Brocade Fabric OS 4.1.0

Release Notes

May 2, 2003

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

General Information

Fabric OS 4.1.0 represents the second major feature release of firmware for Brocade's SilkWorm 3900 and SilkWorm 12000 switches. This release adds a large number of significant new features to an already robust and comprehensive firmware platform.

Overview

About This Release

Fabric OS 4.1.0 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 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 and SilkWorm 12000.

It 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

Fabric OS 4.1.0 supports both the SilkWorm 12000 and the SilkWorm 3900.

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

*FT00X0054E9
FT00X0054E9

The serial number label is located as follows:

- *SilkWorm 2000 series switches:* Bottom of chassis
- *SilkWorm 3200 and 3800 switches:* Back of chassis
- *SilkWorm 3900 switches:* Bottom of chassis
- *SilkWorm 6400 and 12000 switches:* Inside front of chassis, on wall to left of ports

3. Worldwide Name (WWN)

- *SilkWorm 3900 and 12000 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

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

SilkWorm switch 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

Fabric OS v4.1.0 software documentation:

- Brocade Fabric OS Reference
- Brocade Fabric OS Procedures Guide
- Brocade Advanced Zoning User's Guide
- Brocade Advanced Web Tools User's Guide
- Brocade Advanced Performance Monitoring User's Guide
- Brocade Distributed Fabrics User's Guide
- Brocade Fabric Watch User's Guide
- Brocade ISL Trunking User's Guide
- Brocade Secure Fabric OS User's Guide
- Brocade MIB Reference
- Brocade Diagnostic and System Error Message Reference

These documents are provided in PDF format on the documentation CD-ROM provided with the switch, except for the QuickStart Guide, as noted. Also, for Fabric OS 4.1.0, the Brocade Diagnostic and System Error Reference manual is a preliminary edition; a completed version will be available by approximately June 1, 2003. In the interim, the preliminary version will be provided in soft copy form to Brocade's OEM and channel partners.

Note: The documentation on the CD-ROM provides information for both Fabric OS v3.x and Fabric OS v4.x.

Standards Compliance

Brocade Fabric OS v4.1.0 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

Brocade Fabric OS v4.1.0 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 and SilkWorm 3900 switches
    - Non-disruptive failover between CPs (Control Processors) on the SilkWorm 12000
    - Additional background health monitoring of the Standby CP on the SilkWorm 12000
    - Managed hot swap procedure for the SilkWorm 12000 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

Brocade’s 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*.

Information About FICON®[1]

The Fabric OS version 4.1.0 release contains code to allow FICON capable hosts and storage systems to connect to the SilkWorm 12000 and transmit FICON data. However, Brocade’s OEM partners have not yet begun the testing and qualification of Brocade’s FICON support in their mainframe and storage environments. For this reason, the Fabric OS 4.1.0 code should NOT be used for FICON product qualification, end user FICON beta testing, or end user deployment in FICON environments. Brocade continues to test its support for FICON extensively and will provide a release supported for FICON deployments upon completion of FICON environment qualification testing by Brocade and its partners.

Requirements and Compatibility

Brocade Fabric OS v4.1.0 can be installed and run on the SilkWorm 3900 and SilkWorm 12000.

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

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

	SW 2xxx	SW 3200 & 3800	SW 3900	SW 12000	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 3900s 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 SilkWorm 3900 and SilkWorm 12000. 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 SilkWorm 2000 series, SilkWorm 3000 series or the SilkWorm 6400 integrated fabric to inter-operate in the same fabric with the SilkWorm 3900 and SilkWorm 12000 switches, contact your switch provider.

Limitations

SilkWorm 2xxx Scalability Limits

Exhaustive testing has demonstrated that SilkWorm 2000 family switches 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 SW 3900 Hot Code Activation

During code activation on a SilkWorm 3900 running Fabric OS 4.1.0 or later, data keeps flowing between hosts and storage devices. However, fabric services are unavailable for a period of approximately 50-55 seconds. Possible disruption of the fabric can be minimized by ensuring that switches logically adjacent to the SW 3900 (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&.

Other Important Notes:

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

Area	Description
Ethernet Port IP addresses	**NOTE:** When a SilkWorm 12000 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 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, 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:** Refer to the *Fabric OS Procedures Guide* "Firmware Download" chapter for limitations when changing Fabric OS versions. When installing Fabric OS v4.1, the procedure may vary depending on which version of the Fabric OS you are migrating from.

Area	Description
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.**
License removal	**NOTE:** When a user removes a license from the switch, the feature is not disabled until the switch is rebooted or a switch disable/enable is performed.
LTO 2 Tape Drive Support	When using the LTO 2 Tape Drive, the user must perform the following command on both Fabric OS 3.x and 4.x: switch> portcfggport *port# where drive is plugged into* This will allow the tape drive to function in point to point mode rather than in loop.
OS - Hardware	**NOTE:** Bringing up port blades during a failover could cause the port cards to come up in a disabled state. This is a rare occurrence, and when this happens, redo the port blade bringup after the failover on the SilkWorm 12000.
Port Swapping	**NOTE:** While the portSwap command will ultimately be usable on both FICON and Fibre Channel ports, it is not supported in this release. It will be supported concurrently with FICON.
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. 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.

Area	**Description**
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 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.
WWN card FRU repair	**Problem:** If an HA failover or power cycle occurs during a FRU on the WWN card, the SilkWorm 12000 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.

Documentation Addendum

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.”

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 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*.”

Known Defects for Fabric OS 4.1.0

This table of open defects lists those defects that, while still formally “open”, are unlikely to impede Brocade’s customers in their deployment of Fabric OS 4.1.0. The presence of a defect in this list may be prompted by several different circumstances. Several of the defects were not detected in the months of testing on Fabric OS 4.1, but were initially reported against another Fabric OS version in the field. Brocade’s standard process in such cases is to open defects against the current release which *might* experience the same issues, and close them only when a fix is implemented, or if it is determined that the problem does not exist with the current release. In other cases, a fix has been developed, but has not been implemented in this release because it requires particularly extensive regression testing to ensure that the fix does not create new problems, and that testing is not yet complete. Such fixes will appear in future maintenance releases. The remaining defects in this table are still under investigation to determine a root cause. None of them have the requisite combination of probability and severity to cause significant concern to Brocade’s customers.

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000024217	High	Summary: Switch not sending enough LIPs to transition from AL-PA sequence to Old_Port Workaround: Using portCfgGPort causes the issue to be avoided. Customer Impact: The workaround has been agreed upon between Brocade and the manufacturer of the LTO 2 tape drives.

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000024982	High	Summary: Est 5 sessions each to 2 4.1 switches and call GetAllObjectsBySession core dumps msd and returning objects with -209 & -86 when fabric is stable. Symptom: Using the Fabric Access API to retrieve the current FICON mode setting via ten concurrent sessions (five on each switch) caused a core dump of the Management Server process. Customer Impact: Accessing the FICON mode setting is not supported in Fabric OS 4.1.0. A fix for this defect has already been implemented in the FICON code.
DEFECT000025179	High	Summary: When doing AddAttribute to change Switch IP Address to "0.0.0.0", Switch Panics and Dumps core. Switch reboots continuously ... Symptom: Setting switch IP address to 0.0.0.0 during an SNMP or API management session caused the switch to panic. Customer Impact: This action would clearly disrupt any management session, and should never be done.
DEFECT000025331	High	Summary: Modifying switch and CP IP addresses caused a telnet hang. Symptom: Changing the switch IP address before changing the CP IP address will cause the CP IP address to become inaccessible on a subsequent attempt to set the switch IP address. Workaround: • When both CP and switch IP addresses need to be changed: set the CP IP address first and then the switch IP address. • When only a switch IP address needs to be changed, set the CP IP address first (keeping the current value) and then the switch IP address to its new value. • When only a CP IP address needs to be changed, there is no problem; just change the CP IP address. If a customer gets into this scenario, telnet into the switch and set the CP IP address again, accepting the default values. Customer Impact: This behavior is identical to how the code works in 4.0.2. There is a well documented workaround.

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000025474	High	Summary: After fastbooting standby CP of the primary FCS, doing secfcsfailover before HA is in sync results in old primary FCS switch's active CP panicking. Symptom: This is multiple failure test case, on which first the standby CP of the primary FCS switch is issued a fastboot and then prior to the HA state achieving synchronization, a 'secfcsfailover' command is issued from a standby FCS switch. The old primary FCS switch is segmented out of the fabric. Workaround: Issue switchdisable, switchenable to the segmented switch to cause it to rejoin the fabric. Customer Impact: This test case demonstrates a very specific double point of failure that may cause a switch to be segmented from the fabric.
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. Customer Impact: This defect is difficult to reproduce. The fix for this defect will be considered for Fabric OS 4.1.1.
DEFECT000025606	High	Summary: Performance Monitor process dies when switchdisable / switchenable script running. Symptom: With 2+4+28 mixed configuration, which has 6 12000s, 6 3800s, 22 3900s, ~700 device ports, 95Kbytes zone size, and traffic. Action: running a switchdisable/switchenable script on all 4.1 edge switches (include 4 12000s and 22 3900s) 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 with message "Switch: 0, Critical kSWD-kSWD_GENERIC_ERR_CRITICAL, 1, kSWD: '[12]psd:0'...". Customer Impact: The fix for this defect will be considered for Fabric OS 4.1.1.

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000021352	Medium	Summary: fruHistoryTrap does not generated or is not generated properly. Symptom: SNMP FRU history trap is not always generated as expected. Customer Impact: With the addition of the Managed WWN card Hot swap, the FRU trap mechanism does not always catch the fact that the WWN card has been replaced. However, this is not like a blower which can be hot swapped without the administrator knowing about it. Hot swap of the WWN card REQUIRES active participation by the administrator.
DEFECT000021881	Medium	Summary: no trap generated when firmwareDownload completes Symptom: No SNMP trap is generated when a firmwareDownload completes. Customer Impact: This is a request to create a new type of SNMP trap mechanism to inform the SNMP agent upon the completion of a Hot Code Activation. There is no impact to existing environments as this request is a request for enhancement.
DEFECT000023377	Medium	Summary: Contents of sfpshow does not get updated when SFP is replaced Symptom: Replace a IBM SFP with a Finisar SFP. sfpShow still shows IBM SFP information while the physical SFP is a Finisar SFP. Workaround: Wait 5 to 10 minutes and re-issue the sfpShow command.
DEFECT000024542	Medium	Summary: No log message is generated when one CP resets the other CP. Solution: This message was removed in order to fix Defect 25094. Customer Impact: There will be no message printed when one CP resets the other.
DEFECT000024769	Medium	Summary: REG: EVT_TC_154 : When trunk port is disabled on 4.1 proxy switch, API is receiving an EV_STATE_CHANGE event 2 times Symptom: Fabric Access API test case in which a trunking port is disabled, but the disable event is being reported twice via the API. Customer Impact: This issue will only be seen when using the Fabric Access API. The two events being reported are "Trunking port down" followed by "Port Down". If the user did not realize they were disabling a trunking port, then the two status changes could be interpreted as confusing. This behavior will be documented in the Fabric Access API documentation

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000024773	Medium	Summary: When 4.1 Proxy Switch is disabled, switch generates lot of events saying Trunk Ports are disabled. But API is not receiving any such events. Symptom: Fabric Access API test case that causes Trunking port events to be reported to the console, but there are no events reported via the API. Customer Impact: This Trunking port console messages are the result of an end user request to have printed messages on the console port. These are not error log events, and thus are not being reported via the API. This is an RFE that is being considered for a future release.
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. Customer Impact: This is a request to introduce a new error reporting mechanism that can forward an error detected within the Security module up through the zoning module for reporting to the user. This is a request for enhancement that will be considered for possible inclusion in future releases.
DEFECT000024975	Medium	Summary: when configdownload succeeded on zoneDB but failed on sec policy, primary fails to propagate zoneDB to fabric Symptom: When performing a configDownload that modifies both the zoning DB and the security DB, an error within the security DB will prevent the zoning DB from being activated in the fabric, but it will not prevent it from being loaded into the flash memory. Workaround: Correct your mistake in the Security section of the configuration file and repeat the configDownload. Do NOT reboot the FCS prior to correcting the configuration file. Customer Impact: This situation will only happen when both zoning and security DB are modified, and an error is injected into the security DB config. The root cause is well understood; however, the complexity of the required modifications to the configDownload code would have introduced significant risk to the program.

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000025156	Medium	Summary: Error related to blade- 9 and 10 were logged to switch-0 error log instead of switch-1 error log. Symptom: A faulty blade inserted into slot 9 or 10 of the switch was producing the appropriate error messages, but they were being logged under switch 0's error log instead of switch 1 as expected. Customer Impact: The logging mechanism prior to the switch being fully online is to log all errors to switch 0's error log. This is an identical mechanism to 4.0.0 and 4.0.2.
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. Customer Impact: This defect will only be seen when running the Fabric Access API through a proxy switch instead of having Ethernet cable connections to each switch.
DEFECT000025216	Medium	Summary: The time stamp for firmware download from Fabric Manager/Webtools is off by 8 hours compared to time on the switch. Symptom: Users who attempt to upgrade switch firmware from Fabric Manager or Webtools, will see a time difference of 8 hours Customer Impact: There is no operational impact due to this defect.
DEFECT000025259	Medium	Summary: 4.1 switch panic and dump core during switchreboot Symptom: A switch panic was observed during a Fabric Access API test run. Customer Impact: This defect cannot be recreated and has not been seen since it was first observed. The core dump has provided the root cause of the problem and an architectural solution is currently under investigation for a future release.
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. Customer Impact: This does not prevent the firmwareDownload from completing normally.

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000025297	Medium	Summary: "tsd" core dump on SW3900 switch interrupted the time synchronization with Primary FCS switch Symptom: When a switch reboot or panic takes place when a Time Service update is in progress, the time server failed the synchronization with the Primary FCS switch. Customer Impact: The time service synchronization will only fail, if a reboot or panic is observed concurrently with the synchronization. Re-issuing the time service command will cause the synchronization to take place. Probability: Low
DEFECT000025322	Medium	Summary: fabric is reconfigured when doing hafailover w/ reason "Reconfiguration due to HA: RJT EFP resp(port 57)" Symptom: An E-port that is not properly segmented will cause a fabric reconfiguration when a fail-over takes place on the switch. Customer Impact: This is a double point of failure, in which first a faulty segmentation of an E-port must exist. A fail-over taking place while the switch has an E-port in this condition, will cause an extra fabric reconfiguration to take place.
DEFECT000025342	Medium	Summary: No FDMI related events are generated when port that has HBA connected is enabled/disabled Symptom: In a large fabric environment, when an extremely large number of RSCNs are being generated, FDMI events were not generated through the Fabric Access API. Customer Impact: This defect will only affect the Fabric Access API's ability to report events taking place on FDMI devices. Re-running the test cases without the extreme RSCN generation events failed to reproduce the defect, and all FDMI events were properly reported.
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. Customer Impact: This is very difficult to reproduce and requires an error to be reported by the switch during error log retrieval. Probability: Low

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000025371	Medium	Summary: Relocating switch port cable would lose dynamic EE monitors residing on the port Workaround: Dynamic EE monitors will not move with the device. When relocation of device happens, the monitor needs to be deleted and added back manually.
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, cause management of the Security features to be locked out. Workaround: Issue an haFailover to restore management capability over the Security feature set. Customer Impact: This defect requires the user to be connected via the Fabric Access API at the same moment that an empty API policy is created and activated.
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. Customer Impact: This defect will only be seen when using the Fabric Access API. This fix is planned for implementation in Fabric OS 4.1.1.
DEFECT000025479	Medium	Summary: Fabric Manager can't get FirmwareDownload Status, but fwdl actually completed successfully Customer Impact: The fix for this defect will be considered for Fabric OS 4.1.1.
DEFECT000025494	Medium	Summary: WebTools display of segmented trunk ports Symptom: In the WebTools display, when a trunk group is segmented, only the trunk master is shown with a blinking light indicating an error. The other links in the trunk continue to be shown with a solid green light, suggesting no error. Customer Impact: This defect will be considered for Fabric OS 4.1.1.
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. Customer Impact: This defect will be considered for Fabric OS 4.1.1.

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000025530	Medium	Summary: Running switchcfgtrunk0/1 test with 15 minute interval, see RTWR-FAILED, 2, rtwrRespProcess: release_kiu failed Symptom: Simultaneously issuing switchCfgTrunk commands to all 20 switches within a fabric alternating between enabling and disabling Trunking caused an error message to be displayed. Customer Impact: This defect will be considered for Fabric OS 4.1.1.
DEFECT000025534	Medium	Summary: SwitchCfgTrunk leaves ports disabled if a long distance port is configured on the switch. Symptom: Activating Trunking at the switch level (switchCfgTrunk) when a long-distance port is currently configured causes the error message "No Trunking support of long distance port" to be displayed, which is correct. However, other trunk ports are then left in a disabled state. Workaround: There are 2 ways to avoid this issue 1. Use portcfgtrunkport to enable the trunk for each port (recommended) 2. disable long distance port before issue switchcfgtrunk Customer Impact: This defect will be deferred for consideration in a future release.
DEFECT000025543	Medium	Summary: Step 9 of Firmwaredownload Completes With Error: CP1: Standby cp failed to reboot. Symptom: Standby CP failed to reboot when upgrading from 4.0.2c to 4.1.0_rc1; both CPs restore from secondary partition to correct itself. Customer Impact: The firmwareDownload failed at the auto-Commit stage, however the firmwareDownload actually completed. A manual reboot of the machine resulted in the SW 12000 running properly with Fabric OS 4.1.0.
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. Customer Impact: Error messages will be improved in Fabric OS 4.1.1.
DEFECT000025562	Medium	Summary: Oops: kernel access of bad area, sig: 11 during firmwaredownload Symptom: When doing repeated firmwaredownloads of both 12K and 3900 in parallel over a long period of time might experience a kernel panic with message "Oops: kernel access of bad area, sig: 11" Customer Impact: Problem has only been seen once; still attempting to recreate.

Open Defects		
Defect ID	**Severity**	**Description**
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. Customer Impact: Recommended configurations limit loops to about 30 devices each, no one should go over 120 devices per quad. Nonetheless, this will be fixed in Fabric OS 4.1.1.
DEFECT000025573	Medium	Summary: sfpShow output is not consistent across 3800, 3900 and 12000. Customer Impact: This defect will be considered for Fabric OS 4.1.1.
DEFECT000025580	Medium	Summary: Able to reset version time stamp when login as "user" Customer Impact: This defect will be considered for Fabric OS 4.1.1.
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. Customer Impact: This defect will be considered for Fabric OS 4.1.1.
DEFECT000025612	Medium	Summary: Configupload does not accept parameters from command line. Customer Impact: This defect will be considered for Fabric OS 4.1.1.

Defects Closed Since v4.0.2 Release

This table lists the defects that have been closed since the last GA release, Fabric OS v4.0.2.

Defects Closed Since v4.0.2		
Defect ID	**Severity**	**Description**
17838	Critical	Inability to ping or telnet to switch. Data is still running but switches cannot be managed. The interrupt mitigation code was changed to use the "Smart Reset" feature of the ethernet hardware rather than disabling the MAL temporarily.
18525	Critical	Slotpoweroff/Slotpoweron causes slot to lose D_ID . Code has been changed and Slotpoweroff/Slotpoweron does not cause slot to lose D_ID
18967	Critical	nsdb_gepn function, which is invoked through API and MS, when writing to freed memory causes corruption. A new variable has been added to hold response CT instead of wrongly using the request CT.
19034	Critical	FLOGI storm causes the switch to failover due to rejecting the FLOGI on a loopback. The code has been changed to accept the FLOGI, rather than rejecting it to prevent the switch from failing over.
14545	High	Frames are being dropped at the switch with HSV-HSV replication.
14880	High	Web Tools firmwareDownload from and to V4.0.0 <-> V4.0.0a,b,c does not work.
14898	High	Unnecessary link reset causing I/O between sw0 and sw1 to pause for 70 seconds.
14990	High	Changing switch name causes all SW12000 with hosts attached to failover.
14994	High	Firmwaredownload fails to download firmware after FTP server down/restored.
14995	High	Sig=11 seen, Nameserver and Zone Daemon died on restart of daemons.
14996	High	Sig=11 CoreDump files missing after HA failover.
14997	High	Sig =11 CoreDump seen after Fabric Daemon died on Ed-12000B edge switch.
14998	High	Web Tools gives cryptic messages during failed firmwaredownload (CP1:.Null).
14999	High	The switch continues to send the OLS/NOS.
15000	High	ASIC failure specific to the turboramtest command.
15377	High	SW 12000: When the individual logical switches (switch 0 and switch 1) in a SW 12000 chassis are rebooted nearly simultaneously - only a second or two apart - using the switchreboot command, the console port for the active CP card will report that the CP card is out of memory, and will fail over to the Standby CP card. To avoid encountering this problem, do not use successive switchreboot commands to reboot both logical switches; use the reboot command instead. This defect is extremely rare, having occurred only twice in over three months of testing.
15379	High	SW12000 Switch: 0, Critical PDM-SSPFAIL, 1, Snapshot to primary failed (-1) error; explain error condition.

Defects Closed Since v4.0.2		
Defect ID	**Severity**	**Description**
15380	High	SNMP infinite loop response to connUnitLinkUnitId query. If exactly one device is plugged into a SW12000 and you query the FC Management MIB's connUnitLinkUnitId field, it enters into a never-ending stream of identical responses.
15391	High	SW12000 web server vulnerability.
15393	High	SW12000 web server vulnerability.
15584	High	Problem with firmwareDownload command instructions.
15738	High	SW 12000: Rarely, an httpd daemon can die with signal 11 on a SW12000 switch. Web Tools then would not be able to restart httpd daemon.
15835	High	portcfgspeed command variable inconsistency.
15984	High	Switch panic when removing cables.
16048	High	SW 12000: When switchdisable and switchenable operations are performed while a port card is loaded with loop device traffic, the port card may report “Bloom FDET errors”, causing port card to be flagged as faulty. This happens intermittently, on about one out of every fifty switchdisable operations. This is a false negative - the port card is not actually faulty and need not be replaced. To avoid this possibility, the user should stop any loop traffic before performing the switchdisable operation. If the defect occurs, the recovery procedure is to re-enable the port card. Note that this does NOT result in an unplanned disruption of application traffic, since the administrator is shutting down the logical switch, using the switchdisable command.
16190	High	Fan reported as faulty but no LED was lit to indicate which FRU had failed.
16292	High	Switch crashed and rebooted.
16369	High	Rarely, when the speed of ports in a trunk is toggled repeatedly between 1 Gbps/sec and 2 Gbps/ sec, connectivity to devices through the trunk may be temporarily lost. This defect should never occur in an production environment, since end users are recommended not to repeatedly change the speed of ISLs in trunks. This action reduces throughput and causes the trunks to be torn down and rebuilt repeatedly. This is an intermittent problem, and occurs very rarely.
16383	High	Switch is not sending RSCN, after target device registers to name server with RFT_ID.
16385	High	Switch not sending enough LIPs to transition from AL-PA sequence to Old_Port.
16504	High	There is a limit loop initialization fault, such that when the host reboots the SW12000 crashes.
16543	High	Web Tools: When executing a firmwaredownload through CLI and viewing the status in Web Tools, the messaging and status bar may indicate a firmwaredownload in progress when firmwaredownload is not functioning.
16544	High	Interrupting the firmwaredownload process within the first 20 seconds blocks future firmware downloads.
16545	High	Discarded frames during data transfer in 9900 remote copy.

Defects Closed Since v4.0.2		
Defect ID	**Severity**	**Description**
16552	High	Port Blade deemed as faulty with the following message: Switch: 1, Critical BLADE-REG_FAULT, 1, ASIC driver detected Slot 7 port 40 as faulty (reason: 13).
16565	High	Imbalance problem due to routing.
16617	High	Webtools crashes when ethernet cable is removed when running Netscape 4.77 on a Solaris host. Best recovery method to use if this issue is encountered is to end the Netscape session and start a new one.
16634	High	Web Tools fails to resolve switches in Fabric View. Fabric View depends on the fabricshow command to display switches. Occasionally during re-configuration IP address on switches do not get reported correctly by fabricshow command. If you do not see switches in Web Tools, log into the CLI and run fabricshow to confirm the IP addresses of the switches are displayed correctly, this will fix the display problems in Web Tools.
16635	High	Port was faulted and could not recover until user intervened.
16691	High	SW 12000: In a 16 switch fabric, CP on core fabric switch failed over. Related to defects 16721 and 15377.
16721	High	The switchreboot command sometimes fails to re-enable switch, and switch remains in disabled state. Related to defects 16691 and 15377.
16803	High	On a nightly build, systemtest would fail due to a coding error that caused an internal buffer to be released twice.
16983	High	LINIT not working properly; the switch sends a LIP(F7,F7) instead of a LIP(CD,00) in response to a LINIT (CD,00).
17038	High	SW 12000: Error message that standby CP failed to reboot and firmware download was aborted after firmware was downloaded to the standby CP and the standby was rebooted.
17040	High	SW 12000: If firmwaredownload fails on the standby CP, in some circumstances the switch may be left with two different versions of microcode on the switch partitions.
17044	High	After firmware upgrade, name server daemon died while driving I/O, causing switch to reboot.
17195	High	A message Bloom_Bad_ID is reported during fabric instability. This is only a warning message. The BLOOM-BAD_ID error log level was changed from Critical to Warning.
17460	High	A specific type of HBA does not login as F_Port, and the switch port is faulted.
17566	High	SW 12000: The startup timer for http daemon (Web Tools) is too short for an 8-port card system running POST. The daemon start sometimes gives up to soon, and it is necessary to disable POST and perform a switchreboot, hafailover, fastboot, or power cycle.
17648	High	In one instance, running zoning manipulation tests simultaneously on both logical switches of a SW12000 resulted in a switch reboot.
17655	High	Storage device’s private loop port is taking ~3.5 minutes to login to switch.

Defects Closed Since v4.0.2		
Defect ID	**Severity**	**Description**
19740	High	The switch reboots due to spurt of Loss of Sync interrupts. The code has been changed to monitor the number of LLI interrupts and if the number goes beyond the threshold, the port will be faulted.
22631	High	If a cable is continuously pulled from one L port with a device using ALPA 0xEF, the other L port in the same quad will occasionally start to LIP. The timeout frame on list0 is not removed, which prevents the timeout flag from being cleared.
23119	High	After a host reboot the switch port is faulted before the HBA can establish a connection with the switch port. This problem is only observed with QLogic 2310 with BIOS 1.30 not with any other versions of the Qlogic HBA or BIOS. This issue is resolved with 4.0.2d and Qlogic BIOS v1.34
24156	High	Semaphore blocking occurs when a Terminal server flow control is set to on. Flow control enabled on a terminal server connected to the serial port of a switch can cause the switch to hang and telnet and serial ports to become inaccessible. The following commands shellFlowControlEnable and shellFlowControlDisable were added to address this issue. shellFlowControlDisable is the default setting.
24574	High	L-Port cannot be re-initialized after the HDS RCU's hot code load.
16852, 17240	High	API usage of Zoning: Switch RPCD and ZONED daemons core dumped by API application.
17197, 17194	High	On a specific fabric, a single SW 3900 was found trying to restart its http daemon unsuccessfully and continuously.
17227, 17192	High	In one case, an older zoning configuration replaced changes made an hour earlier.
18099 (secondary of 16545)	High	Frames discarded during data transfer in 9900 remote copy
17819 (secondary of 17313)	High	Management server is sending incorrect WWN in the ACC for an ADISC.
17139, 17238, 17239	High	API usage of Zoning: Using the API, the switch rebooted after repeated uses of Create Zone; Add to ZoneSet.
14673	Medium	SW 3900: XML, Using SW 3900 as proxy switch, GetObjectsByType() returns missing attributes for Port objects of 4.0 switch.
14896	Medium	cfgenable takes more than 1 minute and 30 seconds to finish.
15002	Medium	(2) HALT modified units are not reporting digital smart features correctly.
15003	Medium	WWN is not displayed in the Web Tools GUI representation of a SW12000 switch.
15114	Medium	firmwaredownload from v4.0.0d to v4.0.0c had file system corruption after reboot with new CP card.
15126	Medium	firmwaredownload command fails after issuing a false server IP address.
15342	Medium	emd panic while doing slotpoweroff/slotpoweron on all port cards overnight.

Defects Closed Since v4.0.2		
Defect ID	**Severity**	**Description**
15426	Medium	The filterportshow command during switchreboot command caused kernel panic.
15604	Medium	The switch serial # does not match the internally stored serial #. WWN of switch matches internally stored SN.ch View in Web Tools for logical SW1 then remove the ethernet cable, the error “Lost connection to the switch” displays for SW1 only.
15645	Medium	There is no configshow output when a supportshow command is issued on SW12000.
15862	Medium	Unit serial # label does not match internally stored Serial # on switches. WWN of switch matches internally stored SN.
15920	Medium	Double-clicking Route Row Values in Admin-Routing locks out all Web Tools panels with no dismiss info.
15981	Medium	In Web Tools, you cannot “Reset” any of the selections in the “Upload/Download” tab.
16000	Medium	SW 12000: Running a script caused active CP to hang. The Standby CP is ok. Hashow shows that active CP information not available.
16050	Medium	ASIC error, then port card is faulted (if labmode is 0). The switch is not returning R_RDY after receiving 16 frames, and consequently, panic on bloom error happens.
16081	Medium	The httpd died with signal 11. Error log indicated that core files were being dumped, but there are no files.
16185	Medium	GA labeled build version string not consistent with other releases.
16223	Medium	Firmware download failed through CLI but Web Tools reported it as successful.
16338	Medium	Principal switch selection fails over remote switch devices.
16442	Medium	“Savecore” utility is no longer working.
16524	Medium	Version string is incorrect.
16535	Medium	The chassis serial number is not stored with unit, remote dispatch of service hampered. Need addition of chassis serial number for unit identification through CLI and GUI. The chassis serial number has been added to the "Info" panel within WebTools switchview and the chassisshow command for CLI.
16537	Medium	Port was non-functional with amber light blinking, but the switchshow command did not indicate fault.
16539	Medium	The following message posted in error log: “0x27a (fabos)...Detected unstable fabric....”
16540	Medium	SW 3900: All messaging relating to dual CP and or its architecture should be removed from Web Tools.
16541	Medium	HBA not able to login to ports 8 and 9 until portdisable and portenable executed.
16579	Medium	Switch exception, no element available.

Defects Closed Since v4.0.2

Defect ID	Severity	Description
16636	Medium	Two switches report critical EM NULL_NULL inventory messages after receiving a reboot command via user script.
16710	Medium	firmwareDownload help text does not accurately describe command switch function.
16718	Medium	On the Fabric Watch screen, in Web Tools, the time base for current value and last value in (every class) Fabric class, SFP state change area is not correct.
16730	Medium	"Savecore" utility does not delete core files and gives unexpected error messages.
16731	Medium	SW 12000: Modem ports are not initializing correctly. The modems are not getting the proper configuration strings, based on the return data, which appears to reflect a FASTER baud rate than 9600.
16863	Medium	configDownload command does not verify domain ID, allowing download of config file with incorrect domain ID.
16900	Medium	Zone member displayed as unavailable (red with X) even though it was available.
16935	Medium	Ignore the following message; it is a debugging message left in by mistake. There is no impact to the functionality of the switch. Critical PLATFORM-FUNCT_FAIL, 1, fabsys_set_HwUnitFatal i2c bus error, can't recover If this message is followed by an "EM, I2C_TIMEOUT" error message, follow standard troubleshooting procedure for an I2C time-out message.
17045	Medium	No error message displayed to indicate failed port speed negotiation / E_Port initialization.
17468	Medium	Rarely, while running an overnight script of continuous switchreboot command entries, a switch can sometimes run out of shared memory resources.
17744	Medium	During Random changes from healthy to marginal the warning by the switch in fabric testing at 40 deg C. the switch status message does not include a reason. The code has been changed to add the reason string to switch status message.
18019	Medium	cfgsave does not issue error message when trying to save cleared zoning config when cfg is enabled.
18128	Medium	'rpcd' processes are left in a "zombie" state because an API application connection is broken abnormally. The processes should be cleaned-up within 2 hours, but are continuing to exist indefinitely until the switch is rebooted. The code was changed so that the semaphore is cleared which the cleanup handler was waiting for.
19518	Medium	E-port Link Timeout from silkworm 2800 switches in a 20 switch mixed fabric.
11926, 14255	Medium	v4.0 BFOS documentation does not list SSN.
14881	Low	Help command prompts should auto-exit when all help commands have already displayed.

Defects Closed Since v4.0.2		
Defect ID	**Severity**	**Description**
14887	Low	API: Error print message printing offending IP in reverse order.
14891	Low	API: Intermittent Problem: Switch rebooted automatically.
15051	Low	Tool tip for the “Reset” button is incorrect.
15072	Low	Wrong data byte #3 displayed as pinging Host's FCIP address.
15462	Low	Switch 0 is not accessible after removing the ethernet cable during the configDownload, then replacing the cable.
16063	Low	Add switch name to banner for firmware download completion message.
16130	Low	Diagnostic summary and error messages need rewording.
16147	Low	Fabric Watch (fwmailcfg) created bogus email recipients.
16199	Low	To be consistent with the configDownload command, add a caution message to the Confirm Configuration Download dialog box.
16319	Low	Received critical message after rebooting, even though switch is functioning.
16700	Low	Control processor card host names not persistent across reboots.
17047	Low	Error message for an aborted firmware download was sent 30 minutes after failure.
17309	Low	BurninStatus command does not issue correctly. A path was added for the Linux commands to allow admin login to run burninststus.