancements:
    - Improved reporting of port and switch uptime statistics
- Ports may be configured to negotiate directly to R_RDY flow control mode, simplifying operations by allowing the connection of many WAN gateway products without requiring a Remote Switch license.

Information About Secure Fabric OS

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

- *Secure Fabric OS Quick Start Guide*

More detailed product information may be obtained from the *Secure Fabric OS Users Guide*.

Documentation Addendum

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

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, another possible hardware status is offline."

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

(publication number 53-0000520-02)

Page 1-3 of the 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 5km at the full speed permitted by the link. With LWL media, the throughput begins to fall off beyond 5km, 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*."

Fabric OS Procedures Guide v4.1

(publication number 53-0000501-02)

The following information should be to Step 7, of the procedure for "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."

Fabric OS Reference Guide v4.1

(publication number 53-0000519-02)

The following note should added to the **firmwaredownload** command:

"The User ID required for the firmwaredownload process must have an account on the FTP server."

Requirements and Compatibility

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 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	4.0.2d or later	4.0.2d 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-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 the Fabric OS v2.x switches or Fabric OS 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 2109-F32 and 2109-M12. For more information regarding the Core Switch PID Format, please refer to "Updating the Core PID Format" in the *Fabric OS Procedures Guide*.

For more information about configuring 2109-S08/S16, 3534-1RU, 2109-F16, or 3534-F08 to inter-operate in the same fabric with the 2109-F32 and 2109-M12 switches, contact IBM.

Important Notes

SilkWorm 2xxx Scalability Limits

Exhaustive testing has demonstrated that SilkWorm 2000 family switches (S08/S16/1RU) should not be deployed in fabrics whose size exceeds 500 user ports (device ports). Such switches will not be supported in fabrics that exceed this size, regardless of Fabric OS version.

Maximizing Fabric Availability during 2109-F32 Hot Code Activation

During code activation on 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 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 manual.

Microsoft Internet Explorer Issue

An issue has been identified with Microsoft Internet Explorer 5.0 and 5.5 running on Windows NT 4.0. The problem is as follows. Normally, when you launch a copy of the Switch Explorer applet, the left hand panel displays a tree of switches in your fabric. Clicking on a tree node will cause the right hand panels to refresh to the currently selected switch. However, under NT/4.0 and IE 5.0/5.5, the right hand panel will NOT update for the 2nd 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 2 workarounds for this:
1. Always use a single instance of the SwitchExplorer on NT/4.0 and IE 5.0/5.5
2. Install IE 6.0 SP1

Alternatively, it is possible that you can 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

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 may be reported via Fabric OS v4 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 v4.1.1.

Area	Description
Ethernet Port IP addresses	**NOTE:** 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 may 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 Commands	The commands moredisable and moreenable were added to the Fabric OS.

Area	Description
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 (2109-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** followed by reboot or switch disable/enable will cause the fabric to segment due to possible domain overlap. **Solution:** Therefore, 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 potentially corrupting your flash.**
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.

Area	Description
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, and when this happens, redo the port blade bringup after the failover on the SilkWorm 12000 (2109-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 onto 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 switchnames of any switches in the fabric. The Web site that processes the CSRs and generates the digital certificates does not accept switchnames 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 sec mode to complete before rebooting or doing HA failover on the SilkWorm 12000 (2109-M12). If Sec mode is enabled and a reboot occurs before Sec 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.
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 to be 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 switchName, the SilkWorm 12000 (2109-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 the Web Tools and the user selects another dialog box from Web Tools, this causes a windows 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.

Area	Description
WWN card FRU repair	**Problem:** If an HA failover or power cycle occurs during a FRU on the WWN card, the 2109-M12 will become non-operational. **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 re-installed back properly on the affected switch before attempting **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.

Defects Closed Since Fabric OS 4.1.0

This table lists the defects that have been closed since the last GA release.

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000024217	High	**Summary:** Switch not sending enough LIPs to transition from AL-PA sequence to Old_Port **Solution:** Defect was closed by documentation of work-around
DEFECT000024312	High	**Summary:** 'RTC_RD_TIME: Invalid Argument' error message on Standby CP during firmwareDownload procedure **Symptom:** The Standby CP reported an invalid argument error during a firmwareDownload.
DEFECT000024854	High	**Summary:** Executing switchdisable/enable and saw ASSERT – Failed expression: NULL. **Symptom:** After running stress tests for several days on a large fabric, as the next set of stress tests were being prepared, an ASSERT was seen indicating that a kernel operation failed when the switch was enabled.
DEFECT000025162	High	**Summary:** 3900 (2109-F32) Panic on v4.1 Beta 2 after upgrade from v4.0.2c **Symptom:** When upgrading from v4.0.2c to v4.1_beta2, a panic was observed on a SW3900 (2109-F32). **Solution:** Defect closed as non-reproducible with customer consent.
DEFECT000025531	High	**Summary:** Running a stress test script over night caused software watchdog to reboot the Standby CP on a core switch. KSWD, uSWD critical errors, also secd and panic core files were created. **Symptom:** Running a stress test script where switches in the secure fabric continuously run: switchdisable/enable, switch speed set to 1G/2G/AN, disable/enable trunking, secfcsfailover, create/activate and remove/activate a security policy commands, with core-edge type topology, could cause a standby CP to reboot.

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000025606	High	**Summary:** psd dies when switchdisable/switchenable script running in very large fabric **Symptom:** With 2+4+28 mixed configuration, which has 6 12000s (M12), 6 3800s (F16), 22 3900s (F32), ~700 device ports, 95 Kbytes zone size, and traffic. **Action:** running a switchdisable/switchenable script on all 4.1 edge switches (include 4 12000s (M12) and 22 3900s (F32)) at the same time. The script is: 1. send command "switchdisable" to all 26 switches at the same time. 2. sleep 60s 3. send command "switchenable" to all 26 switches at the same time. 4. sleep 600s. 5. repeat step 1, 2, 3, 4 again. **Results:** psd dies on two 3900s (F32) with message "Switch: 0, Critical kSWD-kSWD_GENERIC_ERR_CRITICAL, 1, kSWD: '[12]psd:0'...".
DEFECT000025669	High	**Summary:** Booting over SAN issues on Brocade 12000 (M12), v4.1.0_rc2 firmware. **Symptom:** Boot over SAN fails
DEFECT000025703	High	**Summary:** After about 9.5 hours of stress test, core switches panicked with "Application zoned from switch Instance 0 failed to refresh" message. **Symptom:** Core switches can panic after a long stress operation that causes the fabric to become unstable.
DEFECT000025717	High	**Summary:** Need updates applied to FA-MIB as outlined below. **Symptom:** A new trap should be sent from switch when CP/Blade/WWN cards get failure. **Solution:** Monitor CP failure, WWN failure and Blade failure to update switch state. Add policy for these 3 monitors. This has been requested by RFE 2745 Need to send an connUnitStatusChange trap when any of these monitored objects matches the policy.

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000025781	High	**Summary:** Message "Critical SYSC-ERROR, 1, sysc_main.c:214", and emd dies when script switchdisable/enable running. **Symptom:** With 2+4+28 mixed configuration, which has 6 12000s (M12), 6 3800s (F16), 22 3900s (F32), ~700 device ports, 95 Kbytes zone size, and traffic. **Action:** running a switchdisable/switchenable script on all 4.1 edge switches (include 4 12000s (M12) and 22 3900s (F32)) at the same time **Results** in a SW Watchdog error being detected. **Solution:** This defect was caused by an invalid configuration installed on the test station. This invalid configuration was caused by a corrupted set of data structures generated by an internal FICON code build that was on the switch prior to the upgrade. This defect cannot be recreated when upgrading or downgrading between official versions of 4.1.0 and 4.1.1 code releases.
DEFECT000025792	High	**Summary:** The Cp should not allow the active cp to failover to a missing or non- redundant cp blade.
DEFECT000025827	High	**Summary:** get fcpd core dump after running the script overnight: doing login to the switch, switchenable, logout **Symptom:** Running an overnight script that issues switchenable to the same switch over and over, a panic and core dump was observed. Overnight scripts that issue switchenable, switchdisable, switchenable, over and over are able to run for the entire night.
DEFECT000025887	High	**Summary:** kSWDs being encountered along with full CF error condition **Symptom:** Over a long period of time running with an application that attempts to login with the switch but fails due to invalid passwords, the switch will encounter a kSWD panic and reboot. Some switches have also exhibited a full CF along with the kSWD error.
DEFECT000025891	High	**Summary:** Switch Panic, KSWD Error for MSD Failure Caused Reboot and Core Dump. **Symptom:** CP was marked faulty, due to KSWD error when MS Daemon failed causing the CP to fail over and reboot
DEFECT000025893	High	**Summary:** Switch Panic, KSWD Fabric Watch Daemon Caused A Reboot Of Switch and Core Dump. **Symptom:** CP was marked faulty, due to KSWD error when Fabric Watch Daemon failed, CP was failed over and rebooted.

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000025894	High	**Summary:** CF (Compact Flash Memory) Full 100% Capacity; Writes Failures Seen. Symptom: Writes to compact flash will fail.
DEFECT000025906	High	**Summary:** Using API Lib 3.0.0a_0530, with firmware v4.1.1_rc2_bld02, API performance is severely degraded.
DEFECT000021225	Medium	**Summary:** After failover SECd died and caused new active CP to reboot **Symptom:** While performing fail-over testing, the security module failed and caused the system to reboot.
DEFECT000023384	Medium	**Summary:** Running a switchcfgtrunk script on 2+6 SW 12000 fabric caused msd core dump **Symptom:** Running a stress test that continuously configured and unconfigured switches to support Trunking in a mixed fabric, a Management Server daemon panic was observed.
DEFECT000023877	Medium	**Summary:** Call AddAttributes to modify AlarmState and AlarmLevel attributes of FwFruCfg object to invalid values returns SUCCESS. **Symptom:** Call AddAttributes to modify AlarmLevel attributes of FwFruCfg object to invalid values returns SUCCESS Solution: Add function fwValidateFruAlarm to verify fru alarm state and level before setting.
DEFECT000024553	Medium	**Summary:** Upon running diag, SW 12000 (M12) switch core dumps in Management Server daemon. **Symptom:** Running a diagnostic through the Fabric Access API caused the switch to panic and reset.
DEFECT000024660	Medium	**Summary:** Firmwaredownload with option -sf on standby CP: "Oops: kernel access of bad area, sig: 11; TASK = c301c000[2195] 'rpm' Last syscall: 181" **Symptom:** Firmwaredownload on single CP (standby CP) gets error Oops kernel access; system will abort the download process and goes back to original firmware version.

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000024695	Medium	**Summary:** In some rare occurrences, zone DB may get out of sync after fabric merge under security. Usually involves large zone DB (128k) **Symptom:** Test case that exceeds documented boundaries. A zoning DB that is larger then the maximum size supported on 3.1 switches is downloaded to a 4.1 switch in a mixed fabric. The 3.1 switches are appropriately segmented from the 4.1 switches after this happens. Then the security version stamp is reset to zero, and a valid sized zoning DB is downloaded to a 3.1 switch which is a backup FCS switch, which is then enabled so that it will join the fabric. Then a second 3.1 switch is disabled/enabled to cause it re-join the fabric, but in some rare instances, this second 3.1 switch remains in a segmented error state.
DEFECT000024697	Medium	**Summary:** Add non-FCS switch to FCS policy and activate the policy, the non-FCS version stamp becomes "0" **Symptom:** Add non-fcs switch to fcs_policy and activate the policy. Once activation is done, will see the newly added switches are in "Error" status when do secfabricshow. The version stamp on those switches is "0". Security fabric will not see those newly added backup FCS.
DEFECT000024794	Medium	**Summary:** FirmwareDownload failed due to out of disk space or timeout. This happened on 2109-M12 (by Fabric Manager) & 2109-F32 (by CLI)
DEFECT000024879	Medium	**Summary:** Switch stays in 'Red' state in Fabric Manager display; Status reason in events says 'Switch is Not Responding'. Eventually the switch could run out of memory.
DEFECT000024890	Medium	**Summary:** (negative testing) run "systemverification" on both logical switches at the same time. Switch will run out the memory within 5 minutes **Symptom:** Negative test case: Running "systemverification" on both logical switches on the same time will cause the switch to run out memory. **Solution:** Closed by documentation: Systemverificationtest is specifically designed to operate and diagnose both logical switches simultaneously. This command only needs to be run against one logical switch, and both logical switches will be verified. Running this test on both logical switches at the same time causes a duplication of the verification diagnostic to be run, and an over subscription of free memory.

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000024923	Medium	**Summary:** Users should not be allowed to create new Node-WWN zoning configuration, when OPTION_POLICY is activated. A warning message should also be displayed. **Symptom:** If OPTION_POLICY is selected to request that no Node WWN zoning should be allowed, and then later they attempt to create a zone with node WWNs: The zoning transaction is appropriately not allowed to be activated, but the error message as to why the zoning request was not allowed does not clearly state it was due to the OPTION_POLICY enforcement.
DEFECT000024972	Medium	**Summary:** Call AddAttributes to modify SwitchTime attribute of Switch object when External Clock Server is running returns SUCCESS, should return error.
DEFECT000024997	Medium	**Summary:** Improper error code is returned -87 (ERR_SWITCH_ALLOCATION_FAILURE) when calling GetObjects() w/ OID for a HBA that has dropped out of the fabric
DEFECT000025008	Medium	**Summary**: Error message "PD_TRACE-GENERIC" appearing in log file after rebooting the switch every time **Symptom:** Will see this message every time the switch is rebooted. Message is very misleading to the customer
DEFECT000025043	Medium	**Summary:** Continuously ping the 2109-M12 fcip address from the 2109-F32, and do hafailover on the 2109-M12. Then OOPS occurs on the 2109-F32. **Symptom:** This is a stress test in which a denial of service type attack is performed via the in-band FCIP protocol. 2109-M12 was continuously issued pings through 2109-F32 switch. When a fail-over of the 2109-M12 took place, the 2109-F32 saw a panic and a reboot.
DEFECT000025134	Medium	**Summary:** Running stress test to perform security policy operations, transaction flag will out of sync
DEFECT000025196	Medium	**Summary:** Unable to get Telnet Parity or SwitchSupportLog when the target switch Ethernet cable is disconnected. The GET call returns –1 (ERR_INVALID_FABRICLIST) or –56 (ERR_ACCESS_ERROR). **Symptom:** The Fabric Access API command requests SwitchFSPFInterface, SwitchMemoryUsage, SwitchStatus, SwitchVoltageLevel and SwitchCoreFiles) GetObjects/GetSingleObject are unable to retrieve their data objects when the target Ethernet cable is disconnected.
DEFECT000025256	Medium	**Summary:** When RLSServiceEnable attribute of Switch Object is DISABLED, GetObjects on PortErrorsOID of NPort object should return error, still succeeds. **Solution:** Add check for DisabledRLS to interface functions.

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000025286	Medium	**Summary:** EV_API_DOWNLOAD_SUCCESS is still received immediately after issuing FWDLSelf **Symptom:** This is a Fabric Access API issue, in which the Success message for a firmwaredownload is given immediately after issuing the command, even though the download itself may take several more minutes to complete.
DEFECT000025363	Medium	**Summary:** When Target Switch is a 4.1 Switch (doesn't matter about proxy switch), GetObjects or GetSingleObject on SwitchErrorLog OID Multiple Times, API returns Corrupted Error Log Data! **Symptom:** The Fabric Access API fails to recognize an error occurring during retrieval of the error log from the switch.
DEFECT000025400	Medium	**Summary:** Restricting API access to local Fabric Manager host causes transaction to be held until failover **Symptom:** Creating an empty API policy through the FM Security admin screen, and responding YES to the warning about restricting API access, while the API is currently connected to the switch, causes management of the Security features to be locked out.
DEFECT000025451	Medium	**Summary:** Able to download zoneset using CfgDownload **Symptom:** The Fabric Access API was able to download a new zoneset when it was expected to have that functionality blocked.
DEFECT000025469	Medium	**Summary:** 4.1 FabWatch, EncodeFWThresholdEntry using invalid Index, GetSingleObject on the FWOID returns –102 (INVALID_CLASS_AREA) instead of –103 (INVALID_INDEX) **Solution:** thaThresholdStructGet command was returning 0 on success and -1 for all failure cases. It should have returned an error code that identified the specific error. Modified return value in library call such that it returns the proper failure code rather than always returning -1 on any error. In addition, a bug within *InvalidIndex functions where negative numbers were not evaluated as invalid was fixed.
DEFECT000025517	Medium	**Summary:** Port LED behavior with segmented trunk ports **Symptom:** Only the trunk master shows a blinking green light if the switches are segmented. The other trunk member shows a solid green light, which leads one to suspect there is no problem with that link. All trunk members should blink indicating an error condition.

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000025529	Medium	**Summary:** cfgenable different cfg files in a loop resulted in rcsd failed to refresh SWD **Symptom:** Running an overnight script in which different Zoning configurations are enabled over and over in a loop. Configurations switch between hardware-enforced Zoning and soft Zoning, and the configuration is enabled from a different switch in the fabric each time. Running on a 16-switch fabric, a Software Watchdog failure was detected.
DEFECT000025544	Medium	**Summary:** Error message is misleading to the end user **Symptom:** Error messages are not at user level, and do not reflect actual area of failure. Messages: hilsetfruHistory failed, rc=4 for WWN2, WWN 2 removal, WWN 2 insertion, WWN 2 not present. **Solution:** The fix refines the 6 messages related to an intermittent inability to access the WWN FRU, to more clearly indicate what failed and how.
DEFECT000025562	Medium	**Summary:** Oops: kernel access of bad area, sig: 11 during firmwaredownload **Symptom:** When doing repeated firmwaredownloads of both 2109-M12 and 2109-F32 in parallel over a long period of time might experience a kernel panic with message "Oops: kernel access of bad area, sig: 11"
DEFECT000025569	Medium	**Summary:** Incorrect failover with > 32 zone groups or > 128 devices on a quad during filter recovery **Symptom:** The problem can show up in one of two scenarios: Both scenarios require you to have loop devices, this problem will not show up with F-port devices. 1. If you have more then 32 zone groups within one quad (four ports). This means that if you have enough loop devices, and they are all zoned to unique hosts such that more then 32 unique groupings need to be defined within the CAM tables or 2. If you have more then 128 devices total per quad (four ports). If you had a large enough configuration of loop devices in a zoning configuration described above, then a fail-over may improperly zone out the devices that go beyond the limits shown above.
DEFECT000025573	Medium	**Summary:** sfpShow output is not consistent across 2109-F16, 2109-F32 and 2109-M12.

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000025597	Medium	**Summary:** HBAFirmwareDownload fails unexpectedly over short and/or long time periods with error -1000. **Symptom:** While running a stress test that performs continuous HBA firmware downloads to multiple HBAs, sometimes an error -1000 is observed on one or more HBAs.
DEFECT000025612	Medium	**Summary:** Configupload does not accept parameters from command line **Solution:** Parser expected all parameters to be in a single string; combined multiple arguments into single string.
DEFECT000025647	Medium	**Summary:** some of the 3.1 switches are not receiving HBA related API Events **Symptom:** When a Fabric OS 4.1 switch was used as the proxy switch, some HBA-related API events were not delivered to Fabric OS 3.1 switches.
DEFECT000025653	Medium	**Summary:** change telnet timeout default to 10 minutes in v3.0.2c, 2.6.0.c
DEFECT000025682	Medium	**Summary:** BootP installation of v4.1.0 FOS does not load properly on 2109-F32 switches. **Symptom:** Overwriting the switch Flash by running the "install" script, does not properly load the v4.1.0 FOS in the primary and secondary partitions.
DEFECT000025732	Medium	**Summary:** Unzoned Name Server (MS) should reject any registrations or deregistration command codes **Symptom:** Customer will be able to issue Register/Deregister Name Server Command Codes via Management Server Unzoned Name Server sub-type
DEFECT000025743	Medium	**Summary:** passwddefault command will be executable in the backup switch
DEFECT000025751	Medium	**Summary:** get a lot of messages "FSSK 2: fcsw1-swc: FSSK 2: too many concurrent TX" when fabric is reconfigured; then out of memory happened **Solution:** Defect was caused by the temporary presence of a bad fix for another defect that has since been corrected. This symptom caused by this defect will not be seen in any official released version of code.

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000025756	Medium	**Summary:** switchdisable, wait 5 secs, switchenable, wait 20 sec, and haFailover: then fabric keeps reconfiguring **Symptom:** the fabric keeps reconfiguring after doing the following steps switchdisable, sleep 5 secs, switchenable, sleep 20 sec, hafailover the workaround is do switchdisable and switchenable, then the fabric will be stable. **Solution:** Defect was caused by the temporary presence of a bad fix for another defect that has since been corrected. This symptomcaused by this defect will not be seen in any official released version of code.
DEFECT000025763	Medium	**Summary:** When 'ctrl-c' is entered before the login completes, it drops to a shell prompt with no path **Symptom:** When 'ctrl-c' is entered before the login completes, it drops to a shell prompt with no path available. This is easily reproducible in v4.1.0 and all previous v4.x versions of firmware as root. This does not occur as admin.
DEFECT000025770	Medium	**Summary:** Switch panic with msd and psd core files Symptom: After upgrading from an internal FICON code release to v4.1.1, a switch panic was seen shortly after the switch started running. **Solution:** This defect was caused by an invalid configuration installed on the test station. This invalid configuration was caused by a corrupted set of data structures generated by an internal FICON code build that was on the switch prior to the upgrade. This defect cannot be recreated when upgrading or downgrading between official versions of 4.1.0 and 4.1.1 code releases.
DEFECT000025800	Medium	**Summary:** Cannot disable timeout value for logical switch 1 of 2109-M12 switch **Symptom:** Disabling telnet session timeout value for logical switch 1 of 2109-M12 switch will not work correctly
DEFECT000025807	Medium	**Summary:** fail on upgrading firmware to 4.2, cause EM core
DEFECT000025809	Medium	**Summary:** In WebTools event log, enabling a zone config does not register an event. **Symptom:** Enabling a new zone config file does not register an event

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000025828	Medium	**Summary:** Occasionally, some ports are still disabled after bladeEnable, immediately followed by haFailover. **Symptom:** If blades are being enabled in the chassis and haFailover was initiated for some reason, at the same time, some switch port blades are marked disabled **Solution:** Fixed in the 4.1.2 Fabric OS Reference, see attachment.
DEFECT000025877	Medium	**Summary:** JBOD disk disappearing after reboot **Solution:** code changes to vary the old fixed value of LISM. The new LISM timeouts will be from 100ms to 400ms.
DEFECT000025882	Medium	**Summary:** secFabricShow and fabricShow have different number of switches **Solution:** Closed as not reproducible
DEFECT000025905	Medium	**Summary:** after the download is completed on standby getting VERIFY - Failed expression: newPdbP != NULL, file = ucast.c, line = 1347, user mode args = 7, 10, 52, 54 **Symptom:** after all package is downloaded successfully on standby CP, in the middle of hafailover, a VERIFY error was reported. However, the download still completed, and the switch still functions normally.