Brocade Fabric OS v4.4.0

Brocade Release Notes_v1.0

October 22, 2004

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v4.4.0 Release Notes v1.0	First release.	October 22, 2004

TABLE OF CONTENTS

Overview

Brocade Fabric OS version 4.4.0 contains significant enhancements in the areas of Fibre Channel long-distance support, scalability, and manageability. In addition, several improvements since the release of Fabric OS version 4.2.0 have been incorporated in this release. Major new features include:

- Support for the SilkWorm 4100 and the SilkWorm Multiprotocol Router Model AP7420.
- Greater than two-fold increase in Brocade Extended Fabrics support:
    - SilkWorm 3250, 3850, and 24000-series distance support up to 200 km at 1 Gbit/sec and 100km at 2 Gbit/sec
    - SilkWorm 4100 distance support up to 500 km at 1Gbit/sec and 100 km at 4 Gbit/sec
- Trunking over Brocade Extended Fabrics
    - SilkWorm 3000-, 12000-, and 24000-series two links up to 50 km at 2 Gbit/sec and 4 links at 10km at 2Gbit/sec
    - SilkWorm 4100 three links up to 250 km at 2Gbit/sec and 100 km at 4 Gbit/sec
- Increased scalability to 2560 ports and 50 domains
- Ports on Demand (POD) for instant scalability via license keys
- Fabric Watch improvements:
    - Improved notification
    - Switch health reports
- Standardized messaging: for example, including information such as time stamp, message number, severity, and switch name for all system messages
- Updated security enhancements:
    - SSH
    - RADIUS
    - DH-CHAP authentication
- Fabric Watch and Web Tools usability enhancements
- FICON®/CUP support for SilkWorm 3900, 12000, and 24000.

Brocade software release policy is to carry forward all fixes in patches to subsequent maintenance and feature releases of Fabric OS.

Supported Switches

Fabric OS v4.4.0 supports the SilkWorm 3016, 3250, 3850, 3900, and 4100 switches and the SilkWorm 12000 and 24000 directors.

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 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 numbers and messages received
   - **supportSave** 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 here.

   

   The serial number label is located as follows:

   - SilkWorm 3016: Side of switch module
   - SilkWorm 3250, 3850, and 3900 switches: Back of chassis
   - SilkWorm 4100 switches: On the switch ID pull-out tab located on the port side and on the inside of the chassis, near power supply 1 (on the right when looking at the nonport side)
   - SilkWorm 12000 and 24000 directors: Inside front of chassis, on wall to left of ports
   - SilkWorm Multiprotocol Router Model AP7420: On the bottom of the chassis and on the back of the chassis.

3. **World Wide Name (WWN)**

   - SilkWorm 3016, 3250, 3850, 3900, and 4100 switches, and SilkWorm 12000 and 24000 directors: Provide the license ID. Use the **licenseIdShow** command to display the license ID.
   - SilkWorm Multiprotocol Router Model AP7420: Provide the switch WWN. Use the **switchShow** command to display the switch WWN.
   - All other SilkWorm switches: Provides the switch WWN. Use the wwn command to display the switch WWN.

Standards Compliance

Brocade Fabric OS v4.4.0 conforms to the following Fibre Channel Standards in a manner consistent with accepted engineering practices and procedures. In certain cases, Brocade might add proprietary supplemental functions to those specified in the standards. Brocade verifies conformance with Fibre Channels Standards by subjecting its switches to SANmark Conformance Tests developed by the Fibre Channel Industry Association. Brocade switches have earned the SANmark logo, indicating such conformance. SANmark is a limited testing program and does not test all standards or all aspects of standards.

- FC-AL ANSI X3.272: 1996
- FC-AL-2 NCIT S 332: 1999
- FC-FLA NCIT S TR-20: 1998
- FC-GS-4 ANSI INCITS 387-2004 (Includes FC-GS-2 and FC-GS-3)
- FC-PH ANSI X3.230: 1994 (Included in FC-FS)
- FC-PH-2 ANSI X3.297: 1997 (Included in FC-FS)
- FC-PH-3 ANSI X3.303: 1998 (Included in FC-FS)

- FC-PLDA NCIT S TR-19: 1998
- FC-SW-3 INCITS 384:2004 (Includes FC-SW and FC-SW-2)
- FC-VI INCITS 357:2002
- FC-DA Rev 3.1 (Under Development)
- FC-SP Rev 1.6 (Under Development)
- FC-MI INCITS/TR-30:2002
- FC-MI-2 Rev 2.5 (Under Development)
- FC-PI INCITS 352:2002
- FC-FS INCITS 373:2003
- FC-BB-2 INCITS 372:2003 (Includes FC-BB)
- FC-SB-3 1.6 (Includes FC-SB-2)
- RFC 2625 IP and ARP Over FC
- RFC 2837 Fabric Element MIB
- RFC 3643 FC Frame Encapsulation
- FCP ANSI X3.269: 1996
- FCP-2 INCITS 350:2003
- SNIA Storage Management Initiative Specification Version 1.02

Important Notes

This section lists information you should be aware of when running Fabric OS v4.4.0.

OS Requirements

The following table summarizes the versions of Brocade software that are supported in conjunction with this release. These are the *earliest* software versions that interoperate. Brocade recommends using the *latest* software release versions to get the most benefit from the SAN.

Effective February 2004, Fabric OS v2.4.x or earlier, v3.0.0x or earlier, and v4.0.0 or earlier have reached their end-of-life and are no longer supported.

Effective September 2004, Fabric OS v2.6.0x and earlier, v3.0.2x and earlier, and v4.0.2x and earlier reached their end-of-life and are no longer supported.

	SilkWorm 2000 Series	**SilkWorm 3200 & 3800**	**SilkWorm 3016, 3250, 3850, 3900, 12000, & 24000** [1]	**SilkWorm 4100** [2]	**Fabric Manager**
General compatibility	v2.6.1 or later	v3.1.0 or later	v4.1.0 or later	v4.4.0 or later	3.0.2c or later
With Secure Fabric OS enabled	v2.6.1 or later	v3.1.2 or later	v4.2.0 or later	v4.4.0	3.0.2c or later
Recommended software versions	v2.6.2	v3.2.0	v4.4.0	v4.4.0	4.1.1 or later

1 SilkWorm 3016 is supported by Fabric OS v4.2.1x and v4.4.0 or later.
SilkWorm 3250, 3850, and 24000 are supported by Fabric OS v4.2.0 or later.
SilkWorm 3250, 3850, and 24000 are supported by Fabric Manager 4.1.1 or later.
SilkWorm 3900 is supported by Fabric OS v4.1.0 or later.

2 SilkWorm 4100 is supported by Fabric Manager 4.4.0 or later.

General

The major features incorporated in Fabric OS v4.4.0 are summarized in the following table.

Category	Feature	Release
SilkWorm 24000 Enhancements	Mixed-blade support for the SilkWorm 24000: ▪ Two-domain support ▪ Mixed SilkWorm 12000 and SilkWorm 24000 port blades	v4.4.0
SilkWorm 4100 Platform Support	Ports on Demand (16, 24, or 32 ports) Condor ASIC support: ▪ 1, 2 and 4 Gbit/sec automatic speed negotiation ▪ 4 Gbit/sec trunks ▪ 8-port trunk groups for up to 32 Gbit/sec trunks ▪ More distance options (see below) ▪ Dynamic path selection (DPS) with the exchange-based and device-based polices. The SilkWorm 4100 uses the frame information to determine the routing paths dynamically. Port-based policy is independent of the traffic pattern. ▪ Network boot using TFTP	v4.4.0
Reliability	Compact flash capacity monitoring	v4.4.0
Manageability	Advanced Performance Monitoring - ISL monitoring (CLI only) Fabric Watch enhancements Export performance data FDMI host name support	v3.2.0, v4.4.0 v3.2.0, v4.4.0 v3.2.0, v4.4.0 v4.4.0
RAS	New logging and tracing infrastructure Enhanced error message format **supportShow** command enhancements New **supportSave** command	v4.4.0 v4.4.0 v4.4.0 v4.4.0
Security-Related	RADIUS support Multiple user accounts SSL/HTTPS support SNMPv3 support DH-CHAP authentication (switch-switch) SAN gateway security	v3.2.0, v4.4.0 v3.2.0, v4.4.0 v4.4.0 v4.4.0 v3.2.0, v4.4.0 v3.2.0, v4.4.0

<table>
<tr><th>Category</th><th>Feature</th><th>Release</th></tr>
<tr><td>Long-Distance Enhancements</td><td>
200 km at 1 Gbit/sec or 100 km at 2 Gbit/sec (SilkWorm 3250, 3850, 24000, Bloom II ASIC-based switches)

500 km at 1 Gbit/sec, 250 km at 2 Gbit/sec, or 100 km at 4 Gbit/sec (SilkWorm 4100, Condor ASIC-based switches)

Trunking over Brocade Extended Fabrics (SilkWorm 3xxx, 12000, 24000, all Bloom ASIC-based platforms, with v4.4.0) is only supported at 2 Gbit/sec speed, as follows:

4 links at 10 km @ 2 Gbit/sec per trunk group
3 links at 25 km @ 2 Gbit/sec per trunk group
2 links at 50 km @ 2 Gbit/sec per trunk group

Buffer limited ports

Enhanced trunking support with the Bloom ASIC is summarized below:
<table>
<tr><th>Distance</th><th>Number of 2-Gbit/sec ports (Bloom to Bloom)</th></tr>
<tr><td>LE 10 km</td><td>4 (one 4-port trunk)</td></tr>
<tr><td>L0.5 25 km</td><td>3 (one 3-port trunk)</td></tr>
<tr><td>L1 50 km</td><td>1 (one 2-port trunk)</td></tr>
<tr><td>L2 100 km</td><td>0</td></tr>
<tr><td>LD 200 km</td><td>0</td></tr>
<tr><td>LD 250 km</td><td>0</td></tr>
<tr><td>LD 500 km</td><td>0</td></tr>
</table>
Enhanced trunking support with the Condor ASIC is summarized below:
<table>
<tr><th>Distance</th><th>Number of 2-Gbit/sec ports or trunks (Condor to Condor)</th><th>Number of 4-Gbit/sec ports (Condor to Condor)</th></tr>
<tr><td>LE 10 km</td><td>32 (four 8-port trunks)</td><td>32 (four 8-port trunks)</td></tr>
<tr><td>L0.5 25 km</td><td>32 (four 8-port trunks)</td><td>15 (one 8-port trunk)</td></tr>
<tr><td>L1 50 km</td><td>15 (one 8-port trunk)</td><td>7 (one 7-port trunk)</td></tr>
<tr><td>L2 100 km</td><td>7 (one 7-port trunk)</td><td>3 (one 3-port trunk)</td></tr>
<tr><td>LD 200 km</td><td>3 (one 3-port trunk)</td><td>0</td></tr>
<tr><td>LD 250 km</td><td>3 (one 3-port trunk)</td><td>0</td></tr>
<tr><td>LD 500 km</td><td>0</td><td>0</td></tr>
</table>
</td><td>
v4.4.0

v4.4.0

v4.4.0

v4.4.0
v4.4.0

v4.4.0
</td></tr>
</table>

Category	Feature	Release
MPRS Enhancements	Max hop count (SilkWorm Multiprotocol Router Model AP7420) – CLI only	v3.2.0, v4.4.0
	WAN_TOV (FC Router) – CLI only	v3.2.0, v4.4.0
Scalability	Supports 1280 total ports and 34 domains with or without security enabled.	v3.2.0, v4.4.0
	Supports 2560 total ports and 50 domains in a fabric consisting of switches with 32 ports or more running Fabric OS v4.4.0.	v4.4.0
Usability Improvements + RFEs	Security Management – enables/merges secure fabrics (Fabric Manager only)	v3.2.0, v4.4.0
	Web Tools and Fabric Manager usability improvements	v3.2.0, v4.4.0
	Enhanced Fabric Watch Support	v3.2.0, v4.4.0

Advanced Web Tools Updates

- For instructions on installing Mozilla 1.6 on Solaris 2.8 and Solaris 2.9, refer to the following Web site:

  http://ftp27f.newaol.com/pub/mozilla.org/mozilla/releases/mozilla1.6/README

- **Issue:** The Mozilla browser does not support the Switch Admin module properly in Fabric OS v2.6.x. In Fabric OS v2.6.2, a warning message is displayed. For other v2.6.x versions, no warning message is displayed.

  Workaround: Use Netscape 4.7.7 or later.

  The additionally supported browsers, operating systems, and Java Plug-ins introduce the following limitations when using mixed OS versions in Advanced Web Tools v4.4.0.

Launch Switch Environment	Problems
Firmware: Fabric OS v3.1+ or v4.1+ **Operating System**: any supported operating system (with supported browser) **Browser**: any supported browser (on supported operating system	**Issue**: When viewing the topology from WebTools, if your initial login was a v3.1+ or v4.1+ switch and you view the topology from a switch with a previous version of the Fabric OS, there is no print function available in the Fabric Topology window. Web Tools v3.1.0+ and v4.1.0+ includes a Print button in the Fabric Topology window. Earlier versions do not. **Workaround**: If the Fabric Topology window does not display a Print button, you can right-click anywhere inside the window and select Print from the popup menu.

Launch Switch Environment	Problems
Firmware: Fabric OS v2.6.x **Operating System:** Solaris **Browser:** Mozilla	**Issue**: The Switch Admin does not launch correctly. If you try to launch the Switch Admin using Fabric OS v2.6.2 on a Solaris operating system with a Mozilla browser, a warning dialog displays, telling you to use the Netscape browser. If you try to launch the Switch Admin using Fabric OS v2.6.1 or earlier on a Solaris operating system with a Mozilla browser, the Switch Admin fails and no warning is displayed. **Workaround**: Although the Netscape browser is not supported by Web Tools for switches running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later, if you must access the Switch Admin on a switch running Fabric OS v2.6.x from a Solaris operating system, use the Netscape 4.77 browser.
Firmware: version *prior* to Fabric OS v2.6.2, v3.1.2, or v4.2.0 with secure mode enabled **Operating System:** Solaris Browser: **Mozilla**	**Issue**: If you try to launch the Switch Admin, Zoning, Fabric Watch, or High Availability Admin using firmware versions prior to v2.6.2, v3.1.2, or v4.2.0 on a Solaris operating system with a Mozilla browser, the browser might crash due to a buffer overflow problem with Mozilla. **Workaround**: Although the Netscape browser is not supported by Web Tools for switches running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later, if you must access the Switch Admin, Zoning, Fabric Watch, or High Availability Admin on a switch running firmware versions prior to v2.6.2, v3.1.2, or v4.2.0 or later from a Solaris operating system, use the Netscape 4.77 browser.
Firmware: version *prior* to Fabric OS v2.6.2, v3.1.2, or v4.2.0 **Operating System:** any supported operating system (with supported browser) **Browser:** any supported browser (on supported operating system)	**Issue**: When trying to access a switch running firmware versions prior to Fabric OS v2.6.2, v3.1.2, or v4.2.0 from the launch switch, Switch Explorer will display a null pointer exception, and the SwitchInfo applet will not display; Switch Explorer does not work properly with switches running the latest firmware. **Workaround**: Use a launch switch running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later to access the switch.
Firmware: version *prior* to Fabric OS v4.4.0 **Operating System:** any supported operating system (with supported browser) **Browser**: any supported browser (on supported operating system)	**Issue:** When trying to perform end-to-end monitoring (Advanced Performance Monitoring) on a local switch with a Fabric OS prior to v4.4.0, the SilkWorm 4100 is displayed as a 16-port switch. **Workaround:** For a SilkWorm 4100, use a launch switch running Fabric OS v4.4.0 or later to perform end-to-end monitoring on the switch.

Launch Switch Environment	Problems
Firmware: version *prior* to Fabric OS v4.4.0 **Operating System:** any supported operating system (with supported browser) **Browser:** any supported browser (on supported operating system)	**Issue:** When trying to perform zoning on a local switch with a Fabric OS version prior to v4.4.0, the SilkWorm 4100 is displayed as a 16-port switch. **Workaround:** If you are running Brocade Secure Fabric OS, select a switch running Fabric OS v4.4.0 or later as the primary FCS switch. If you are not running Brocade Secure Fabric OS, use a launch switch running Fabric OS v4.4.0 or later to perform zoning on the switch.
Firmware: version *prior* to Fabric OS v2.6.2, v3.1.2, or v4.2.0 **Operating System:** Solaris **Browser:** Netscape	**Issue**: Any switches running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later are unsupported through Netscape. **Workaround**: The Netscape browser is not supported by Web Tools for switches running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later. Use the Mozilla browser v1.6 to manage all of your switches from a Solaris operating system.
Firmware: version *prior* to Fabric OS v2.6.1, v3.0.x, or v4.0.x **Operating System:** Windows **Browser:** Internet Explorer	**Issue**: When you are trying to run Fabric View with a large fabric, the browser might crash. **Workaround**: Use a launch switch that runs Fabric OS v2.6.1, v3.0.x, or v4.0.x or later so that you can use Switch Explorer (not Fabric View). Use a launch switch with v.2.6.2, v3.1.x, or v4.1.x and later.

Other Notes

This table lists other important information you should be aware of regarding Fabric OS v4.4.0 and the SilkWorm 3016, 3250, 3850, 3900, 4100, 12000, and 24000 platforms.

<table>
<tr><th>SilkWorm 4100</th><th>Description</th></tr>
<tr><td>SWL and LWL SFP module release mechanism</td><td>
SilkWorm 4100 uses an octal-style SFP cage that places SFPs in close proximity. As a result of the physical space limitation between the SFPs, Brocade requires the use of approved SFP modules only.

Using an approved SFP module eliminates issues associated with the fit and removal of the module. Specifically, SFPs with wide bail latch mechanisms that are not flush with the body of the SFP or SFPs with “push-tab” removal mechanisms might prevent the proper insertion or removal of the SFP module. Consult the Brocade compatibility matrix for the appropriate SFPs.

At the time of release, the following SFPs were certified compatible with the SilkWorm 4100 switch.
<table>
<tr><th>2 Gbit/sec Media</th><th>Type</th><th>Manufacturer</th><th>Manufacturer’s Part Number</th></tr>
<tr><td>SWL</td><td>Digital Diagnostics</td><td>Finisar</td><td>FTRJ-8519P1BCL-B1</td></tr>
<tr><td>LWL</td><td>Digital Diagnostics</td><td>Finisar</td><td>FTRJ-1319P1BCL-B1</td></tr>
<tr><th>4 Gbit/sec Media</th><th>Type</th><th>Manufacturer</th><th>Manufacturer’s Part Number</th></tr>
<tr><td>SWL</td><td>Digital Diagnostics</td><td>Finisar</td><td>FTRJ-8524P2-BNV (In Qualification)</td></tr>
</table>
</td></tr>
<tr><td>LED, system status</td><td>The system status LED blink behavior in the SilkWorm 4100 is different from that of legacy SilkWorm switches. Legacy products blink system status with amber/off, amber/off. The SilkWorm 4100 blinks amber/green, amber/green. Refer to the appropriate hardware specification.</td></tr>
<tr><td>LED, system power</td><td>The system power LED behaves differently in the SilkWorm 4100 than in SilkWorm 3250 and 3850 switches. In SilkWorm 3250 and 3850 switches, it is solid amber when a power supply FRU has failed. In SilkWorm 4100, the system power LED remains green, and the system status LED will blink, indicating an error.</td></tr>
<tr><td>Fan, RPM reading</td><td>The RPM range can differ by as much as 1000 RPM from fan to fan, which is within Brocade’s specification. At the lowest RPM, the cooling specification is met, and at the highest RPM, the acoustic specification is met. In other words, during normal operation, both the lowest and the highest observed fan speeds are within adequate margin of the acoustic and cooling specifications.</td></tr>
</table>

SilkWorm 4100	Description
WWN	Brocade has consumed the majority of WWN numbers originally allocated by the IEEE. This is due to the rate of switch shipments and the preallocation of World Wide Name (WWN) blocks to current and past switch products. The SilkWorm 4100 products use a new block of WWN numbers. In response, in addition to the current WWN, Brocade uses the IEEE Organizationally Unique Identifier (OUI) that was formally owned by Rhapsody Networks (now a part of Brocade Communications Systems, Inc.) for the new block of WWNs. The official IEEE OUI database has been updated to reflect this ownership change. Network and fabric management applications that rely on the use of the original Brocade OUI (00:60:69) to identify Brocade network elements must be updated from the IEEE Web site database (location below) to also include the new Brocade OUI (00:05:1E). **IEEE OUI and Company_id Assignments:** NEW 00-05-1E (hex) **Brocade** Communications Systems, Inc. 00051E (base 16) **Brocade** Communications Systems, Inc. 1745 Technology Drive San Jose CA 95110 UNITED STATES OLD 00-60-69 (hex) **BROCADE** COMMUNICATIONS SYSTEMS, Inc. 006069 (base 16) **BROCADE** COMMUNICATIONS SYSTEMS, Inc. 1901 GUADALUPE PKWY SAN JOSE CA 95131 UNITED STATES **IEEE list of public OUI assignments:** *http://standards.ieee.org/regauth/oui/index.shtml* In a management application using a Fabric Access version earlier than v3.0.2, SilkWorm 3250 and 3850 switches are displayed as Rhapsody switches.

SilkWorm 12000	Description
Power supply requirements	Customers reconfiguring SilkWorm 24000-only configurations by adding SilkWorm 12000 blade(s) will have to ensure that all three power supply FRUs are installed, as SilkWorm 12000 blades have greater power requirements.

Fabric OS Area	Description
Compatibility	Sometimes in a mixed fabric of Fabric OS v4.x/v3.x/v2.x, fabric reconfiguration is caused by link reset on v3.x/v2.x. This only happens in a fabric containing Fabric OS v3.x versions released prior to v3.1.0 or Fabric OS v2.x versions released prior to v2.6.1 that are under heavy traffic or CPU-intensive operations such as large (50 KB) zone database propagation. Use the latest revision of code across all releases in a mixed fabric.

Fabric OS Area	Description
Ethernet port IP addresses	When a SilkWorm 12000 or 24000 fails over to its standby CP for any reason, the IP addresses for the two logical switches move to that CP blade's Ethernet port. This might cause informational ARP address reassignment messages to appear on other switches in the fabric. This is normal behavior, because the association between the IP addresses and MAC addresses has changed.
FICON®	When deploying the SilkWorm 24000 director in FICON environments and planning to use CUP in-band management, port 126 should not be used for I/O. Due to the addressing of CUP management frames, I/O on an area 7E address is not supported simultaneously with CUP management. This constraint does not apply to the SilkWorm 3900 or 12000.
FICON®, mixed-blade support	SilkWorm 24000 two-domain and mixed-blade configurations are not supported for FICON. FICON is supported for SilkWorm 24000 single-domain environments only.
Firmware download	During a firmware download, rebooting or power cycling the CPs could corrupt the compact flash. **CAUTION:** Do not attempt to power off the CP board during firmware download, to avoid high risk of corrupting your flash**.**

Firmware download	Fabric OS v4.1.x, v4.2.x, and v4.4.x nondisruptive firmware download allows for firmware downgrades and upgrades; however, you might see warning messages such as the following:
	
	`0x239 (fabos): Switch: 0, Info PDM-NOTFOUND, 4, File not found`
	
	`(/etc/fabos/mii.0.cfg)`
	
	These warnings can be ignored.

Firmware download, boot ROM	The boot ROM in Fabric OS v4.4 is automatically upgraded, by firmware download, to version 4.5.0 in all v4.x switches. After it has upgraded, the boot ROM will not downgrade should a firmware downgrade be performed. This boot ROM version supports a redundant boot ROM capability and redundant boot environments in the SilkWorm 4100.
HA switch reboot failure	When a switch reboot or a failover occurs before POST is complete, the HA resynchronization is disrupted. HA will not resynchronize until POST completes. **CAUTION:** Allow POST to complete before performing a switch reboot or failover, to avoid disruptive failover**.**

Invalid gateway IP address error message	The user will see the following message on the console during startup when the Ethernet IP and gateway IP addresses are set to the defaults:
	
	`SIOCADDRT: Invalid argument`
	`.....`
	`ip.c:311:Invalid gateway IP address 0.0.0.0`
	
	This is a display issue only and does not affect the functionality of the switch.

IP addresses	CAUTION: Do not set a switch or CP IP address for the Ethernet interface to 0.0.0.0.
Logging, *syslog.conf*	As a result of multiple requests for enhancements, in Fabric OS v4.x, the "kern" facility for syslog is no longer supported. You must update all *syslog.conf* files to support "local7" facilities. There is a new syslogdFacility command to set the facility level that will be used.

Fabric OS Area	Description
Logging, Solaris syslogd local7 users	When using the new syslogdFacility command to set the local7 level, if an even-numbered facility level is selected (for example, 0, 2, 4 or 6), all Brocade switch Critical system messages will appear in the *odd*-numbered *.emerg* facility level file on the target Solaris systems: for example, *local6.emerg* will appear in *local7.emerg* if syslogd facility level 6 is selected. This behavior is not observed when selecting an odd-numbered facility level initially on the Brocade switch. The problem also does not occur on Linux server systems and is currently under investigation with Sun. The immediate workaround is to select an odd-numbered syslogd facility level when using the syslogdFacility command.
Logging, **supportFTP** command	When setting the automatic FTP IP address, userid, password, and associated directory path for use with the supportFtp command, the parameters are not checked immediately for validity. Generate a manual trace dump to confirm the FTP transfer immediately. First, use supportFtp to set up FTP parameters. Next, use traceFtp -e to enable automatic transfer of the trace dumps. Finally, use the traceDump -n command to create a dump. Confirm that the FTP transfer was successful.
Logging, **chassisName** command	Run the chassisName command before upgrading to Fabric OS v4.4 so that any subsequent error messages related to the chassis and switch services will be logged correctly to the system error log. For further information, refer to the *Brocade Fabric OS Procedures Guide.*
Logging, **errClea**r command	All error logs are persistent in Fabric OS v4.x, so the use of the errClear command must be carefully considered, as all persistent errors (all messages) will be erased on v4.4 switches as opposed to just those in local memory.
Ports on Demand	SilkWorm 4100 with a 16-port factory configuration requires Ports on Demand licenses in order to enable and use switch ports 16 thru 31.
rsh and rlogin	For Fabric OS v4.2.0 or later, programs rsh and rlogin are not supported. If you try to use an rsh or rlogin client, Fabric OS rejects the login attempt; however, because most rsh or rlogin clients continue to retry the login for several seconds before timing out, your system appears to hang. Secure connections are available via a secure shell (SSH).
Security, default password length	The initial login prompt for a switch accepts a maximum password length of eight characters. Any characters beyond the eighth are ignored.
Security, error counter	Telnet security errors that arrive in quick succession are recorded as a single violation by the telnet error counter. For example, a login error from a host whose IP address is 192.168.44.247 is logged as follows: `"Security violation: Login failure attempt via TELNET/SSH/RSH. IP Addr: 192.168.44.247"` If another login violation occurs immediately, the message remains the same and only the error counter is incremented.
Security, fabric segment	When two secure fabrics are continuously joined and separated while the CPU is under heavy load, the fabric will segment after approximately 30 cycles.
Security, FCS list	Adding switches to the FCS list does not automatically join the switches in a secure fabric. Add the switches to the FCS list of the new switches and the target fabric. Reset the version stamp to 0 and either reset the E_Ports or perform a switch disable and enable for the switches to join.

Fabric OS Area	Description
Security, HTTP policy	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, invalid certficate	Web Tools and Fabric OS are not consistent in how they report switch certificate status. Web Tools reports a valid certificate with extra characters appended to it as invalid, whereas Fabric OS accepts the certificate and allows a **secModeEnable** command to complete successfully.
Security, PKICERT utility, CSR syntax	Before using the PKICERT utility to prepare a certificate signing request (CSR), ensure that there are no spaces in the switch names of any switches in the fabric. The Web site that processes the CSRs and generates the digital certificates does not accept switch names containing spaces; any CSRs that do not conform to this requirement are rejected.
Security, PKICERT utility, installing certificates	PKICERT version 1.0.6 is the most current version of the PKICERT utility. When running the PKICERT utility to install switch certificates in a fabric that did not previously contain switch certificates and now includes a SilkWorm 24000 director, select the option to specify that certificates are installed on only those switches that do not currently contain certificates. SilkWorm 24000 directors are delivered with switch certificates preinstalled. Switches that were originally shipped with Fabric OS versions 2.5/3.0/4.0 and have never installed and enabled Secure Fabric OS do not have certificates installed. Should you need to reinstall switch certificates in a SilkWorm 24000 director, follow these guidelines: • The host running PKICERT 1.0.6 must be connected to a proxy switch running Fabric OS versions 2.6.2/3.1.2/4.2.0 or later. • All other non-SilkWorm 24000 switches in the fabric can run v2.6.1/v3.1/v4.1 or newer firmware.
Security, sectelnet	If you try to log in to a switch through a sectelnet client while that switch is in the process of either booting or shutting down, you might see the message, "Random number generation failed." The message is printed by the sectelnet client because the switch telnet service is not running (the service has either already been shut down, if the switch is shutting down, or is not yet established, if the switch is booting). If the switch is booting, wait a few seconds and try again.
Security, secure mode	If an upgrade from Fabric OS version 4.0.x to version 4.1.x/4.2.x is performed, followed by a downgrade to Fabric OS version 4.0.x and upgrade back to Fabric OS version 4.1.x/4.2.x, the switch password state is reset and will prompt the user for new secure-mode passwords. This does *not* apply to upgrades from v4.2 to v4.4.
Security, secure mode, passwd telnet	**CAUTION**: Using the "passwd" telnet command in secure mode to change the password results in all sessions using that password being logged out, including the session that changed the password. This is expected behavior. The session will terminate if you change the password in secure mode.
Security, SLAP fail counter and two switches	The SLAP counter is designed to work when all the switches in the fabric are in secure mode. All the switches in the fabric must be in secure mode for accurate SLAP statistics.

Fabric OS Area	Description
Security, SSH login	To properly connect SSH login, wait for secure mode to complete before rebooting or performing HA failover on the SilkWorm 12000 or 24000 directors. If secure mode is enabled and a reboot occurs before secure mode completes, SSH login will not connect and will go to the wrong MAC address because the active CP changes after an HA failover.
Support	Fabric OS v4.4 users should run the **supportSave** command instead of, or in addition to, the **supportShow** command. Doing so will gather additional switch details and FTP all files to a customer server. Refer to the *Brocade Fabric OS Procedures Guide* for instructions on setting up FTP services.
Trace dump	Fabric OS v4.4 users should set up automatic FTP trace dump transfers to customer FTP servers. Doing so will minimize trace dump overwrites. Refer to the *Brocade Fabric OS Procedures Guide* for instructions on setting up FTP services.
SilkWorm 12000 large fabric constraints	Under extreme stress-test conditions in a large fabric configuration (over 2000 ports), the SilkWorm 12000 platform could ASSERT or PANIC in extremely rare circumstances due to memory or processor limitations. Other SilkWorm platforms do not have these limitations. The stress-test cases that reveal these limitations on SilkWorm 12000 require all switches in a large fabric configuration to go through reboot, fastboot, or switch disable/enable repeatedly in quick succession over long periods of time. Subjected to these stress-test cases, the SilkWorm 12000 fails only rarely and only after long hours of testing. Under normal operating conditions, customers should not encounter these failures. Related defects: 48168, 49254
Upgrading to Fabric OS v4.4.0	Recommended upgrade procedures to Fabric OS v4.4 include the following: Before loading v4.4: • Run **configupload.** Creates a backup configuration, should the user want to return to v4.2. • Run **supportShow.** Captures the previous error logs in v4.2. • Run **chassisName.** Changes the default factory configuration to a more meaningful name. After loading Fabric OS v4.4, refer to "Logging, **supportFTP**," earlier in this table.
WWN card FRU repair	If an HA failover or power cycle occurs during a FRU replacement on the WWN card, the SilkWorm 12000 or 24000 director becomes nonoperational. **CAUTION**: When performing a FRU replacement on a WWN card, complete the FRU procedure before attempting an HA failover or power cycling the chassis.
Zoning	**Issue:** Domain 0 in a zoning configuration file is invalid but has not been previously enforced. **Workaround:** Prior to upgrading a switch to Fabric OS v4.2.0 or later, ensure that the fabric's zoning configuration does not contain domain ID 0, which is used for zoning. This is specific only to v4.x switches.

Fabric OS Area	Description
Zoning	When enabling a new zone configuration, the user must ensure that the size of the zone configuration does not exceed the minimum size supported by all the switches in the fabric. Zone configuration sizes can be determined by executing cfgsize on all the switches in the fabric.

Commands Modified in v4.4.0

supportSave

Under the **supportSave** command, in the "Description" section, replace this text:

"RASLOG *switchname-slot-YYYYMMDDHHMM-errDumpAll.ss*

TRACE *switchname-slot-YYYYMMDDHHMM-tracedump.dmp*

supportShow *switchname-slot-YYYYMMDDHHMM-supportShow* (saved in the specified remote directory)"

Add this text:

"RASLOG *chassisname-slot-YYYYMMDDHHMM-errDumpAll.ss*

TRACE *chassisname-slot-YYYYMMDDHHMM-tracedump.dmp*

supportShow *chassisname-slot-YYYYMMDDHHMM-supportShow* (saved in the specified remote directory)"

Documentation Updates

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

The most recent Fabric OS 4.4.0 documentation manuals are provided on the Brocade Website, through Brocade Connect.

SilkWorm 24000 Hardware Reference Manual

(Publication number 53-0000619-01)

Table 4-7 on page 4-15 within the "WWN Card" section in Chapter 4 needs to be revised. Replace Table 4-7 with the following:

Table 4-7. WWN Bezel LED Patterns

LED Location/Purpose	Color	Status	Recommend Action
16-port card/CP card power	Steady green	Power is okay.	No action required.
	Flashing green	Power to port card is okay; however, this LED flashes if the port card status LED is flashing.	Check port card status LED and determine if it is flashing slowly (2 second increments) or quickly (1/2 second increments); then take appropriate action.
	No light (LED is OFF)	No port card present or power source is unavailable.	Insert port card, or check AC switch or power source.
	NOTE: Check the individual port card (see Figure 4-1 on page 4-2) or CP card power LEDs (see Figure 4-2 on page 4-6) on the port side of the chassis to confirm the LED patterns.		
16-port card/CP card status	Steady amber	Port card is faulty.	Check port card.
	Slow-flashing amber (on 2 seconds, off 2 seconds)	Port card is not seated correctly or is faulty.	Pull card out and reseat it. If LED continues to flash, replace card.
	Fast-flashing amber (on 1/2 second, off 1/2 second)	Environmental range exceeded or port card failed diagnostics (run during POST or manually).	Check for out-of-bounds environmental range and correct it. Replace card if it fails diagnostics.
	No light (LED is OFF)	Port card is either healthy or does not have power.	Verify that the port card power LED is on.
	NOTE: Check the individual port card (see Figure 4-1 on page 4-2) or CP card status LEDs (see Figure 4-2 on page 4-6) on the port side of the chassis to confirm the LED patterns.		

Power supply/ power/status	Steady green	Power is okay.	No action required.
	Steady amber	Power supply is faulty.	Ensure that the correct AC power switch is on and the power supply is seated. If LED remains on, replace the power supply.
	Slow-flashing amber	FRU header (SEEPROM cannot be read) due to I2C problem.	Replace power supply.
	Fast-flashing amber	Power supply is about to fail due to failing fan inside the power supply.	Replace power supply.
	No light (LED is OFF)	No power supply present or is not inserted/seated properly, or power source is unavailable.	Insert power supply module, ensure it is seated properly, or check AC switch or power source.
	NOTE: Check the individual power supply LEDs on the port side of the chassis to confirm the LED patterns (see Figure 4-3 on page 4-9).		

NOTE: If a port card slot or power supply bay has a filler panel installed, the corresponding LEDs on the WWN card do not light up.

SilkWorm 3250/3850 Hardware Reference Manual

(Publication number 53-0000623-01)

Brocade Secure Fabric OS was omitted from the list of supported (optional) features for the SilkWorm 3250 and 3850 on page 1-5 of the *SilkWorm 3250/3850 Hardware Reference Manual*. The complete list should read:

"The SilkWorm 3250 and 3850 supports the following optional Brocade software, which can be activated with the purchase of the corresponding license key:

- Brocade Advanced Zoning
- Brocade ISL Trunking
- Brocade Fabric Watch
- Brocade Advanced Performance Monitoring
- Brocade Extended Fabrics
- Brocade Remote Switch
- Brocade Secure Fabric OS

For further information on any of these features, refer to the *Brocade Fabric OS Features Guide* or the *Brocade Secure Fabric OS User's Guide*."

Two tables within the "LED Patterns" section in Chapter 3 need to be revised. Replace Table 3-1 (and its table heading) on page 3-4 and Table 3-3 on page 3-6 with the following:

Table 3-1. System Power and Status LED Patterns During Normal Operation

LED Name (and Location)	LED Color	Hardware Status	Recommend Action
System Power (bottom LED to the right of the serial port)	No light	Switch is off or failure of both power supplies in SilkWorm 3850.	Verify system power.
	Steady green	Switch is on and power supplies are functioning properly.	No action required.
	Steady amber	One power supply failure in SilkWorm 3850.	No action required, but failure of the remaining power supply will cause the switch to fail.
System Status (top LED to the right of the serial port)	No light	Switch is off or failure of both power supplies in SilkWorm 3850.	Verify system power.
	Steady green	Switch is on and all ports are ready for use.	No action required.
	Steady amber	One or more ports are offline.	Verify switch has completed booting sequence and is not disabled. If LED remains amber, check error log and port status LEDs.
	Slow-flashing amber/green (amber 1 second, green 1 second)	At least one of the following is true: • One or more environmental ranges are exceeded. • Error log contains one or more port diagnostic error messages.	1. Check environmental conditions, error log, port status LEDs, transceivers, cables, and loopback plugs. 2. Correct error condition. 3. Clear error log. 4. Rerun diagnostics to verify error condition is fixed.

Table 3-3. Ethernet LED Patterns

LED Name and Location	LED Color	Hardware Status	Recommend Action
Ethernet speed (below port, on right)	No light	Port speed is 10 Mbits/sec,	No action required.
	Steady green	Port speed is 100 Mbits/sec.	No action required.

Ethernet link (below port, on left)	Steady amber	Link is valid.	No action required.
	Flashing amber (on ½ second, off ½ second)	Link has traffic.	No action required.

Brocade Fabric Watch User's Guide

(Publication number 53-0000524-05)

The following rows replace the existing rows "Invalid CRC Count," "Link Failure Count," and "State Changes" in Table A-6, "Port Class Threshold Defaults," on page A-6:

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Link Failure Count	Monitors the number of link failures	Unit: Error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Invalid CRC Count	Monitors the number of CRC errors	Unit: Error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
State Changes	Monitors state changes	Unit: Change(s) Time Base: minute Low:0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range

The following row replaces the existing row "State Changes" in Table A-7, "E_Port Class Threshold Defaults," on page A-9:

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
State Changes	Monitors state changes	Unit: Change(s) Time Base: minute Low:0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range

The following table replaces the existing Table A-8, “F/FL_Port Class Threshold Defaults,” on page A-10:

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Loss of Synchronization Count	Monitors the number of loss of synchronization errors	Unit: Error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Receive Performance	Monitors the receive rate, by percentage	Unit: Percentage(%) Time Base: minute Low: 0 High: 100 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative Informative
State Changes	Monitors state changes	Unit: Change(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Transmit Performance	Monitors the transmit rate, by percentage	Unit: Percentage(%) Time Base: minute Low: 0 High: 100 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative Informative
Invalid CRC Count	Monitors the number of CRC errors	Unit: Error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Invalid Transmission Word	Monitors the number of invalid words transmitted	Unit: Error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Link Failure Count	Monitors the number of link failures	Unit: Error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Loss of Signal Count	Monitors the number of signal loss errors	Unit: Error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Primitive Sequence Protocol Error	Monitors the number of primitive sequence errors	Unit: Error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range

The following row replaces the existing row “Flash” in Table A-9, “Resource Class Threshold Defaults,” on page A-11:

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Flash	Monitors the percentage of compact flash used	Unit: Percentage(s) Time Base: none Low:0 High: 85 Buffer: 0	Changed: 0 Below: 3 Above: 3 In-Between: 1	Informative Informative Out_of_range In_range

Open Defects for Fabric OS v4.4.0

The following table of newly open defects lists those defects that, while still formally "open," are unlikely to impede Brocade customers in their deployment of Fabric OS v4.4.0.

The presence of a defect in this list can be prompted by several different circumstances. For example, several of the defects were not detected in the months of testing on Fabric OS v4.4.0 but were initially reported against an earlier Fabric OS version in the field. Brocade's standard process in such cases is to open defects against the current release that *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 code changes or regression testing to ensure that the fix does not create new problems. Such fixes will appear in future releases.

None of these defects have the requisite combination of probability and severity to cause significant concern to Brocade customers.

This table lists defects that have been deferred to a release after Fabric OS v4.4.0.

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000045675	High	Summary: CP keeps rebooting (in a loop) because of a corrupted SEEROM Symptom: The CP reboots repeatedly with the following error message on the console: Switch: 0, Critical PLATFORM-SYSPCI_CFG, 1, pciSetUp Can't scan DrawBridge (-99). Solution: Unit's PCI Bridge SEEPROM (#2) was wiped out. Reprogrammed SEEPROM and CP boots up. Workaround: None Customer Impact: The symptom occurs because the SEEROM containing PCI configuration parameters is corrupted and therefore booting cannot proceed. The probability of occurrence is very remote. SEEPROM corruption recovery has been implemented in FOS4.4 for SilkWorm 4100. It will be extended to all platforms in a future release. Probability: Low Service Request# RQST00000030137 Reported in Release: V4.1.1

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000048168	High	Summary: Execute switch fastboot test overnight on a mix chassis 12/24k switch on FID2 caused switch to panic Symptom: During stess testing where switches are going through fastboot over night in a large fabric, on of the SilkWorm 12000 switches might hits a panic condition and reboots. The customer may see "EXCH 0: Out of exchanges!" messages before the panic. Workaround: None Customer Impact: This is a stress test scenario where all the switches are going through fastboot overnight in a large fabric and it is highly unlikely that a customer will run into this problem. The fabric is going through constant change when the switches are getting fastbooted and this eventually could lead to a switch not having enough resources for a very short duration to react to the large magnitude of changes in the fabric. The problem is specific to Silkworm 12000 due to the limited memory available in the system. Reported in Release: V4.4.0
DEFECT000048895	High	Summary: (Scal - FCR) ASSERT - bad route class followed by kernel panic after switchdisable/enable overnight script Symptom: In large configurations (this case being 77 domains), if the customer is enabling and disabling repeatedly, the customer may see the switch panic. Workaround: Do not put SilkWorm 24000 switch into repetitive disable/enable loop. Customer Impact: The impact to the customer is restricted to two well-defined scenarios. 1) If the user makes an ISL, assigns it to a domain, adds routes, and then forces it to be down. In that situation if the customer then attempts to take the ISL down through normal means, the problem manifests. 2) If the user sets up an ISL with paths and routes, forces the ISL to be a slave pointing to itself, then sends the DOWN attempt, the problem will manifest as it tries to update routing statistics. Probability: Low Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000049088	High	Summary: Disabling zoning in a large fabric caused NSd to core dump Symptom: In a very large fabric environment (1280+ ports), while disabling zoning at the same time as HBAs are rebooting, a core dump and subsequent HA failover may occur after several hours. Workaround: It is recommended that customers do not disable zoning in large fabric environments (1280+ ports) Customer Impact: It is unlikely that customers will run with zoning disabled in large fabrics. Therefore the impact of this issue to the customer should be minimal. Reported in Release: V4.4.0
DEFECT000049090	High	Summary: Scal-FCR:Buffer Tag Mismatch leads to a slot being disabled on a 24K switch in large fabric. Symptom: The symptom has only been seen once. In a large configuration consisting of 30 fabrics interconnected by a FC Router, one of the slots in a SilkWorm 24000 switch is faulted. The slot needs to be enabled by performing Slot Power Off/On. Workaround: The faulted slot can be recovered by performing slotpoweroff/slotpoweron. Customer Impact: This symptom has only been seen once. It was seen on a SilkWorm 24000 in a large configuration consisting of a FC Router connecting 30 fabrics together. Two of the fabrics in the configuration are large 1280 port fabrics. It is highly unlikely that this problem will be seen since multiple sequences need to happen in a very small timing window. Probability: Low Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000049148	High	Summary: In a FICON environment, host/targets initialization intermittently fails to complete correctly after a zoning change Symptom: Port activity fails to start automatically after a port entry is removed and then added back into the zoning configuration. This occurs only in a FICON environment. Workaround: Vary the channel path to the device(s) online at the host operating system console or disable and then enable the failing port. Customer Impact: This failure is very intermittent and has only been observed with an Enterprise Server running FICON traffic in a cascaded configuration where the host and target are on different switches. Probability: Low Reported in Release: V4.4.0
DEFECT000049945	High	Summary: Silkworm 24000 cannot propagation zoning with AP switch in the fabric and failover overnight stress test. Symptom: For fabric configurations that have a Router in the fabric, executing an enable/disable of zoning (cfgenable/cfgdisable) from a 24K switch, does not propagate the zoning configuration to all switches. Solution: In a mixed fabric that does not support RCS, Silkworm 24000 will revert back to use non-RCS way to propagate the new zone cfg. If a failover happens before zoning receives the SW_ONLINE SCN, then during warm recovery, zone uses a cached flag to determine switch state. The cached flag says the switch is offline even though the switch is already online. The fix is not to use the cached flag under this condition. Customer Impact: To work around this issue, the customer can simply do a "switchdisable; switchenable" to clear zoning's cached flag. This is a very corner case. Reported in Release: V4.2.2
DEFECT000049983	High	Summary: Boot PROM parameters changed after booting into single user mode Symptom: After booting the switch into single user mode to recover root password, the boot prom changes most of its environment variables in such a way that the switch will only boot into single user mode until the parameters are changed manually. Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000020413	Medium	Summary: Trackchanges indicates "successful login" even if user is rejected. Symptom: If the maximum # of users has been reached, and a user attempts to login with correct username and password, the user will be rejected for exceeding maximum number of users, however, trackchanges will indicate "successful login" Workaround: None Customer Impact: The user will receive an incorrect track-changes notification of "successful login" instead of "unsuccessful login". This problem happens only when a login attempt is rejected after maximum number of users has been exceeded. Reported in Release: V4.1.0
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. Reported in Release: V4.1.0
DEFECT000025559	Medium	Summary: Change IP address while HA not in sync, after HA in sync, new IP is not copied over to Standby CP Symptom: While HA is not in sync, change the IP address of one switch, and wait until HA state is in sync, the new IP setting is not automatically copied over to the standby CP. Workaround: Do haSyncStop and haSyncStart to sync up the data from the active cp to the standby again. Customer Impact: The customer impact is minimal. Customers are not expected to have to change IP address in the middle of an HA failover (i.e., while HA is not in sync.) In the event that the customer symptom occurs, the workaround can be used to synchronize the data. Probability: Low Reported in Release: V4.1.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000033228	Medium	Summary: Cfgdisable command (turning off zone enforcement) in a large fabric can be very disruptive. Symptom: The 'cfgdisable' command turns off zone enforcement which generates a lot of fabric activity and is likely to be very disruptive to devices in a large fabric. Workaround: During cfgDisable, all devices have access to each other. On a big fabric with many devices, doing a cfgDisable will cause lots of RSCN and queries which can be disruptive. The workaround for this is to enable a dummy cfg instead of cfgDisable. This will disable access among the unzoned devices. Customer Impact: Turning off zone enforcement ('cfgdisable' command) is not recommended in large fabrics. Service Request# RQST00000024244 Reported in Release: V4.1.1
DEFECT000033899	Medium	Summary: API: During configurationDownload from API, when the "reboot allow" parameter is turned TRUE, it reboots the SW12000 CP rather than SW12000 switch. Symptom: The customer who uses API to download configuration and specifies the "reboot allow" parameter as TRUE will see a reboot of the SW12000 CP instead of the SW12000 switch. Workaround: None. Customer Impact: This issue impacts customers who use API to download configuration to the switch and turn on the "reboot allow" parameter to TRUE. The active CP will get rebooted and the standby CP will take over. Therefore, the impact to customer will be minimal. Probability: Low Reported in Release: V4.1.1

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000035584	Medium	Summary: loss of sync timer too short Symptom: In DWDM environment, a DWDM failover in the gateway devices can cause ports to go offline and cause fabric reconfiguration. The ports that go offline are the ones directly connected to DWDM equipment that failed over. Workaround: None. Customer Impact: The symptom will occur only if the DWDM equipment has a failover. Only the ports on the switch that are directly connected to the DWDM equipment will get affected. It is expected that this is an infrequent occurrence in a DWDM network. Reported in Release: V4.1.0
DEFECT000037089	Medium	Summary: Temporary internet files may allow user to bypass Web Tools login to perform administrative functions on a switch. Symptom: If an administrator leaves his/her terminal unlocked, someone else can use the temporary internet files on the system to bypass Web Tools login and perform administrative functions on a switch. Workaround: Do not leave the terminal unlocked or purge temporary internet files before leaving the terminal unlocked. Customer Impact: This situation happens only if an admin leaves his/her terminal unlocked and the user looks into the temporary internet files. There is a 2 hour window in which this can happen. The defect is under investigation and a fix is targeted for a future release. Reported in Release: V4.2.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000037370	Medium	Summary: SEC: Fail to ping or telnet to SilkWorm 12000 from management server Symptom: SEC: Fail to ping or telnet to SilkWorm 12000 from management server Workaround: The problem here is that the gateway address for the CP is being cleared to 0 when the switch IP address is being set. The workaround is to have the user always set the IP and gateway address for the CP (via the ipAddrSet command) after making any change to the switch IP address. Customer Impact: The problem here is that the gateway address for the CP is being cleared to 0 when the switch IP address is being set. The workaround is to have the user always set the IP and gateway address for the CP (via the ipAddrSet command) after making any change to the switch IP address. Probability: Medium Reported in Release: V4.2.0
DEFECT000044290	Medium	Summary: CP fail to boot with no Boot Environmentals Symptom: The output of PRINTENV shows that all BOOTENV variables are missing. Solution: We have made the bootenv redundant and at every point it is accessed, made certain that iny failed record will be restored from the other. Workaround: The user can manually enter BOOTENV variables from the prom boot level. Customer Impact: The symptom can happen when an update to bootprom is interrupted. It can also happen by other random events at much lower frequency. Bootenv Redundancy can mitigate this condition. It has been implemented on SilkWorm 4100. Bootenv Redundancy will be implemented on other SilkWorm platforms in a future release fo FOS. Probability: Low Reported in Release: V4.1.2

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000045488	Medium	Summary: Help pages for msTd* commands need to be standardized. Symptom: Help pages are not consistent between platforms. Workaround: None Customer Impact: Customer must rely on the help pages specific to the platform they are working with. Reported in Release: V4.4.0
DEFECT000046367	Medium	Summary: One of the E-ports comes up in "unknown" state after multiple iterations of severe fault injections Symptom: In the unlikely case that a customer sees the problem, the visible symptom will be that, one of the E-Ports will not come up completely. All the other ports of the switch will function as expected. The switchshow will show that E-Port as in an "unknown" state: "0 1 0 id N2 Online E-Port (unknown)". This port will loose ISL connectivity to the other end. Workaround: Once the E-port gets into the Unknown state, the user can perform portdisable followed by portenable to return the E-port back to normal state. Customer Impact: The test case that revealed the symptom is described as follows. On the Silkworm 24000, all the slots with ports connected are disabled and enabled in quick succession and after 1 sec of enabling the ports, hafailover is induced to failover to the other CP. This is repeated over a long period of time and in one of the instances, the E-Port comes up as unknown. The proper sequence of faults need to be introduced to get the E-Port in this failed state. Also, at this time there is no data flowing through the switches since the ports are just being enabled. It is highly unlikely that a system will get in to this state even under adverse conditions. Therefore, the impact to customer is minimal. Probability: Low Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000046395	Medium	Summary: It took almost 10 minutes to change switch IP with ipaddrset Symptom: Telnet sessions will freeze up when ipaddrset CLI command is executed. Workaround: Two possible workarounds: 1) Shutdown all but 1 telnet session. Issue ipaddrset through that telnet session. It will freeze for several minutes, but others will be available. 2) Shutdown all telnet sessions and issue ipaddrset through serial port. Customer Impact: Telnet sessions will freeze up when ipaddrset CLI command is executed. The customer can still telnet into the switch using the new IP address if the maximum number of telnet sessions has not been reached previosuly. Reported in Release: V4.4.0
DEFECT000046637	Medium	Summary: Simple "typo" in supportftp can cause errorlog flood due to FTP transfer errors Symptom: If a customer sets up an incorrect FTP address (e.g., host ip) for auto-FTP transfer, then when a tracedump occur, the FTP facilities will continue to retry indefinitely and overload the system error log with messages causing important customer messages to be erased due to limited buffer size. Workaround: Do not make a mistake with the ftp address. Customer Impact: When setting the automatic FTP IP address, userid, password and associated directory path for use with the supportftp command, the parameters are not checked immediately for validity. It is recommended that a manual trace dump be generated and the FTP transfer confirmed immediately. First, use supportftp to set up FTP parameters. Next, use traceftp -e to enable automatic transfer of the trace dumps. Finally, use the tracedump -n command to create a dump. Confirm that the FTP transfer was successful. Probability: Low Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000046910	Medium	Summary: (Scalability) secfabricshow takes a long time (20+ seconds) to complete for a single switch Symptom: The secfabricshow command may take over 20 seconds to complete in a large fabric (50 domains). Workaround: The state of a secure fabric may be verified by executing the secfabricshow command on the Primary FCS switch only. It is not necessary to execute the secfabricshow command on every switch in the fabric. Customer Impact: The secfabricshow command may take upwards of 17 seconds to complete in fabrics approaching 50 switches. Reported in Release: V4.4.0
DEFECT000047411	Medium	Summary: Changing from 1 domain to 2 domains on 24000 in secure mode will leave logical switch 1 in secure mode Symptom: When changing from 1 domain to 2 domain on 24000 in secure mode, Switch 1 could be left in secure mode. Workaround: Customer would need to do chassisconfig back to option1 (which will delete switch 1 information) then back to option2 (or 3 or 4). Refer to procedures guide for detailed procedure. Customer Impact: This symptom will occur only under extremely rare circumstances. It would occur only if a customer repeatedly convert a system back and off between 1 domain and 2 domain and at the same time performing firmware download in between the 1 domain/2 domain conversions. Given the workaround and the unlikely exact sequences that need to happen in order for the symptom to occur, the customer impact is minimal. Probability: Low Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000047590	Medium	Summary: Switch status should set to faulty if the only slot on a single slot system is faulted Symptom: When the SilkWorm 3016 (blazer) slot is faulty, the switch overall status is still Healthy/OK although third party management software did notice it's faulty. Solution: Set switch status to faulty if there is only one slot on the switch and that slot is faulted. When a slot is faulted, system control module in kernel will be notified. If it's a single slot system, system control module will set switch status flags into faulty. Upper layer management application can pull the correct status. Workaround: No workaround. Customer Impact: The overall switch status did not display to faulty when the blade in a single slot system is faulted. The original defect that makes the slot faulty has been fixed. This fix will make management tool to show the switch as faulty. The impact is upper layer management tool will not notify user when the slot is faulted. Service Request# RQST00000031112 Reported in Release: V4.2.1
DEFECT000047597	Medium	Summary: Remove/Replace Offline Device wizard does not show Offline Fabric Assist(FA) Host device(s). Symptom: Remove/Replace Offline Device wizard does not show Offline Fabric Assist(FA) Host device(s). Workaround: Do not remove/replace offline Fabric Assist(FA) host devices using the remove/replace offline device wizard. Changes can always be made to the zone members using regular zoning applet. Customer Impact: Customer impact is very minor. Only sites using Fabric Assist(FA) hosts get affected. The only impact is that for offline FA host devices, you have to use the regular zoning applet to modify zone members. Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000047805	Medium	Summary: Must Include Port No. when FM Event Log shows Marginal Port Warning from Fabric Watch Symptom: Customer sees Fabric Watch warning messages in the event logs about Marginal Port(s) without any idea which port(s) is marginal to correct the problem. Workaround: Customer needs to look back at the event log history for any port related error logs. May require debugging the problem using portlogdump or supportshow. Customer Impact: The impact to the customer is that they are given warnings but no easy way to correlate them to the actual port number. Probability: Low Reported in Release: V4.3.0
DEFECT000047815	Medium	Summary: Commands that display physical "user-port" number needs to be updated to display the "area" number Symptom: After changing the PID format to 2, the Area number of a port is shifted by sixteen bits, but it does not get reflected in the "islshow" command executed from other switches in the fabric. Executing the "islshow" command on the Silkworm 24000 itself also does not show the new Area number of the port properly. Workaround: The workaround is to use the logical port number displayed in the "islShow" command output to compute the area number (Area_number = Logical_port_number + 16 when PID format is set to 2 (i.e. Displaced PID format)) and use the area code to get the physical slot and port numbers from the "switchShow" output. Customer Impact: There is no operational impact other than the misleading output of the "islShow" command when using PID format 2. Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000047966	Medium	Summary: Removing SW24k's active CP without following deinstall procedure and inserting it back cause a kernel panic and reboot of the standby CP Symptom: Removing SW24k's active CP and inserting it back cause a kernel panic and reboot of the standby CP Workaround: Most likely the reboot on the standby CP as well as the cold boot of the previously active CP that happens as a result of this defect should already bring up all the port blades and the CP's up. If there is a FAULTY port blade: A slotpoweroff and slotpoweron on that particular port blade should fix this. If either of the CP's comes up as FAULTY, turn off the microswitch of that particular CP, wait for the LED to go OFF and then try reseating the CP and then power it on. Customer Impact: No customer impact if the documented de-install procedure is followed. Reported in Release: V4.4.0
DEFECT000047968	Medium	Summary: Simultaneously inserting a SW24k port blade and insertion of the Active CP that was pulled out before the LED is turned OFF causes the port blade to be reported as FAULTY. Symptom: Simultaneously inserting a SW24k port blade and insertion of the Active CP that was pulled out before the LED is turned OFF causes the port blade to be reported as FAULTY. Workaround: The following should fix the FAULTY condition slotpoweroff 10 slotpoweron 10 Customer Impact: This action is an intentional test of the effects of not following the prescribed installation/uninstallation procedure. The likelihood of this sequence of actions taking place in the customer environment is extremely remote. Probability: Low Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000047994	Medium	Summary: SNMPv3 clients are not able to receive SNMP V3 traps after rebooting the switch unless USM entries are deleted and recreated at the SNMPv3 clients. SNMP V1 clients work fine. Symptom: User will configure the SNMPv3 USM entries at the client, which match the entries on the switch. But, after rebooting the switch, the SNMP V3 client (using these USM entries) will time out trying to access the switch. It also will not receive any SNMP V3 traps from the switch. Workaround: After reboot, user needs to delete the USM entry from the MIB browser and recreate it and all the functionality works fine. Customer Impact: After reboot, user needs to delete the existing USM entry and recreate it again. With this the problem will be solved. Access using SNMP V1 and receiving traps using SNMP V1 work fine. Reported in Release: V4.4.0
DEFECT000048049	Medium	Summary: Route was not set up for an F-Port after issuing switchcfgspeed 2/0 on a single domain SW24000 Symptom: Sometimes an F-Port was ignored and not assigned to any routing path after command switchcfgspeed had been issued to change speed for all ports on a Silkworm 24000; however, issuing portdisable and portenable can recover the route path for the F-Port. There is no customer-visible utility that detects this condition. The customer will first suspect a problem due to I/O timeouts involving the affected port. Workaround: The customer can issue the portdisable and portenable command which will recover the route path for the F-port. Customer Impact: Sometimes an F-Port was ignored and not assigned to any routing path after command switchcfgspeed had been issued to change speed for all ports on a Silkworm 24000. Note that there is no impact to the portcfgspeed command. Customer needs to portdisable/portenable the port in question to restore routing. Probability: Low Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000048070	Medium	Summary: Executing the fastboot command repeatedly causing a 4-port trunk between a SW24000 and a SW12000 to split off into 2 trunks - a 3-port trunk and a single port trunk. Symptom: After multiple iterations of fastboot on SW24000, a 4-port trunk between a SW24000 and a SW12000 may be split into 2 trunks - a 3-port trunk and a single port trunk. Workaround: If the trunk is formed incorrectly, port disable and port enable will reform the expected trunk. Customer Impact: The only visible impact is that after fastboot, a 4 port trunk may be split into 2 trunks, a 3 port and 1 port. There is no loss of connectivity between intiators and targets and the fabric is formed with a 4-port trunk split into 2 trunks. This is a stress test that runs over many iterations, and the problem is very difficult to reproduce. Therefore the customer impact is minimal. Probability: Low Reported in Release: V4.4.0
DEFECT000048123	Medium	Summary: Run multiple third party applications using multiple proxy switches, some web page can no longer to retrieved with RTWR transmit errors. Symptom: In this environment, end user has multiple fabman, and other third party application running in this fabric, after sometime, Webtool can no longer retrieve nsinfo.htm and also zoning information while underneath traffic is running fine . Disable some of the application relieve the situation but does not complete recover. Workaround: Use single proxy switch rather than multiple proxy switches to avoid this situation. Or to reduce the number of concurrent third party applications running on the fabric Customer Impact: This will happen if multiple concurrent applications run in the fabric with multiple proxy switches. In this case, reduce proxy switches to a single switch can avoid the problem. The fix need re-architect management server which is planned for a future release. Service Request# RQST00000031531 Reported in Release: V4.2.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000048173	Medium	Summary: Continuous "[EM-1029], 7241,, ERROR, Silkworm3900, PS 2 I2C access problems (-4): state 40" Message When there is a faulty power supply that gives continuous 'removal' and 'insertion' symptoms. Symptom: When there is a faulty power supply that fails in this particular way, the customer will get the following error/info messages continuously: [EM-1029], 7241,, ERROR, Silkworm3900, PS 2 I2C access problems (-4): state 40 [EM-1050], 10261,, INFO, Silkworm3900, FRU PS 2 removal detected. [EM-1049], 10262,, INFO, Silkworm3900, FRU PS 2 insertion detected. Workaround: Replace the faulty power supply. Customer Impact: The current implementation is that the error logging does happen very often. In this scenario, the customer impact is that the error log will be predominantly filled with the error message about the bad/flakey power supply. Probability: Low Reported in Release: V4.4.0
DEFECT000048198	Medium	Summary: When querying USM MIB, the index on the USM MIB is changed to CP IP address instead of the switch IP address. Symptom: snmpEngineID (and thus usmUserEngineID) will be based on CP IP address and not switch IP address. For non-bladed switches CP IP address and switch IP address are the same and hence this is not an issue. Only for bladed switches configured in dual-domain mode, same snmpEngineID will be used for both logical switches. Workaround: No workaround exists at this time. For non-bladed switches, such as 4100 etc., this is not an issue. Only for bladed switches, such as 12000 and 24000, same snmpEngineID will be used for both logical switches. Customer Impact: The snmpEngineID may be used by some SNMPv3 clients (or managers) to identify SNMP agents. Other SNMPv3 agent related variables, such as, snmpEngineBoots and snmpEngineTime, may be tied to snmpEngineID. And thus, having the same snmpEngineID for both the logical switches on a bladed system can cause confusion at the SNMPv3 client side. However, this problem will be there only for bladed systems configured in the dual-domain mode. For non-bladed systems and bladed-system configured in a single-domain mode, unique snmpEngineID will be used for each SNMP agent. Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000048299	Medium	Summary: When Web Tools is launched from a 2.x system which is in a fabric with a Blazer (blade for IBM Blade Center), a vertical Blazer icon is shown but the switch information shown below it is cut off. Symptom: When webtools is launched from a v2.6.1 or earlier FOS switch, the embedded switch will not display this information (ethernet netmask, FCip, FCip Netmask, Gateway, and switch wwn) Workaround: Double clicking the Blazer icon will bring up Switch View of the Blazer. All Blazer information is available in this view. Customer Impact: Minimal impact since Brocade recommends customers to launch webtools from a switch with later FOS version. If the customer doesn't have later version of FOS in their fabric, they can get this information by selecting the embedded switch and clicking on the info button. Reported in Release: V4.2.1
DEFECT000048341	Medium	Summary: SwitchAdmin Switch Tab does not display chassis name. Symptom: The Switch Tab under WebTools SwitchAdmin does not display chassisname as an editable field. This is important in v4.4 since a distinction is now made between chassis events and switch events. Workaround: Use FOS chassisname command to view and change the chassis name. Customer Impact: Works as before. Users can make the change from the CLI. Reported in Release: V4.4.0
DEFECT000048408	Medium	Summary: FOS4.2.x Environment Variables are not correctly set up. Symptom: "MACHTYPE", "HOSTTYPE" and "OSTYPE" clearly reference a "sparc-sun-solaris 2.8" environment instead of a "powerpc-linux" environment as it should. Customer Impact: Terminal sessions will not page correctly when executing the help command and when the terminal window is larger than 24x80. Service Request# RQST00000031688 Reported in Release: V4.2.2

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000048595	Medium	Summary: The swEventRepeatCount variables show the event count as "1" for all the events, despite some events repeated. Also, some non-repeated event numbers are missing on SNMP query on Silkworm 4100 and 12K. Symptom: Some of the error log entries are skipped when swEventTable and connUnitEventTable are queried. Also, for the missed entries, no swEventTrap and connUnitEventTrap will be sent. Workaround: There is no workaround for this problem. Customer Impact: The problem happens very rarely and is hard to reproduce. Even when it happens, only a few entries are missed. What we have seen is that out of 1000 entries 2-3 have been missed. Reported in Release: V4.4.0
DEFECT000048618	Medium	Summary: Delayed RSCN from switch when FCP probing failed. Symptom: Customer will notice that the RSCN will be delayed, say up to a few seconds after FLOGI happened on a port. Workaround: none. Customer Impact: This target will not be listed in the Name Server database (and so hosts will not discover those targets) until the RSCN is generated. Service Request# RQST00000031207 Reported in Release: V4.4.0
DEFECT000048635	Medium	Summary: WT doesn't display port diagnostic LED status after the user installs a 2-domain/4-domain license. Symptom: When a 4-domain license is installed on a switch and the fabric size is larger than 4 switches, the port diagnostic LED on each would display blinking amber on the physical switch. On Webtools, the port diagnostic LED is shown as off. Webtools will constantly pop up another window message to inform the user their fabric size exceed the 4-switch limit. Workaround: There is no workaround required since the user is nagged periodically to indicate that the fabric size has exceeded the limit. Customer Impact: Webtool display does not match the physical switch status. However, another pop-up window will remind them that their fabric size has exceeded the 4-switch limit. Reported in Release: V4.2.1

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000048657	Medium	Summary: CLI user not logged off when account disabled from WT user admin, and can re-enable the account. Symptom: CLI user not logged off when account disabled from WT user admin, and admn user can can re-enable the account. Also, admin and user account sessions not logged off when password changed from WT, or even when accounts are removed, and admin user can recreate the account from orphaned CLI session. Workaround: Use only CLI for disabling user accounts in non-Secure fabric. Customer Impact: Disabling an account using WT does not log off existing CLI sessions. If the disabled account user has an active CLI session at that moment, the account can be re-enabled. Reported in Release: V4.4.0
DEFECT000048666	Medium	Summary: "chassisname" command interface needs some clean up on error syntax Symptom: The user interface for handling incorrect string lengths needs to be improved. The switchname command could also use some improvement in notifying customers on error conditions seen with illegal characters and supplied string length. Workaround: None required when command is used as specified. Customer Impact: When incorrect information is entered (illegal number of characters, etc), the error handling is not as helpful as it could be. When correct information is entered, there is no customer impact. Reported in Release: V4.4.0
DEFECT000048672	Medium	Summary: Device Name field in Web Tools Name Server display is not populated for devices not directly connected to the launch switch. Symptom: For devices that are not directly connected to the launch switch, the Device Name field in the name server table is empty. Workaround: If you want to find out the symbolic node name for devices connected to a particular switch, launch Web Tools directly from that switch. Customer Impact: Some inconvenience in reading the device table and identifying devices. The workaround allows the customers to view the missing information. Service Request# RQST00000031386 Reported in Release: V4.2.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000048673	Medium	Summary: After 166 iterations of performing the sequence of switchdisable, switchenable and CP failover (by resetting the microswitch), slot 8 became FAULTY (21) Symptom: After multiple iterations of performing switchdisable, switchenable and CP failover (by resetting the microswitch), a slot may become FAULTY Workaround: None Customer Impact: The sequence of events for this defect to occur is very complicated. After > ~ 150 iterations on stress test which includes switchdisable/switchenable/CP failover (by resetting the microswitch), one of slots get faulted. It is highly unlikely for a customer system to go through even a few iterations of this sequence of events. Probability: Low Reported in Release: V4.4.0
DEFECT000048752	Medium	Summary: Firmwaredownload -s, without a reboot, followed by a firmwaredownload which gets interrupted, causes badrootdev. Symptom: In rare cases, the system could get into a situation where the FWDL code would timeout while updating one of the partitions. On reboot, the attempt to repair the situation would fail and the system could no longer be updated without modification of the bootENV's. Workaround: The problem can be resolved by running the root command "bootenv -u BadRootDev" at the FOS command prompt and rebooting the system. Customer Impact: If a customer were able to reproduce this scenario, the FWDL code would timeout during an installation and leave a partition in a bad state. On reboot, FWDL would be unable to repair the partition. Probability: Low Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000048785	Medium	Summary: Alert message, displayed after removing Performance Monitoring License and attempting to load a saved graph, does not report reason for failure as a missing License. Symptom: The alert message, displayed by WebTools after removing the Performance Monitoring License and loading a saved graph, does not report the reason for failure as a Missing License. Workaround: If you remove Performance Monitor license, please make sure that you do not access performance monitor functionality in Web Tools. Customer Impact: Customer impact is very minor since a customer that removes Performance Monitor license is not going to use Performance Monitor features. Reported in Release: V4.4.0
DEFECT000048855	Medium	Summary: In Windows IE, after clicking on a switch that does not have the web server running, a click on any switch that has web server running does not open switchview for this switch Symptom: In Windows IE environment, after clicking on a switch that does not have the web server running and following it up with a click on any other switch in the fabric does not produce a switch view. Workaround: Use Mozilla to bring up web subsystem on the switch where the web server is not running or avoid clicking such a switch in the fabric tree view. Customer Impact: Once the customer runs into this problem, the customer has to bring up the web subsystem on the switch where it is not running. Reported in Release: V4.4.0
DEFECT000048924	Medium	Summary: After a switch reboots, the fabric tree node collapses with each poll. Symptom: After a switch reboots, the fabric tree collapses with each poll even though there are switches in the fabric. Workaround: Click on the collapsed node when you want to see the fabric members. Otherwise, restart Web Tools. Customer Impact: Some annoyance because the node keeps collapsing every polling period. Service Request# RQST00000031913 Reported in Release: V4.2.2

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000048968	Medium	Summary: Continuous removal and insertion of a SW24K's Standby CP before the LED turns OFF, caused I/O disruption on all the ports connected to devices. Symptom: Continuous removal and insertion of a SW24K's Standby CP before the LED turns OFF, caused I/O disruption on all the ports connected to devices. The time interval between powering off the 24K CP's ON/OFF switch and removal of the CP is 1 second This is a test for SW24K CP removal and insertion that DOES NOT follow the SW24K CP installation/replacement procedures. Workaround: Follow the SW24k CP installlation/replacement procedures. Customer Impact: I/O will be disrupted on all the ports Reported in Release: V4.4.0
DEFECT000048974	Medium	Summary: Removed the SW24k Standby CP quickly w/o re-inserting the blade, and 2 critical errors seen: 1) [BLL-1000], 1417,, CRITICAL, ?, ASIC driver detected Slot 5 port 47 as faulty (reason: 11) ; 2) [BL-1003], 1418,, CRITICAL, ?, Faulting blade in slot 5. Symptom: When a SW24k's standby CP is removed before the power LED goes out and with POST disabled, two critical errors are seen: 1) [BLL-1000], 1417, CRITICAL, ?, ASIC driver detected Slot 5 port 47 as faulty (reason: 11) ; 2) [BL-1003], 1418,, CRITICAL, ?, Faulting blade in slot 5. The time interval between dropping teh slider and blade removal is <1 second. This is a test for SW24k CP removal and insertion that does not follow the SW24k CP installation/replacement procedures. Workaround: Follow the SW24k CP installation/replacement procedures. Customer Impact: There is no customer impact if SW24K CP Installation/replacement procedure is followed Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000048981	Medium	Summary: Removed the SW24k active CP quickly w/o re-inserting the blade. 1 error & 1 warning msgs seen: 1) [SWCH-1004], 5691,, ERROR, ?, Blade attach failed during recovery, ...; 2) [BL-1007], 5692,, WARNING, ?, blade #5: blade state is inconsistent with EM. ... Symptom: When a the SW24k's active CP is removed before the LED goes off and with POST enabled, one error and one warning messages are seen on the active CP: 1) [SWCH-1004], 5691,, ERROR, ?, Blade attach failed during recovery, disabling slot = 5; 2) [BL-1007], 5692,, WARNING, ?, blade #5: blade state is inconsistent with EM. bl_cflags 0x0, slot_on 1, slot_off 0, faulty 0, status 0. The time interval between dropping teh slider and blade removal is <1 second. This is a test for SW24K CP removal and insertion that DOES NOT follow the SW24K CP installation/replacement procedures. Workaround: Follow the SW24K CP installation/replacement procedures. Customer Impact: There is no impact to the I/O and no frame loss was observed. Reported in Release: V4.4.0
DEFECT000048983	Medium	Summary: Removed the SW24k's active CP w/o waiting the LED to drop and re-inserted it back. After failover, one warning msg was seen: [BL-1010], 2355,, WARNING, ?, Blade in slot 7 inconsistent with the hardware settings, and slot 7 got re-initialized. Symptom: When a SW24k's active CP is removed before the LED goes off and then re-inserted with POST disabled, after failober one warning message is seen on the active CP: [BL-1010], 2355,, WARNING, ?, Blade in slot 7 inconsistent with the hardware setting, and slot 7 gets re-inialized. The time interval between dropping the slider and blade removal is <1 second, between blade removal and blade re-insertion is 1 seconds, and between blade re-insertion and sllider up on that blade is 2 seconds. This is a test for SW24K CP removal and insertion that DOES NOT follow the SW24K CP installation/replacement procedures. Workaround: Follow the SW24K CP installation/replacement procedures. Customer Impact: Any I/O though the re-initialized port blade will be disrupted. Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000048984	Medium	Summary: Removed the SW24k's active CP w/o waiting for the LED to dop and re-inserted it. After failover, 1 warning msg (BL-1010) against slot 9 and 10 respectively and a number of VERIFY msgs were observed. Both slot 9 and 10 got re-initialized as a result. Symptom: When a SW24k's active CP is removed before the LED goes off and then re-inserted with POST enabled, after failover one warning message against slot 9 and 10 respectively are seen on the active CP: [BL-1010], 2355,, WARNING, ?, Blade in slot x inconsistent with the hardware setting. In addition, lots of VERIFY messages are also observed: VERIFY - Failed expression: (pt->p_info->p_if_id == msg->msg_prev_if_id), file = switch_port.c, line = 3959, kernel mode args = 42, 1133641749, 1133641748, 1133641749 Both slot 9 and 10 get re-initialized as a result. The time interval between dropping the slider and blade removal is <1 second, between blade removal and blade re-insertion is <1 second, and between blade re-insertion and sllider up on that blade is <1 second. This is a test for SW24K CP removal and insertion that DOES NOT follow the SW24K CP installation/replacement procedures. Workaround: Follow the SW24K CP installation/replacement procedures. Customer Impact: The I/O though the re-initialized port blades will be disrupted. Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000048985	Medium	Summary: Removed the SW24k's active CP w/o waiting for the LED to dop and re-inserted it. After failover, 2 critical msgs (HAM-1001 & EM-1009) and 2 warning msgs (EM-1041) were seen on the console, and this CP was faulted with a faulty code 52. Symptom: When a SW24k's active CP is removed before the LED goes off and then re-inserted with POST disabled, after failover, 2 critical and 2 warning messages are seen on the active CP: [HAM-1001], 3325,, CRITICAL, Silkworm24000, Standby CP is not Healthy, device CP Blade (Rsn: 52) status BAD, severity = CRITICAL [EM-1041], 3328,, WARNING, Silkworm24000, Sensor values for Slot 5: Temperature 1 = 0 C 1.8V = 0.00 V 2.5V = 0.00 V 3.3V = 0.00 V 5V = 0.00 V 1.2V Bloom = 0.00 V 3.3V Blade = 0.00 V [EM-1041], 3329,, WARNING, Silkworm24000, Sensor values for Slot 5: 3.3V IIC = 0.00 V 1.8V CP = 0.00 V 2.5V CP = 0.00 V 3.3V CP = 0.00 V 3. 3V Flash = 0.00 V [EM-1009], 3330,, CRITICAL, Silkworm24000, Slot 5 powered down unexpectedly The CP under test is faulted with a faulty code 52. The time interval between dropping the slider and blade removal is 11 seconds, between blade removal and blade re-insertion is <1 second, and between blade re-insertion and slider up on that blade is <1 second. This is a test for SW24K CP removal and insertion that DOES NOT follow the SW24K CP installation/replacement procedures. Workaround: Follow the SW24K CP installation/replacement procedures. Customer Impact: The haShow command indicated the CP section on both CPs are in sync. But, the sloshow command indicates the standby CP is faulted with a faulty code 52, which means the core section of this CP is faulty. To verify a successful failover, both hashow and slotshow should be executed to make sure both CP section and the core section of both CPs are healthy. Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000049118	Medium	Summary: ISL monitors tracking traffic across incorrect domains when visible domains significantly outnumber EE resources Symptom: Customer can potentially see ISL counters incrementing for incorrect domains, as well as, the correct domains. Domains that might not have any traffic could display high word counts. This is only observed if the number of domains significantly outnumber the end-to-end monitor resources on an ISL. The incorrect domain counters will cease to count after a short amount of time, however, the initial word counts will remain. Workaround: This problem only happens on SilkWorm 4100. The ISL counts will be accurate if there are enough hardware resources. Delete end-to-end monitors to free up hardware resources for ISL monitors. Customer Impact: Customers should not count on the ISL monitor to display accurate counts when the number of domains being monitored significantly outnumbered the number of available hardware counters Reported in Release: V4.4.0
DEFECT000049119	Medium	Summary: hafailover during zone propagation in a large fabric causes some E-Ports to get segmented due to zone conflict Symptom: Fabric is still operational. Some of the E-Ports may become segmented if hafailover is tried at the same time zone configuration is changed. Workaround: Execute portdisable/portenable on the segmented E-Ports. Customer Impact: The issue is seen only if the CP failed over at the same time as a zone configuration change is being made. In a customer environment, the probability of that happening is low and so the impact to the customer is minimal. Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000049201	Medium	Summary: When a user adds a graph to an existing canvas, all the ports are selected by default, instead of allowing individual port selection, for snapshot graphs. Symptom: When a user adds a graph to an existing canvas through Edit Canvas Configuration dialog, all the ports are selected by default for snapshot graphs: SCSI vs. IP, Port Snapshot Error, Switch Percent Utilization, Switch Throughput Utilization instead of allowing the users to select individual ports. Workaround: For snapshot graphs, after adding the graph, click the edit button to select the ports for which the graph is to be drawn. Customer Impact: This is a minor inconvenience. The customer has to select the ports for which the graph is to be drawn by clicking on the edit button. Reported in Release: V4.4.0
DEFECT000049215	Medium	Summary: IP table in standby CP is not updated with new IP address after a new IP address is set Symptom: IP table in standby CP is not updated with new IP address after a new IP address is set. As a result the user cannot telnet to the standby CP with the new IP address. Workaround: The new IP address will take effect if the standby CP is rebooted after changing the IP address. Customer Impact: When the IP address of the standby CP is changed, it won't take effect until the standby CP is rebooted. Since it is the standby CP that needs the reboot, the impact to the customer should be minimal. Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000049275	Medium	Summary: swAgtCmtyTable is empty when queried through a SNMPv3 client. Symptom: swAgtCmtyTable lists SNMPv1 community strings and trap targets (and their severity levels) configured at the switch. When queried using SNMPv3 client, swAgtCmtyTable shows no entries. When queried through SNMPv1, swAgtCmtyTable shows entries matching those shown by agtcfgshow CLI command. Workaround: The swAgtCmtyTable returns community strings and trap recipients when queried through SNMPv1. The same data is also available through agtcfgshow CLI command. Also, details of configured trap targets are available by quering trapRegTable (FA-MIB) using both SNMPv1 and SNMPv3 clients. Customer Impact: Using SNMPv3 client it will not be possible to get list of SNMPv1 community strings configured on the switch. However, there is no loss of functionality as using other means (SNMPv1 query and CLI command agtcfgshow) one can always get the SNMPv1 community strings. Reported in Release: V4.4.0
DEFECT000049283	Medium	Summary: SilkWorm 3850: "temperature" index disappeared from fwconfigure, switchstatuspolicyshow/set command Symptom: Customer is not able to configure temperature threshold, alarm actions and policy on Silkworm 3850. Workaround: fwclassinit will reinitialize the threshold. Rebooting the switch should get all functionality back because this is an intermittent issue Customer Impact: This is a hard to reproduce symptom that occurred only on the SilkWorm 3850. Given the workaround, the impact to customer should be minimal. Probability: Low Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000049290	Medium	Summary: User cannot enable port after disabling it in the Web Tools Switch Admin Ports tab when FICON Management Server mode is enabled and active=save mode is set. Symptom: On the Web tools Switch Admin Ports tab user is unable to enable port after disabling it by unchecking the port enable box when FICON Management Server Mode is enabled and active=save mode is set. Workaround: Using Web Tools telnet function, telnet into the switch and issue a portenable command to the disabled port. Customer Impact: The impact to the customer is that one cannot enable the port through Webtool. Given the workaround, the customer impact should be minor. Reported in Release: V4.4.0
DEFECT000049348	Medium	Summary: Running the hafailover command on the Primary FCS while a secmodedisable is running will result in a Verify being displayed on the console for both the active and standby CPs of a SW12000 or SW24000. Symptom: Customer will see the Verify -Failed expression on both Active and Standby CP consoles. The fabric will not segment and security will be disabled successfully. Workaround: There is no workaround since the operations complete successfully. The console message should be ignored. Customer Impact: Other than the Verify message on the consoles there are no side effects of running hafailover and secmodedisable at the same time. Both commands will complete successfully. Reported in Release: V4.4.0
DEFECT000049381	Medium	Summary: Many consecutive tries of merging switches with conflict domain ID may cause missing routes on SW4100 - stress test. Symptom: Many consecutive tries of merging switches with conflict domain ID may cause missing routes on SW4100. Workaround: Identify the switch(es) with missing routes Issue switchdisable and switchenable command on the switch(es) to resume the routes Customer Impact: Many consecutive tries of merging switches with conflict domain ID may cause missing routes on SW4100. When the issue occurs, some traffic on switches will be stopped, or switches are segmented from the fabric. Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000049407	Medium	Summary: Panic occurred at POST2 on Silkworm3850 after over night test Symptom: When all switches were rebooted simultaneously, one of the SilkWorm 3850 switches panic'd Workaround: None Customer Impact: This problem was observed once during an overnight test. It has not been reproduced since and so the impact to customer is minimal. Reported in Release: V4.2.2
DEFECT000049418	Medium	Summary: Under extreme load and stress testing, software watchdog kills stuck process - raslogd. . Symptom: If a lot of raslog messages are generated, it's possible to cause the raslogd to core dump. Workaround: none Customer Impact: Under extreme load and stress, the software watchdog may be called on to kill a process that is perceived as being stuck. In this case, the stuck process is raslogd. Several rounds of testing have been unsuccessful in recreating this defect. Probability: Low Reported in Release: V4.4.0
DEFECT000049488	Medium	Summary: Retrieving all dynamic EE monitors fails on large (3000 port) fabrics when the PerfMon internal cache is not populated Symptom: On large fabrics, the retrieving end-to-end monitors using the API library can fail when the PerfMon internal cache is not populated. In most cases, this would only happen in the first try to retrieve monitors. Workaround: Re-try instantiation of the End-to-End monitors after approx 5 minutes and that will succeed. Customer Impact: On very large fabrics (3000+ ports), End-to-End monitors may fail to instantiate on the first attempt. Probability: Low Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000049627	Medium	Summary: PortName function without operands does not match documented behavior Symptom: The portName command does not agree with its man page. When used without operands, customer will get an error message instead of the documented behavior. Workaround: none Customer Impact: Customer initiating a portname command without operands will expect certain output but will instead get invalid argument error. There is no direct impact to switch operation. Probability: Low Service Request# RQST00000032189 Reported in Release: V4.2.0
DEFECT000049684	Medium	Summary: Port 22 disabled on initial power on. Symptom: One of the ports shows up as disabled after switch bootup. Workaround: Issue the portenable command. Customer Impact: This defect is under investigation. Repeated testing has not been successful in recreating this defect. Service Request# RQST00000032506 Reported in Release: V4.4.0
DEFECT000049770	Medium	Summary: Performance monitor port-2 filtermonitor# 0 alias got lost during performance monitors configuration data transfer from RAM to ROM/CF back and forth. Symptom: Performance monitor configuration data lost during CF data read and write stress test. One of the filter monitor's alias is lost after repeatedly executing "perfcfgrestore; perfcfgclear; perfcfgsave" for 30 minutes. Workaround: None. Customer Impact: The filter monitor will not be identifiable by its alias. This issue was seen during a stress test. Probability: Low Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000049841	Medium	Summary: FM: Long distance changes - change columns, display long distance type and correct buffers Symptom: The current behavior does not interpret/represent the long distance data correctly and we do not match CLI. The buffers usage is a riuntime parameter. so, when the port is offline, we should show this as N/A in WT and FM. cuurently we show the values which is inaccurate representation. when trying to analyze the buffer credit information on the switch, this misrepresentation may lead to confusion in calculation of buffer credit information like buffer credits left/usage etc. Workaround: Use portbuffershow command from CLI to get accurate information. Customer Impact: Customer impact for this misrepresentation is none in terms of switch functioning or operating. But when trying to analyze the buffer credit information on the switch, this misrepresentation may lead to confusion in calculation of buffer credit information like buffer credits left/usage etc. Reported in Release: V4.4.0
DEFECT000049849	Medium	Summary: On pressing either the "Synchronize Services" or the "refresh" botton, the Service tab window within the HA Admin window becomes blank upon completion of either request. Symptom: Launch the WebTools for a sw24000. Click the "Hi Avail" button. The HA Admin window displays. Press either the "Synchronize Services" button or the "Refresh" button in the Service tab window within the HA Admin window. The Service tab window becomes blank upon completion of either request. But, if you move the cursor to the CP tab within the HA Admin window, the Service tab window gets re-displayed correctly. Workaround: Move the cursor to the CP tab within the HA Admin window, the Service tab window will get re-displayed correctly. Customer Impact: Customer will see a blank Service Tab window. To correct this problem, just move the cursor to the CP tab within the HA Admin window, and the Service tab window will get re-displayed correctly. Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000049857	Medium	Summary: SilkWorm 24000 fails to initialize Fabric Watch during firmwaredownload when a defective FAN is present Symptom: Fabric Watch client switch turns blue, and FM client can not manage switch and the overview switch status is unknow. User would see following EM message: 2004/10/01-02:23:40, [EM-1029], 574,, ERROR, Silkworm24000, Fan 3 I2C access problems (-23): state 10 2004/10/01-02:27:08, [EM-1048], 575,, INFO, Silkworm24000, Fan 3 I2C access recovered: state 10 2004/10/01-02:27:42, [EM-1014], 576,, ERROR, Silkworm24000, Unable to read sensor on Fan 3 (-23) Workaround: Reboot the switch and replace bad FAN. Customer Impact: This issue was seen when the system had a defective FAN that needed to be replaced. When the issue occurs, Fabric Watch will not work properly. Reported in Release: V4.4.0
DEFECT000049937	Medium	Summary: SilkWorm 4100 echoes back link cmd's (LR,LRR,FLOGI,PLOGI) Symptom: If the port is locked as G-port and a specific HBA is reset, under certain circumstances the port might take several seconds to come up online. If the Fibre Channel trace is checked, it will show the frames being echoed back. Workaround: If the port is not locked to G-port, there's no such issue. Customer Impact: After some specific HBA ports are reset, the port might take a bit longer than usual to come online. This problem doesn't happen if the port is not locked to G-port. Service Request# RQST00000032734 Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000049988	Medium	Summary: Cancel button in the finishing step of "Remove Offline Devices" wizard is not required and does not work as a Cancel button. Symptom: The Cancel button shows up in the final step of "Remove Offline Devices" dialog. It is not required and does not function as a Cancel button. Workaround: Do not press the Cancel button in the final step. If pressed, understand that it is the same as the Finish button. Customer Impact: Minor annoyance to see a button that should not be visible. Step indicates that the operation is already over. There is no real damage because the confirmation step precedes this step. Reported in Release: V4.4.0
DEFECT000049998	Medium	Summary: SilkWorm 4100 - Linkinit transmitting (LIP's ----17 NOS's ---- LIP's) NOS in the middle of Loop Initialization Symptom: No known side effect, operation wise (as the customer port initializes fine). But if a Fibre Channel trace is taken, customer will see a number of NOS primitives being echoed back by the switch port between SN completion and the start of LPSM. Customer Impact: None (because the customer port initializes fine). Service Request# RQST00000032760 Reported in Release: V4.4.0
DEFECT000050019	Medium	Summary: tempShow shows inconsistent data when Fabric Watch license is not present Symptom: The tempShow command can display somewhat different information for the "State" field, depending on whether Fabric Watch is installed or not. Workaround: Install Fabric Watch license Customer Impact: There is no impact on modular SilkWorms nor on single-board SilkWorms with Fabric Watch. The impact on single-board SilkWorms that do not have Fabric Watch is that a customer who runs the tempShow command (and the equivalent function in Web Tools) the "State" may not reflect over-temperature conditions for individual sensors. However, their systems will continue to monitor temperatures and if any system becomes too hot (as determined by platform-specific policies) it will take action and print one or more console logs to tell the customer what is happening. Service Request# RQST00000032852 Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000050037	Medium	Summary: WebTools allow users to set switch PID format to 2 (16-base, 256 port Encoding) when FICON management server mode is enabled. Additionally, when PID format is set to 2 and the user enables FICON management, error message displayed says unknown error. Symptom: When FICON mode is enabled, Web Tools allows PID format to be set to 2 without any error messages. Additionally, when the PID format is set to 2 and FICON mode is enabled, the error message that is displayed indicates unknown error. Workaround: None Customer Impact: For the first case (when PID format is set to 2 successfully), the customer does not know that he/she entered an illegal combination. For the second case (FICON mode is enabled), he/she does not know what the reason for the error is. Reported in Release: V4.4.0
DEFECT000050199	Medium	Summary: In a fabric consisting of v2.6 switches, when trying to propogate a zone configuration whose size exceeds the supported v2.6 limit, the propagation fails, and no further zoning changes can be made in the fabric. Symptom: The customers would not be able to start another transaction. Workaround: If a fabric has 2.6 switches, then the customers should not create a zone cfg larger than 96 KB. Or the customers can upgrade their 2.6 switches to Pulsar running 4.4 code. Customer Impact: If the customers have v2.6 switches in their fabric, then they cannot create zone configurations larger than 96 KB. The issue is seen when zone DB is propagated from newer switches that support larger configuration sizes compared to the older versions of Fabric OS and the size of the new zone DB is larger than the size supported by older versions. Switches that do not support the larger zoning DB sizes with lose their zoning DBs when committing a larger zoning DB. Reported in Release: V4.4.0

Closed Defects in Fabric OS v4.4.0

This table lists the defects that have been closed since the last Fabric OS GA release, version 4.2.2.

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000018023	Critical	Summary: Switch is rebooting- version 4.0.0c Solution: The misrouted ct response frame later on picked up by API callback caused nsd core dump. The fix is to guarantee never misrouting the response in nsa_in under any condition. Customer Impact: This issue has been resolved since 4.0.0e, 4.0.2 release. Close defect as part of defect cleanup. Service Request# RQST00000019248 Reported in Release: V4.0.0
DEFECT000018650	Critical	Summary: Switch is rebooting- version 4.0.0c Customer Impact: This issue has been resolved since 4.0.2c release. Close defect as part of defect cleanup. Service Request# RQST00000019248 Reported in Release: V4.0.0
DEFECT000035587	Critical	Summary: Compact Flash is full due to large wtmp file Service Request# RQST00000025580 Reported in Release: V4.0.2
DEFECT000045848	Critical	Summary: Meteor fails to come online to MVS - Command Rejects. Symptom: Meteor switch won't come online to MVS - Unit checks Solution: Read Port Descriptor command wasn't setting 'Port Address Not Implemented' bit correctly for area 0xFF. Due to this MVS to fail bring CUP online. The fix is to set 'Not implemented' bit for area 0xFF. Reported in Release: V4.3.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000046988	Critical	Summary: Unsupported version 2/3 Name Server entry object caused switch fail to interop with specific vendor switch. Symptom: Host does not see targets attached to specific vendor switch, also switch panic after firmwareupgrade Solution: 1. Add support for version 2 and 3 for name server entry object to interop with specific vendor switch. 2. Populate an inq response data with dummy values when size mismatch. Workaround: Remove target from specific vendor switch. Reported in Release: V4.2.1
DEFECT000015586	High	Summary: During zone merge of zone DB > 55k, zoning block transmit task and causes fab reconfiguration Service Request# DEFECT000015235 Reported in Release: V4.0.2
DEFECT000015984	High	Summary: Switch panic when removing cables. Service Request# RQST00000018282 Reported in Release: V4.0.0
DEFECT000016383	High	Summary: Switch is not sending RSCN, after target device registers to name server with RFT_ID Customer Impact: This issue has been resolved since 4.1.0 release. Close defect as part of defect cleanup Service Request# DEFECT000014517 Reported in Release: V4.0.0
DEFECT000016966	High	Summary: QLV2352 HBA speed negotiation problem in 2 Gb/s switch Customer Impact: This issue has been resolved since 4.0.2 release. Close defect as part of defect cleanup Service Request# DEFECT000016865 Reported in Release: V4.0.2

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000017882	High	Summary: Host cannot see the target on a remote switch Symptom: After created and enabled a new zone configuration, one target port was not seen by the host which was zoned with. - PLOGI was not responded accordingly - On one switch, fabricshow missed one IP for one switch. Initial investigation indicated a routing issue that prevented to complete a PLOGI. Solution: Blade driver detects route conflicts, and reports to FSPF where this conflict forces the domain route to actually be placed. FSPF updates its internal books accordingly. Reported in Release: V4.0.2
DEFECT000018541	High	Summary: Frame are being dropped at the switch Customer Impact: This issue has been resolved since 4.0.2 release. Close defect as part of defect cleanup Service Request# DEFECT000013820 Reported in Release: V4.0.2
DEFECT000019171	High	Summary: Track Logging Feature does not detect failure login to the switch via SSH. Symptom: When user login to a switch via regular rlogin/rsh or telnet, the login attempted (success or failure) is reported by Track Log Changes feature. However, when SSH (Secure Shell) is used, the login attempt is not reported. Customer Impact: With Security Event logging using the RAS log support, this problem no longer applies to FOS 4.4. Reported in Release: V4.0.3
DEFECT000024431	High	Summary: Switch (active CP) reset when switchdisable/enable script running. Symptom: Overnight stress test that involves issuing simultaneous switchdisable commands to all 34 switches of a core-edge fabric, followed by simultaneous switchenable commands to all 34 switches. Customer Impact: This is a Stress to Fail test case that requires running for long periods of time before encountering the CP reset on one of the core switches. The switch performed a fail-over, and the fabric continued to run without disruption. Probability: Medium Reported in Release: V4.1.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
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: There is a well documented workaround. Reported in Release: V4.1.0
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. Reported in Release: V4.1.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000025747	High	Summary: Message "Oops: kernel access of bad area, sig: 11" shows up and switch reset. Symptom: Stress test involving a 34 switch fabric, on which one of the core switches is constantly being issued the hafailover command. Simultaneously, one of the edge switches is constantly having its zoning configuration updated. Workaround: The problem was caused by an error in the test script, in which the zoning cfg command was issued to the Standby CP by accident. Customer Impact: The problem was caused by an error in the test script, in which the zoning cfg command was issued to the Standby CP by accident. Reported in Release: V4.1.0
DEFECT000025890	High	Summary: Switch Status Marked As Healthy When CF (compact Flash) 100% Full With Write Errors. Symptom: Switch status does not reflect the down graded potentially critical condition of the switch Customer Impact: The new feature to mark the switch status as "marginal" will be implemented in a future release Service Request# RQST00000023238 Reported in Release: V4.1.1
DEFECT000025910	High	Summary: After changing Ethernet IP address from CLI or from WT, can not launch WT with new IP address Symptom: WebTools can not be launched with new IP address Customer Impact: Issue is being investigated, and will be targeted for a future release of Fabric OS. Reported in Release: V4.1.1

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000025948	High	Summary: Switch Failed To Generate Any Event, KSWD, Core Dump Notification After RPCD Issue. Symptom: Errshow contains no event notification regarding the failed status of the switch in some extreme cases of running out of memory. Customer Impact: The condition of generating multiple rpcd has been removed since FOS 4.2. and therefore there will not be conditions leading to the inflated memory consumption. These changes would eliminate the "rpcd core dump" due to the specific reason of running out of memory as multiple copies of "rpcd" would not be invoked. Also, there will be a significant performance impact, if logic needs to me added to monitor memory consumption this low level of granularity. Service Request# RQST00000023346 Reported in Release: V4.1.1
DEFECT000025949	High	Summary: v4.1.1_rc2 Firmware Download Hangs Switch After Critical SYSC-ERROR Seen. Symptom: Switch lost connectivity, services not able to support commands, firmware not able to commit until rebooted. Customer Impact: Switch was unable to close all open processes due to an error condition created prior to the firmware download. Improvements to the error detection and reporting during the hot code load are currently under development to address this issue for a future release of the Fabric OS. Service Request# RQST00000023347 Reported in Release: V4.1.1
DEFECT000026033	High	Summary: SilkWorm3900 error and reboot 'Critical kSWD-kSWD_GENERIC_ERR_CRITICAL, 1, kSWD:' Customer Impact: This issue has been resolved since 4.2.0 release. Close defect as part of defect cleanup. Service Request# RQST00000023508 Reported in Release: V4.0.2

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000026274	High	Summary: Secure Fabric OS does not handle all SAN gateways properly Symptom: With certain SAN gateway products, Secure Fabric OS will segment the link that uses the gateway product. Workaround: This is actually a request to enhance the capability of the Secure Fabric OS functionality to operate with all gateway products. The capability of the 4.2 firmware to interoperate with gateways is identical to the capability of the 4.1.1 Fabric OS. Customer Impact: This is actually a request to enhance the capability of the Secure Fabric OS functionality to operate with all gateway products. The capability of the 4.2 firmware to interoperate with gateways is identical to the capability of the 4.1.1 Fabric OS. Probability: High Reported in Release: V4.1.1
DEFECT000033399	High	Summary: Downloading configurations(by line) too quickly causes switch panic/crash. Symptom: The switch will panic if the config download is done in very quick succession. Workaround: Do not execute repeated configdownload commands in rapid succession. The user is advised to either have a sleep(6) or to just wait between download attempts which will avoid the problem. Customer Impact: The customer impact is that they will not be able to rapidly config-download to their switch. They need to put delays in between efforts so as to avoid the problem. Probability: Low Reported in Release: V4.1.1
DEFECT000033980	High	Summary: Domain RSCN sent when IP-Address of switch is changed Symptom: Causes FICON Host channels to churn unnecessarily and results in IFCC. Customer Impact: Sending the Domain RSCN follows the current standards. Changing this behavior at this point would require extensive testing to ensure backward compatibility. A solution is being investigated that will involve a proposed change to the standards. Reported in Release: V4.1.2

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000034297	High	Summary: While running API automated suite on both halves of a 12000, the switch dumped core on nsd, panic, and psd. Symptom: While running API automated stress tests on both switches in a SilkWorm 12000, there was a core dump on the switch. Reported in Release: V4.1.2
DEFECT000034473	High	Summary: Mechanism needed to monitor or prevent all instances of compact flash using 100% of capacity. Symptom: Under some rare circumstances, the flash file system fills up completely. Workaround: In 4.2.0, we have implemented several fixes: 1. All known causes of the flash full condition have been fixed in the software. 2. We restrict the size of a Linux file that is known to contribute to the flash full condition. 3. A utility has been added that monitors the utilization of the Compact Flash and reports errors if the flash is above 80% utilization. If this error message is ever seen, customer service should be contacted so that the proper steps can be taken to prevent the flash from completely filling up. We are leaving this defect open, because we will be implementing user configuration of the flash full monitoring in the next release of fabos. Customer Impact: The change to monitor compact flash usage has been implemented in Fabric Watch in a future release. A temporary solution to warn the user of high compact flash usage has also been implemented in the 4.2 release. Service Request# RQST00000024877 Reported in Release: V4.1.1

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000034830	High	Summary: Switch reboot with CF Error: hda: status timeout .... Symptom: Observed switch reboot with following message logged on switch console: hda: status timeout: status=0xd0 { Busy } hda: no DRQ after issuing WRITE ide0: reset timed-out, status=0x80 hda: status timeout: status=0x80 { Busy } hda: drive not ready for command ide0: reset timed-out, status=0x80] end_request: I/O error, dev 03:01 (hda), sector 75792 end_request: I/O error, dev 03:01 (hda), sector 75800 end_request: I/O error, dev 03:01 (hda), sector 71632 end_request: I/O error, dev 03:01 (hda), sector 71640 XFS: device 0x301- XFS write error in file system meta-data block 0x117d0 in ide0(3,1) end_request: I/O error, dev 03:01 (hda), sector 74128 end_request: I/O error, dev 03:01 (hda), sector 74136 end_request: I/O error, dev 03:01 (hda), sector 109020 I/O error in filesystem ("ide0(3,1)") meta-data dev 0x301 block 0x1a9dc ("xlog_iodone") error 5 buf count 3584 xfs_force_shutdown(ide0(3,1),0x2) called from line□. Watchdog Exception: current process c2c04000, r1=c2c059f0 □. Service Request# RQST00000025100 Reported in Release: V4.1.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000034835	High	Summary: Switch: 0, Critical SCN-SCNQ_OVERFLOW, 1, SCN queue overflow for nsd Symptom: Critical SCN-SCNQ_OVERFLOW, 1, SCN queue overflow for nsd Workaround: Staying within the scalability limits that 4.2 has been tested with will avoid this problem. This problem can also be avoided if not all devices are brought online at the same time. This problem occurs in a stress condition in a fabric with more devices and switches than it can handle with the current release. (See Scalability limits for fabrics supported with 4.2.0). Scalability enhancements are planned for a future release. Customer Impact: This problem occurs in a stress condition in a fabric with more devices and switches than it can handle with the current release. (See Scalability limits for fabrics supported with 4.2.0). Scalability enhancements are planned for a future release. Probability: Medium Service Request# RQST00000025031 Reported in Release: V4.1.1
DEFECT000035672	High	Summary: NoNodeWWNZoning - cfgenable is no longer sufficient to truly activate this feature. Symptom: NoNodeWWNZoning - cfgenable is no longer sufficient to truly activate this feature. Unable to activate NoNodeWWNZoning with just the cfgenable command. Workaround: Use cfgdisable followed by cfgenable, instead of just cfgenable. Customer Impact: The problem only happens when Node WWN is used in Zoning and will be resolved in a future release. Probability: Medium Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000036096	High	Summary: SCAL WT: Critical error on SCN queue overflow for weblinker.fcg after disabling all trunks on core switches Symptom: In a large fabric stress scenario when a fabric administrator disables/enables all trunking links on a core 24k switch, the following message Critical 0 "SCN-SCNQ_OVERFLOW SCN queue overflow for weblinker.fcg" may be seen in the event page of WT. This message is also seen on the console when the action is performed repetitively on the core 24k switch. This message is benign. It does not have any impact on the operation of the switch. Solution: To avoid SCN message queue overflow, dynamically register/de-register for remote SCN on getting domain valid/invalid scn respectively. Customer Impact: This happens only in a large fabric (26 switch, 1280 port) stress environment when a fabric administrator disables/enables all trunking links on a core 24k switch. The message Critical 0 "SCN-SCNQ_OVERFLOW SCN queue overflow for weblinker.fcg" is seen in the event page of WT. Even though message is reported critical, it is NOT critical. This message is benign. It does not have any impact on the operation of the switch. This problem will be fixed in a future release Reported in Release: V4.2.0
DEFECT000036446	High	Summary: Enhancement is needed for frureplace when replacing WWN card. Symptom: When frureplace procedure was executed for a "bad wwn card". The corrupted data on the bad card is copied over to new card. Solution: First check to see if the data is corrupt before backing it up. In Customer Impact: The request will be partially addressed in a future release. In this release the detection and logging of the underlying error will be provided. A later release will address issues beyond notification of error having been detected Service Request# RQST00000025999 Reported in Release: V4.1.1

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000037154	High	Summary: Firmware download on SW3250/3850: power cycle switch - Oops panic, in swapper Symptom: During a firmwaredownload operation, if the power to the switch is interrupted, the message "Oops kernel access of bad area" may appear on the console. Workaround: During a firmware download, user must not interrupt the power supply to the switch. Customer Impact: This symptom only occurs in the exceptional situation that power is interrupted during the firmware download operation. The likelihood that there would be a power failure at the precise time of a firmware download is low considering how infrequently (if ever) the customer would need to reload firmware. This defect will be fixed in a future release. Probability: Low Reported in Release: V4.2.0
DEFECT000037345	High	Summary: SW3900 reports of a fan at 0 RPM Service Request# RQST00000026671 Reported in Release: V4.1.0
DEFECT000037667	High	Summary: For multi-frame sequences in an acknowledged class of service the end of frame delimiter's for the ACK_1's should be EOFn for all frames except the last frame, which should be EOFt. Symptom: During large zone DB merge, third party vendor switches stop to send frame upon receive EOFt ACK_1 frame in a multi sequence from Silkworm 3900, result incomplete zone merge. Solution: Set the IU_LASTFRAME flag only if the ACK frame is sent to the last frame of the sequence. Customer Impact: This issue has been resolved since 4.2.2a release. Close defect as part of defect cleanup. Reported in Release: V4.1.2

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000038363	High	Summary: Web Tools and CLI Fan, Power Supply, and temperature status should use fabric watch thresholds. Additionally, the temperature status should use all the sensors (in both halves of a bladed switch) Symptom: WebTools shows wrong thermal status Solution: Update temperature sensor monitoring to monitor chassis wide sensors; update tempshow, sensorshow to reflect the change. Probability: Low Reported in Release: V4.2.1
DEFECT000039297	High	Summary: Firmwaredownload from 4.2.0_rc1 to 4.2.0_rc2, seeing "sysctrld: error in loading shared libraries: sysctrld: undefined symbol: hilGetSysTotalUport" and CPs started failing over back and forth with panic. Customer Impact: The problem happened when SW tried to execute a binary that wasn't removed when a firmwre download occurs. The firmwaredownload was from 4.1.x to 4.2.0 . We do not know how the switch still had the left-over binary. Effort to reproduce this problem has not yielded the same failure. Probability: Low Reported in Release: V4.2.0
DEFECT000040532	High	Summary: encout errors 3900 Symptom: Enc_out errors are being generated on ports with nothing plugged into them other then the SFP. Service Request# RQST00000028106 Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000041674	High	Summary: CP in slot 5 set to faulty. Symptom: CP in slot 5 (CP0) was set to faulty and did not recover after reboot. Minicycle diagnostic errors were observed: 0x268b (fabos): Mar 24 12:30:20 Switch: 0, Error DIAG-ERRSTATS, 2, minicycle, pass 0, Pt5/-1(59) Ch7/3 CRC_err Error Counter is 7483 sb 0, Err# 1400831 053B Solution: Clean up code to set private state data hold flag for normal powerdown request not for shutdown, also during inconsistent cp recovery sequence clear state flag when intervening state calls are encountered. Service Request# RQST00000028670 Reported in Release: V4.2.0
DEFECT000041767	High	Summary: Disable the secure mode using secmodedisable, rpcd failed to refresh and the active CP panics and reboots. Symptom: Disable secure mode, rpcd failed to refresh. Haven't seen this problem occur again. Customer Impact: This problem was seen once and unable to reproduce. Reported in Release: V4.3.0
DEFECT000041768	High	Summary: MMI SCN processing is incorrect in 4.3.0 Symptom: This problem only applies to model SW3016 due to the way that SCNs were handled in this model. Workaround: No Known workaround. Reported in Release: V4.3.0
DEFECT000041846	High	Summary: The internal interfaces are exposed when the switch is on a 10.0.x.x network Symptom: If the IP addresses are set up on a network that is configured with IP address that are 10.0.x.x and a subnet mask of 255.255.0.0, there will be routing between eth0 and eth1. This is not the expected behavior, as eth0 traffic should not be routed to eth1. Based on the v4.2.0 Procedures guide the switch should be preventing routing of packets to and from the internal network. Solution: Drop icmp packets destined for internal network. Service Request# RQST00000028723 Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000041996	High	Summary: PORT-LINK_FAULT boundary Symptom: Switch ports are set to faulty when certain tasks are performed in Win2003 clustered environment. A portshow that was taken before and after starting the cluster services were started and shows that the link failure count increases by the number of attached diskdrives (this means, 33 disks = 33 link failures) At a certain point switch disables the port and the following error message is observed: Switch: 0, Warning PORT-LINK_FAULT, 3, Port 6 Faulted because of many Link Failures Solution: When too many link-down events occur, fault the port rather than disable it. This allows the port to self-recover rather than requiring manual intervention to recover the port. NOTE that the switch port behavior changes in this case: the port will attempt to recover after two minutes, rather than remaining disabled. Service Request# RQST00000028026 Reported in Release: V4.1.1
DEFECT000042029	High	Summary: fwd core dump with fcntl (F_SETLKW): Bad file descriptor error message Symptom: Abserve this error message: INIT: Sending processes the TERM signal FSSME exiting.. signal = SIGTERM fcntl(F_SETLKW): Bad file descriptor fwd:1 (pid=784), signal=11 Solution: Threading model change of Fabric Watch fixes this problem. Reported in Release: V4.1.1
DEFECT000042181	High	Summary: Changed the time and the tsd crashed on all switches in fabric Service Request# RQST00000028869 Reported in Release: V4.1.1

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000042221	High	Summary: Switch is not allowing enough time for LISM for a specific vendor's new JBOD. Symptom: The switch is not waiting long enough for the drive to change LISM ID's before it decides something is wrong and it reinitializes the loop. As a result, a large loop of JBOD disks will not come online. Solution: The problem is caused by an interaction between the Switch (number and frequency of the LISM frames we send out) and a specific vendor's "new Loop init in hardware" feature. Switch side fixed the problem by send many more LISMs at a time. The vendor side also adjusted their firmware to disable the feature if they get into this state. Customer Impact: This has only been seen with specific vendor JBOD disks that do Loop Init in hardware. Probability: Low Service Request# RQST00000027882 Reported in Release: V4.2.0
DEFECT000042979	High	Summary: RTC: i2c_master_send() failed while writing RTC registers. RTC_SET_TIME: Bad address. ioctl() to /dev/rtc to set the time failed. Symptom: Observed this message during boot process "RTC: i2c_master_send() failed while writing RTC registers" Solution: Modified the algorithm for Single Board Platforms (440) for the sensor drivers to acquire the semaphore (i2c_sem) for all access to the i2c bus. This provides serialization with FOS. Also reduced the overall worst case delay, experienced in case of bus access failures Customer Impact: Internal error. No known side effect. Reported in Release: V4.2.0
DEFECT000043225	High	Summary: cfgEnable doesn't work with Error -22 Symptom: This problem occurred when a large zone configuration (> 120K in size) is used. Cannot reproduce this issue anymore. Reported in Release: V4.3.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000043233	High	Summary: Switch should display customer-visible error messages when recovery or bootup fails. Symptom: There will be no error messages shown when switch recovery or bootup failed. Solution: Reset the pointer whose data was freed even if a wwn change was detected; before returning error to indicate a cold recovery is needed. With new defect name to display the right error massages, the solution is to display error messages in 2 places: 1. sysctrld to display a log when recovery or bootup times out 2. fssme to display a log when there is a recovery error during warm or cold recovery. The customer action in both these cases is to reboot the chassis, and if it happens repeatedly, then call manufacturer for support. Workaround: Don't do hot code load after doing an uncommitted change of wwn number. Customer Impact: The probability of this occuring is low and under very specific condition. The problem occurs when the wwn number for the switch was changed, but not committed, sometime before the firmware download was done. In this case, the wwn had been changed on the wwn card only or in memory only. When the warm recovery after download starts, the difference between the memory value and what is in the wwn card is detected results in this problem. Probability: Low Reported in Release: V4.2.0
DEFECT000043337	High	Summary: Need to get license name for FICON/CUP changed from just "FICON" to "FICON in-band management license" Service Request# RQST00000029229 Reported in Release: V4.2.0
DEFECT000043616	High	Summary: Two CPs that were in the same director will not boot after power cycle. Symptom: CP doesn’t complete it□s boot sequence Customer Impact: This happens when power is pulled while the system is accessing compact flash on both CPs, the likelihood of this failure is very low. Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000044859	High	Summary: Critical SWD error on a SW24000. msd died and switch panicked twice while rebooting all the switches in the fabric at the same time Symptom: In a mixed fabric, a SilkWorm 24000 director at the core panicked and ms daemon died with error message on the console when executed a test script to reboot all the switches in the fabric at the same time. Workaround: Disable platform services Reported in Release: V4.3.0
DEFECT000044911	High	Summary: it failed to write to switch when try to enable long distance capability from WT Symptom: Cannot enable long distance mode from WebTools. CLI works fine. Workaround: Use CLI to enable long distance modes. Reported in Release: V4.3.0
DEFECT000044978	High	Summary: Ficu coredump when activating PDM Symptom: Ficu daemon stops functioning, which prevents users from accessing Ficon CUP functions. In the test scenario, user will get "IPC error cannot set CUP configuration" when trying to activate the PDM. Customer Impact: This issue has been resolved in 4.4.0 release prior to rc1. Close defect as part of defect cleanup. Reported in Release: V4.3.0
DEFECT000045033	High	Summary: The scan tool has indicated that the embedded apache server exposes Cross-site tracing vulnerability Symptom: Cross-site tracing vulnerability was reported after running scan tool on SAN. Solution: The scan tool has indicated that the embedded apache server exposes Cross-site tracing vulnerability due to exposure of TRACE method. This vulnerability does not result in sensitive data being exchanged via standard HTTP headers. The fix is to follow the standard recommended solution by the apache community to block http TRACE and remove access to cgi_bin directory. Service Request# RQST00000029630 Reported in Release: V4.1.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000045042	High	Summary: FM: FM Database shows less number of devices for 2+6 fabric than what is seen in nameserver entries Symptom: We cannot reproduce this issue with the latest build. Reported in Release: V4.3.0
DEFECT000045319	High	Summary: Silkworm 12000 CP failover due to zone daemon failure Symptom: Switch failover caused by zoned cannot warm recover. Solution: Fixed an IPC problem between zoned and nsd. Customer Impact: zoned never completed warm recovery; this is a known issue caused by an IPC problem between zoned and nsd. This problem is a timing issue that happens only in rare instances. It is fixed in a future release. Service Request# RQST00000029911 Reported in Release: V4.1.2
DEFECT000045465	High	Summary: Domain port level zoning enabled port cannot be seen. Symptom: After zoning is changed from mixed to all wwn zoning, host F-Ports loses access to target F-Ports. This is very intermittent and hard to reproduce. Solution: Synchronize the completion of a F-port coming online even when there is no effective zone cfg. Also, during warm boot recovery, zoning will scan the F-ports even when there is no effective zone cfg. Workaround: Do a portzoneshow and note any ports reporting F-Port = 0. Disable and then enable these ports so port logs back into fabric. Issue a portzoneshow and all F-Ports should be F-Port = 1. Customer Impact: This issue is hard to reproduce. Given the work around, there should be very little customer impact. This defect is currently under investigation and the fix will be available at RC. Service Request# RQST00000030010 Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000045612	High	Summary: FM enabling FMSMode does not disable port x'7E' aka Port 126 Symptom: Fabric manager does not disable port 126 when FMS mode is enabled. Solution: Disable the FMS port if it enabled and offline during FMS mode enabling. Reported in Release: V4.3.0
DEFECT000045617	High	Summary: Termination of Name Server daemon and switch reboot during receiving continuous rscn. Symptom: During configuration change on a target, a continuous flood of RSCN's was generated in a short time frame which caused Name Server daemon to panic. Solution: In the case when devices send port-detected RSCN in a very frequent rate, it could take a lot of CPU time to process. To reduce the cpu and memory usage, we will check whether the same RSCN is currently being processed. If it is, then simply ignore the incoming RSCN. Customer Impact: The fix for this defect is in progress. It will be available at RC. Service Request# RQST00000030119 Reported in Release: V4.2.0
DEFECT000046070	High	Summary: Unit Check 0xCA returns when releasing a file lock with PDCM set on its own port Symptom: The switch returns Unit Check on the CUP port after a file lock is released with a configuration file where PDCM has ports prohibited to themselves. Solution: 1. Modify Block State was setting the connectivity attributes in the CFRec File structure incorrectly. As a result it was wiping out other bits that were previously set in that bit mask 2. CUP should return 0xC5 reject code if the internal port bit is ON in PDCM for the normal ports (i.e., implemented ports sans internal port) when saving a configuration file. 3. CUP should ignore the internal port bit in PDCM for port 0xFE when saving a configuration file. In fact, the bit will stay on in the saved file if it□s been turned on by Modify PDCM command 4. PD Bit in the Port Descriptor should be set when any bit in the corresponding PDCM for that Port is ON Reported in Release: V4.3.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000046108	High	Summary: False x'29C7' errors running MVS Symptom: Equipment checks on MVS Solution: 1. Modify Block State was setting the connectivity attributes in the CFRec File structure incorrectly. As a result it was wiping out other bits that were previously set in that bit mask 2. CUP should return 0xC5 reject code if the internal port bit is ON in PDCM for the normal ports (i.e., implemented ports sans internal port) when saving a configuration file. 3. CUP should ignore the internal port bit in PDCM for port 0xFE when saving a configuration file. In fact, the bit will stay on in the saved file if it□s been turned on by Modify PDCM command 4. PD Bit in the Port Descriptor should be set when any bit in the corresponding PDCM for that Port is ON Workaround: None Reported in Release: V4.3.0
DEFECT000046113	High	Summary: IU Leaks in Processing BA_ACC to ABTS from Channel Symptom: When running error injection/recovery stress tests, memory leaks are observed. Solution: Problem isolated to IU leaks in processing BA_ACC to ABTS from channel. Fix IU leak in case of BA_ACC processing. This was caused by non-zero seq_cnt field set by IBM channel on BA_ACC frames which was causing an extra IU hold. Since BLS sequences are always single frame, this extra hold is not required. Reported in Release: V4.3.0
DEFECT000046114	High	Summary: Incorrect BA_Rjt Implementation per FC-FS spec Symptom: When running an error injection test with recovery, the OX ID / RX ID fields in the BA_RJT were observed to be modified, resulting in the channel sending ABTS again and again. Solution: BA_RJT response was not compliant with FC-FS. Change made to the FC Driver to leave OX/RX_ID fields untouched in BA_RJT response Reported in Release: V4.3.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000046129	High	Summary: Webtools won't display Switch #1. Symptom: "swType" has bogus value when WebTool retrieve the data from the switch prevent display switch information. Solution: Use sysconModel rather than depending on fspf information for switch type. Service Request# RQST00000030394 Reported in Release: V4.1.1
DEFECT000046246	High	Summary: Kernel images are corrupted after overnight testing of firmware upgrade and down grade. Symptom: CP keeps on rebooting after overnight testing of firmware upgrade and down grade. Solution: When the primary kernel image is corrupted, the boot monitor uses the secondary image to boot up. However, when firmwarecommit command is started, it would blindly overwrite the secondary kernel image (the good one) with the primary kernel image (the bad one) and result in both corrupted kernel images. The change involves adding a new bootenv OSBooted to indicate the kernel image that is actually used to boot up. In firmwarecommit, we check whether this bootenv is consistent with the first value in OSLoader. If it is, the primary kernel image is used to boot up and firmwarecommit will proceed normally; otherwise, the secondary image is used to boot up and firmwarecommit will fail. Customer Impact: This happened during overnight looping on downgrading firmware, then upgrade firmware. Reported in Release: V4.2.2
DEFECT000046679	High	Summary: Runing Sak-excite with recovery, fails to recover after 'resets' Symptom: Running an error injection stress test with recovery results in 'hangs' after switching test cases. Solution: The resetting event indication was getting erroneously set when Selective Reset was received while control device was in contingent allegiance state. This problem has been corrected. Reported in Release: V4.3.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000046704	High	Summary: Coredumps while processing Read Node Identifier CUP command Symptom: While running a stress test on the CUP port over a long period of time, the switch took a core dump while processing a RNID request. Solution: When processing a Read Node Identifier command and retrieving the RNID from a neighboring switch, the FICON/CUP module was not handling all return codes properly. If the attempt to retrieve RNID from a neighboring switch fails, the FICON/CUP module will now set the invalid flag in the RNID and respond to the Read Node Identifier command, when the interface is an E-Port. Reported in Release: V4.3.0
DEFECT000046767	High	Summary: SilkWorm3250 won't reboot even all fans failed. Symptom: When all the fans are stopped (0 RPM) on SW3250. It did not send out the message and switch did not shutdown (=reboot) itself. Solution: Silkworm model 3250s will issue a warning message and then reboot within two minutes when two or more of the three fans fail. Similarly, Silkworm model 3850s will issue a message and reboot within two minutes when three or more of the fans fail. THERE IS NO HAZARD ASSOCIATED WITH THIS DEFECT. These products are designed with enough margins to continuous run without fans and have been extensively tested to run continuously at 40 Degrees Celsius. Further more, running full diagnostic of switch at 60 Degrees Celsius for 8-hours with all FANs disconnect; the system temperature never reached the maximum limits. Service Request# RQST00000030747 Reported in Release: V4.2.0
DEFECT000047032	High	Summary: IBM: Devices Not Accessible After Mainframe "Config POR" Symptom: Some CHPIDs are not able to access the devices after an IOCDS change and 'config POR'. It appears that FLOGI to the devices get F_RJT with reason code x04. A port disable and port enable at the switch for the CHIPID corrects the problem. Reported in Release: V4.3.0
DEFECT000047240	High	Summary: Voltagemargin command supported ? Service Request# RQST00000030975 Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000049027	High	Summary: telnet timeout on SW12000 with FOS V4.1.x and later. Symptom: Using Script continuously telnet login/logout, some sessions fail with timeout. Workaround: Adding delay between sending login and passwd Customer Impact: The issue was seen only when a script was used to continuously login/logout to the switch. Therefore the impact to customers should be minimal. Service Request# RQST00000031914 Reported in Release: V4.1.2
DEFECT000049439	High	Summary: Critical PLATFORM-CP_SERVICE, 1, Internal routing error. Disabling switch(es) " Symptom: When POST is running, reset the micro switch on the active CP. The standby CP will become active CP now. However, the console of this current active CP will show an error message "Critical PLATFORM-CP_SERVICE, 1, Internal routing error. Disabling switch(es)". When the POST test are successfully done, the switch is in "disable" state. Solution: This is expected behavior; However, the message "Internal routing error" is unnecessarily alarming, which has been changed to an informative message in FOS4.4. Reported in Release: V4.2.2
DEFECT000049444	High	Summary: Host lost connection to storage after "host reboot" stress script testing. Symptom: After reboot hosts many times, host lost connection to target due to switch side routing did not setup. Workaround: portdisable and portenable the port. Customer Impact: This is a very corner case. It's only observed on a HBA which sends FLOGIN right after idle in micro seconds after multiple host reboot test. Service Request# RQST00000031942 Reported in Release: V4.0.2

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000012972	Medium	Summary: setslot command is a manufacturing command and should not be for general use Symptom: Setslot command help page does not provide any information on how to display the current slot number. Customer Impact: This defect no longer applies to FOS4.4 as setslot is now a manufacturing only command. Reported in Release: V4.0.0
DEFECT000015117	Medium	Summary: [Inconsistency] : Commands not permitted in the present login must display "Permission denied" message Customer Impact: This defect is requesting to have the "permission denied" message used consistently when the login level (user,admin,root) is trying to run a command which is not executable at that shell level. For instance, if a user level login tries to execute a root command, the message "rbash: command not found" may be displayed. This has no effect on the functionality of the commands executed or the ability to have proper access to the commands for the particular login level. Probability: High Reported in Release: V4.1.0
DEFECT000018526	Medium	Summary: perfShowEEMonitor slot/port, interval of 5 will print out one line of all ZERO when it reach the RX and TX count some where around 0x40000000 Symptom: perfShowEEMonitor slot/port, interval of 5 will print out one line of all ZERO when it reach the RX and TX count some where around 0x40000000 Customer Impact: The current implementation of end-to-end and filter based monitors dictates that hardware counters be probed at 5 second intervals. As a result, the RX and TX counts could show values of 0 occasionally. When that happens, the next RX and TX values will show the correct values again. The fix for this problem will be implemented in a future release Reported in Release: V4.1.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000021272	Medium	Summary: Scalability: don't show the Broadcast message of one switch instance in another switch (when they are on same CP) since they might be part of different secure/non secure fabric Symptom: On SilkWorm 12000 platforms, security event messages are broadcast for any switch instance are broadcast to the users of both switch instances. Workaround: None. Customer Impact: This is the defined behavior of the current implementation. An enhancement to restrict the broadcast of messages to the switch instance on which the event occurs is being contemplated for a future FOS release. Reported in Release: V4.1.0
DEFECT000021352	Medium	Summary: fruHistoryTrap is 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. This is unlike 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. Therefore, there should be minimal customer impact. Reported in Release: V4.1.0
DEFECT000021500	Medium	Summary: Functionality problems w/ Topology Commands(GATIN) Symptom: An update to the standards protocols was made for the GATIN command, and the new modes are not supported This is a MS command used to discover the topology of the fabric. Customer Impact: Standards changes were made after the implementation phase of the project. This request is currently being reviewed and planned for an update in a future release Reported in Release: V4.1.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000024542	Medium	Summary: No log message is generated when one CP resets the other CP. Symptom: There is no longer any message logged or displayed when one CP resets the other CP. Solution: Our code will move away from the use of printk in a future release and will allow the message to be added back in. Workaround: none Customer Impact: The message was removed in order to reduce the amount of printk during panic dump processing. The trade off here is that we have a better chance of capturing a good panic dump. In a future release, printk is no longer used and the message can be added back in. Reported in Release: V4.1.0
DEFECT000024767	Medium	Summary: get urouteconfig _cli: Input port not available for routing when setting a static route for inport 0 but the route is set ok Symptom: When configuring a route the user may in a rare instance receive an incorrect error message "Input port not available for routing". Customer Impact: Incorrect error message is issued due to a minor timing window which does not affect correct operation, however fixing the timing window is too risky at this point in the release, and so the change is being deferred to a future SW release. Reported in Release: V4.1.0
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: The disable event is being reported twice via the 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. Customer Impact: This issue is only seen when using the Fabric Access API to disable a trunked port. This will be fixed in a future FOS release. Reported in Release: V4.1.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000024999	Medium	Summary: Need better switch side solution to re-establish event channels when SilkWorm 12000 failover triggers a cold boot Symptom: Customers will not see a lot of events (e.g login/logout events, config change event, FW events etc.) .Will only see RSCN and Fabroc change events. Workaround: The host lib re-establishes the event channel Customer Impact: This can only happen if the SilkWorm 12000 cold-boots (which is unlikely to happen). There is a workaround available. The customer is unlikely to see this problem. Reported in Release: V4.1.0
DEFECT000025210	Medium	Summary: SW 12000 fails backport test when certain Domain IDs are used Workaround: No workaround Customer Impact: Diag test no impact to switch functionality. The defect has been fixed since FOS 4.1 Service Request# RQST00000022098 Reported in Release: V4.0.2
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. This will be fixed in a future FOS release. Reported in Release: V4.1.0
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. Solution: this was fixed when rpcd was changed from chassis service to switch service 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. Reported in Release: V4.1.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000025318	Medium	Summary: Wrong value in Enterprise field of coldStart Trap from SilkWorm 3900 (FOS v4.0.2c) Symptom: The enterprise field oid of coldStart Trap is 1.3.6.1.6.3.1.1.5. Customer Impact: Workaround available. The other field values are correct. Will be fixed in a future FOS release. Service Request# RQST00000022147 Reported in Release: V4.0.2
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. Solution: Get the segmented reason from the kernal and display to the user. Customer Impact: This is a WebTools display problem. The fix for this defect will be considered for future release Service Request# RQST00000022076 Reported in Release: V4.1.0
DEFECT000025498	Medium	Summary: 2 new entries in this table called fruHistoryOEMPartNum and fruHistoryFactorySerialNum that pull out the OEM specific information that is programmed in manufacturing for them. Symptom: Vendor specific part number of the switch is not accessible thru SNMP. Vendor specific soft serial number can be accessed thru swSsn (SW mib), if the ssn entry is available in configuration database. Otherwise, swSsn gives the WWN of the switch. Solution: Added new mib object fruSupplierId, fruupplierPartNum, fruSupplierSerialNum and fruSupplierRevCode to fruTable in HA mib to pull out the supplier data. The data will be similar to the output of 'fruInfoSet wwn 1'. Workaround: Use CLI command instead of SNMP. Also, The supplier serial number can be accessible thru swSsn and connUnitSn. Customer Impact: There is a workaround. Will be fixed in a future FOS release. Service Request# RQST00000022398 Reported in Release: V4.0.2

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000025519	Medium	Summary: Failover during hardware configuration operations may leave the port in an inconsistent state. Symptom: It is possible for a port to remain non-operational if a zoning configuration action is interrupted by a switch failure. Customer Impact: This combination of switch failure during a configuration operation happens rarely and there is a manual recovery available. Fixing this symptom at this time has a high risk of destabilizing the tested code base so the changes will be deferred to a future next release. Reported in Release: V4.1.0
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. Using command port portcfgtrunkport to enable the trunk for each port (recommended) 2. Disable long distance port before issue switchcfgtrunk Customer Impact: This symptom is a minor annoyance and has an easy workaround. Since the symptom will go away in the next release because trunking on long distance ports will be supported, the effort and risk are not worth the short term benefit of correcting this behavior. Reported in Release: V4.1.0
DEFECT000025578	Medium	Summary: Trying to commit after creating an alias that's about 128K would fail with -55 (ERR_COMMIT_FAILED) while using a SilkWorm 12000 in a secure fabric as proxy. Symptom: Trying to commit after creating an alias that's about 128K would fail with -55 (ERR_COMMIT_FAILED) Customer Impact: The problem has only been seen in stress test and will be resolved in a future release. Probability: Medium Reported in Release: V4.1.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000025580	Medium	Summary: Able to reset version time stamp when logged in as "user" Symptom: When logged in as 'user' form an API Application, resetting version time stamp will succeed. This should fail and an error code should be returned. -224 should be returned if it is attempted. Customer Impact: This is an API only issue and has low customer impact, as logins from API Applications are normally as 'admin'. This defect will be considered for a fix in a future Fabric OS release. Reported in Release: V4.1.0
DEFECT000025613	Medium	Summary: Trying to Activate a ZoneSet that's about 128K, the AddObjectAttribute() call returns -56 after around one minute. Symptom: Trying to Activate a ZoneSet that's about 128K, the AddObjectAttribute() call returns -56 after around one minute. Customer Impact: Zone propagation time is being enhanced in a future release. Probability: Medium Reported in Release: V4.1.0
DEFECT000025679	Medium	Summary: Right after activated SCC policy, retrieve sec policy through API will fail Symptom: Attempting to retrieve the security policy via the Fabric Access API immediately after activating a new SCC policy will cause the retrieval command to fail. Workaround: Wait several seconds after activating the new security policy before issuing a command to retrieve the security policy. Customer Impact: A simple workaround exists; a fix is targeted for a future Fabric OS release. Reported in Release: V4.1.1
DEFECT000025879	Medium	Summary: Incorrect failover with > 32 zone groups or > 128 devices on a quad during filter recovery Symptom: Some zone groups are lost on a CP failover. Solution: Merge corrected initialization of both cam and group bitmaps from 4.1.x_maint branch. Reported in Release: V4.1.2

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000025944	Medium	Summary: setting fcpProbeDisable will set fanFrameDisable Symptom: When setting fcpProbeDisable to 1 through configure command fcAL.fanFrameDisable will automatically be set to 1. Does not happen in v3.1 Customer Impact: Customer impact is low and workaround is simple, it will be fixed in a future release. Reported in Release: V4.1.0
DEFECT000025989	Medium	Summary: Web Tools shows incorrect "Current" value on the smart sfp. Symptom: The output of sfpshow from the CLI and from Webtools is different. Webtools is displaying an incorrect value for the current value on smart SFPs. Solution: Changes need to be made to the backend to receive the right value. Workaround: Use the command "sfpshow" to see the correct value of current. This is a WebTools display issue. This will be targeted for delivery in a future FabOS release. Customer Impact: This is a WebTools display issue. This will be targeted for delivery in a future FabOS release. Reported in Release: V4.1.1
DEFECT000026068	Medium	Summary: AddSetMember failing to add License key to switch, when 4.1.1 is proxy and other F/W is target Customer Impact: When it is in a mixed environment, use caution in using API to connect: if you use 4.1 as proxy and 4.1 as target, the operation will succeed. 4.2 proxy and 4.3 target succeeds, and 4.3 proxy and 4.2 target succeeds. If API is used to connect to 4.3 as proxy and use 4.2 as target switch, the operation will fail; as is the case with 4.2 using 4.1 as target. Reported in Release: V4.1.1
DEFECT000026115	Medium	Summary: SNMP FW-BELOW Trap for EnvFan is not sent after haFailover. Customer Impact: This issue has been resolved since 4.1.0 release. Close defect as part of defect cleanup. Service Request# RQST00000023588 Reported in Release: V4.0.2

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000033049	Medium	Summary: Webtools Events are using UTC time rather than adjusted timezone time Symptom: Webtools and CLI event time are not the same when the tstimezone is configured. When the tstimezone is not configured then the event times match Solution: Backend should supply a long value that can be used to get the local time. Times are meaningful for an administrator only in his/her domain. Workaround: This defect will be fixed in a later release. Customer Impact: This issue is being investigated and will be addressed in a future Release of Fabric OS. Reported in Release: V4.1.2
DEFECT000033230	Medium	Summary: Webtools Does Not Show Duplicate Entries Contained In Zoning On Switch. Symptom: Webtools Does Not Show Duplicate Entries Contained In Zoning On Switch. Workaround: Deleting one member out of the zone list from the telnet session may resolve the issue. Customer Impact: This is a WebTools display issue. The problem will be resolved in a future release. Probability: Medium Service Request# RQST00000024119 Reported in Release: V4.1.1
DEFECT000033913	Medium	Summary: 156146 Blades Posting Missing From ErrorLog/Eventlog Messsages. Customer Impact: The fix for this problem will generate a large volume of info messages in the error log. These messages will also fill up the burnin log messages on the CP boards which in turn will defeat its intended purpose of recording real errors from the CP. A logging scheme that will satisfy this Defect, and not break the existing burnin requirements for logging will be considered for a future release. Service Request# RQST00000024565 Reported in Release: V4.1.1

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000033947	Medium	Summary: 9830202 Intuit can't set FCIP address on 3900 Service Request# RQST00000024579 Reported in Release: V4.0.2
DEFECT000034257	Medium	Summary: Switch gets into a state where all SNMP queries to ConnUnitEvent table timeout Symptom: When a port bounce (continuous disable/enable of a switch port with a delay) session is running and ITSANM is used to query the connUnitEvent table, all SNMP queries to the switch timeout. If the browser based switch management application is loaded again, it resets the timeout condition and SNMP queries work until we try to read the connUnitEvent table again. Workaround: The problem is not happening any more. The reason could be due to change in the snmp module implementation related to event table (raslog) in 4.4 which might have helped to take care of this problem. Customer Impact: This defect could happen under heavy stress condition with a very large number of error log entries in earlier releases. This defect can no longer be recreated under FOS4.4 Service Request# RQST00000023547 Reported in Release: V4.1.2
DEFECT000034463	Medium	Summary: [Hitachi] The wrong output from the portCfgShow command. Solution: clean up portcfgshow command and related help pages to match other release outputs. Workaround: none. Service Request# RQST00000024864 Reported in Release: V4.2.0
DEFECT000034498	Medium	Summary: zoning Service Request# RQST00000024556 Reported in Release: V4.1.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000034623	Medium	Summary: Missing events (including firmwareUpgrade event) when firmwaredownload with silkworm proxy, SilkWorm 12000 target Symptom: After firmware download to a SilkWorm 12000 switch, an API application does not receive download completion event. Customer Impact: This can only be seen in Brocade Fabric Access API and is a feature enhancement. This will be resolved in a future FOS release. Reported in Release: V4.1.1
DEFECT000035013	Medium	Summary: [preexisting usability] On removing Web Tools license, and later adding it back, an incorrect message is displayed. Symptom: The message displayed when Web Tools license is removed, and later added, is inaccurate. Solution: 1. When web license is absent or expired, all applet windows will be covered with gray panel with error message. User has no interaction, but close windows. 2. The behavior applies to SwitchView, ZoneAdmin, SwithcAdmin, FabricWatch, HaAdmin, NameServer. 3. When switch adds license back, and original session has not been closed. Web Tools will not suppose to behave normally as license present. It will keep showing license absent on the opened windows. User has to relaunch webtools. 4. Corner cases not covered: After license absent, user cannot expect that webtools behave normally. Some components may encounter different exceptions after license missing. There may have exception dialog popped up beside the item1 described screen. User has to ignore those dialog by closing them and close all WebTools windows. Customer Impact: This is a corner case. It is not expected that the user will remove a license he/she has. Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000035168	Medium	Summary: syslogd does not send out the right number of errors to host . Eg. Error#1527 show up (6) on the switch but it only appear once in Sun station. Symptom: The customer will see a different amount of error message from the host perspective as opposed to the switch side. Workaround: None Customer Impact: The extra blank message and the extra info message showed up are side effects of the current design of errlog and linux klogd. FOS 4.4 fixed logging mechanism and this problem can no longer be recreated with the new design. This defect was under test during rc1 (hence open status) so no code changes were required between rc1 and rc2 to close this defect Probability: Low Reported in Release: V4.2.0
DEFECT000035626	Medium	Summary: secmodeenable only report one error from one switch even though there are multiple switches in the fabric have corrupted PKI objects. Symptom: When the secmodeenable fails due to the absence of certificates on multiple switches in the fabric, an error is reported for only one of the switches missing a certificate. Customer Impact: This behavior is a limitation of the current implementation. An enhancement to report all switches lacking certificates is planned for a future release. Once secmodeenable reports that a switch does not contain a certificate, the switch administrator should check all other switches in the fabric to confirm the presence of switch certificates. Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000035962	Medium	Summary: SilkWorm 3250 and SilkWorm 3850: fanshow show OK even if the speed is below the minimum Symptom: If you set the fan threshold below the current fan value, fanshow indicates that the fan is still OK. Solution: In current release, fanshow is an EM command and is independent of Fabric Watch (which is a higher level application above EM) threshold values. Enhancement has been requested for a future release. Workaround: fabricwatch will still generate an error when the rotation is detected below the threshold. Customer Impact: In a future release, basic environmental CLI commands, Webtool dispaly, fabric watch will be synced up. Probability: Low Reported in Release: V4.2.0
DEFECT000036082	Medium	Summary: Zoning db propagation from a switch to the rest of the fabric takes place so slowly that it messes up with API operations. Symptom: Zone DB propagation may seem slow. Workaround: Brocade API will wait for adequate amount of time to let the Zone DB propagation complete. Customer Impact: The zoning DB propagation time taken with this release is the same as in older releases like 4.1.1. However, more enhancements in this area are planned for a future release. Probability: Medium Reported in Release: V4.2.0
DEFECT000036249	Medium	Summary: GATIN returns an accept for a non-existent port wwn Symptom: GATIN will return an accept for a non-existent port in the fabric Customer Impact: This is how the initial implementation of Management Server has been functioning and has not caused any problems in the fieldl. The fix will be implemented in a future release. Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000036328	Medium	Summary: IP address is not recorded correctly in error message of "Security violation: Login failure attempt via TELNET/SSH/RSH. IP Addr: 192.168.44.247" for subsequences login failure from multiple different IP addresses. Symptom: A single security violation error entry is logged when multiple similar violations originating from different IP addresses are detected. Workaround: No workaround for this defect. Customer Impact: This behavior will be changed in a future release to report the IP address for every security violation detected. The current behavior is to omit log entries for similar violations that arrive within a brief timeframe in order to preserve error log storage for other types of events. Reported in Release: V4.2.0
DEFECT000036575	Medium	Summary: Switch panic with out of memory when doing continuously HBA reset. Symptom: errdump shows: 0x25c (fabos): Nov 21 18:56:11 Switch: 0, Critical kSWD-kSWD_GENERIC_ERR_CRITICAL, 1, kSWD: Detected unexpected termination of: "[0]nsd:0'RfP=604,RgP=604,DfP=0,died=1,rt=217363215,dt=38330,to=50000,aJc=217311715,aJp=217295100,abiJc=-430098500,abi Solution: RSCN inter-switch retransimmtion enhancement in a future release has resolved this problem. Customer Impact: This problem is fixed in the next FOS release and was not included in the 4.2.2 due to time to market and severity. Service Request# RQST00000026256 Reported in Release: V4.1.1

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000037135	Medium	Summary: Error SEC-RSENDFAIL, 2, RCS process fails: Bad RCA" message during zoning merge test Symptom: The error "SEC-RSENDFAIL, 2, RCS process fails: Bad RCA" message is reported during a zone merge test. The fabric still forms correctly. Customer Impact: The condition reported is a misleading error message. The error is reported during an intermittent state when the fabric is still forming. Internal logic will retry the failed operation and the fabric still forms correctly. This behavior will be documented in the release notes and in the next revision of the SFOS User Guide. Reported in Release: V4.2.0
DEFECT000037162	Medium	Summary: Ethernet port LEDs for the SilkWorm3250/3850 switch are not shown in the Web Tools Switch View Symptom: In the SilkWorm3250/3850 switch view in Web Tools, no LEDs are shown with the Ethernet Port. Customer Impact: Customers are more concerned with an actual link rather than the speed of the link. This defect will be fixed in a future release. Reported in Release: V4.2.0
DEFECT000037212	Medium	Summary: When discovering a particular switch in a large fabric an ERR_LOGICAL_BUSY is returned Symptom: On a large fabric, when using a v4.x switch as a proxy, an ERR_LOGICAL_BUSY is always returned when discovering one particular switch (dev185) with the API. When using a v3.x or v2.6.x proxy, everything is fine. Rebooting and upgrading firmware did not fix the problem. Solution: No known solution yet. Workaround: Do not attempt to discover a SW3200 running v3.1.1a using API with a v4.x switch as a proxy. Customer Impact: The root cause of this problem is still under investigation. Service Request# RQST00000026735 Reported in Release: V4.1.1

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000037405	Medium	Summary: Upper 15 ports EE monitors change into incorrect values after PID change Symptom: If customer has an EE monitor defined that incorporates the last 15 ports and changes the PID format to "2", the resulting EE monitor will change to an out of range port number. E.g. 7f changes to 8f. Customer Impact: There is an easy workaround for this problem. Customers are not expected to run into this situation and thus the impact is low combined with the workaround, this will be fixed in a future release Reported in Release: V4.2.0
DEFECT000037485	Medium	Summary: SCALABILITY: zone contents between memory and flash end up different. switch will never join in the sec fabric after fastboot. Symptom: switch will never join the security fabric after fastboot. Customer Impact: The problem has only been with random HA failover tests in a large fabric. A simple workaround does exit to correct the problem. We are continuing to look for the right solution to resolve the issue. This will be fixed in a future release. Probability: Medium Reported in Release: V4.2.0
DEFECT000037576	Medium	Summary: API Performance problem in Large Fabric. GetAllObjects from one particular SilkWorm 24000 in the Large Fabric does not return even after 90 minutes. Symptom: API Applications that use GetAllObjects, in a large Fabric with a large number of devices, may observe that this function takes a long time to complete. Customer Impact: The only customer impact is to API applications that use GetAllObjects in a large fabric with large number of devices. Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000037699	Medium	Summary: Firmwaredownload between pre-release builds failed on one of the core chassis (SilkWorm 12000) when there were 21 switches doing firmwaredownload at the same time in 4x30 fabric Symptom: Firmwaredownload failed on one of the core chassis (SilkWorm 12000) when there were 21 switches doing firmwaredownload at the same time in 4x30 fabric Workaround: none Customer Impact: This problem only occurred in a stress (simultaneous firmwaredownload in all switches) test situation in a large fabric. Reported in Release: V4.2.0
DEFECT000037789	Medium	Summary: CP loose its' boot environment variables during run-in. Symptom: Board won't boot all the way if it looses its boot env. Variables. Console output would look like this: The system is coming up, please wait... Unable to read configuration data WARNING: Failed to set EMAC hardware addresses! 1) Start system. 2) Recover password. 3) Enter command shell. Option? 0 Customer Impact: During a factory-only test (runin test) , we have seen an isolated case where the the boot environment variables have been wiped out. A customer never runs this test. Probability: Low Reported in Release: V4.2.0
DEFECT000037843	Medium	Summary: For debugging usage, PortID in the "portlogdump" should refer to the Area number of the "switchshow" when "Extended Edge PID" is set Symptom: run portlogdump, the portid is logical linear port number not area number; Customer Impact: Display problem will be fixed in a future release. Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000037845	Medium	Summary: "Incompatible flow control" warning messages should refer to the "Area number" of the "switchshow" when "Extended Edge PID" (format 2) is set Symptom: Configure 2 switch with different PID format to see the segmentation error message is linear port rather than slot/port or area. Solution: When commands referred to port, we should use slot/port notation; not the logical linear number. Workaround: In switch pid format 2 (Extended Edge PID format), this error message is show as logical linear port, which is different from area number of switchshow. Adds 16 to logical linear port number to match the switchshow area number. Customer Impact: This is a display problem, will be fixed in a future release. Reported in Release: V4.2.0
DEFECT000037866	Medium	Summary: crossporttest -nframes 1000 and failover, got OOPS Symptom: This problem only happens on a SW12k switch when crossporttest -nframe 1000 is executed on switch 1 (does not happen when test is executed on switch 0) issue hafailover, then OOPS occurs on the current standby CP Workaround: When running crossporttest (diagnostic) do not issue the hafailover command. Customer Impact: An unusual combination of commands (Issue a the crossportest diagnostic command, and while the command is running issue the hafailover command) is required to get the problem to occur. It is unlikely that an end user would be running these commands in parallel. Probability: Low Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000037963	Medium	Summary: What is the frame size that spinfab uses the diagnostics is invoked ? Symptom: Our documentation and switch help text does not currently have this information. Solution: Frame size that spinfab uses when the diagnostic is invoked will be documented in a future Release. Workaround: The frame size depends on the amount of buffer credit available on the port. However, there are eight possible frames that can be sent. Especially with trunking groups, all eight are possible frames and are used unless there is extensive traffic running on the link. The payload size of those eight frames are 1024, 12, 8, 1024, 512, 1024, 12, and 1024. This information will be updated in a future reference manual. Service Request# RQST00000027193 Reported in Release: V4.1.1
DEFECT000038022	Medium	Summary: Remove misleading PCI debug message generated during slot scan Symptom: Error message "db_scan_slot: failed to read header type func 0 dev 14 bus 2, ret= -22" observed when powering slot off then back on. Solution: This message occurs when the Drawbridge module fails on a configuration read of the blade's transparent PCI-PCI bridge PCI header type field, which causes a intermediate failure of the scan process. However, the scan process retries the read and eventually succeeds. Therefore, this error message is misleading and unnecessary. Customer Impact: This is a misleading error message. No functional impact. This problem is fixed in the next FOS release and did not make it into the 4.2.2 release. Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000038184	Medium	Summary: Remove manufacturing command references in burnin Solution: The features removed do not effect the tests, nor the test coverage of the existing burnin testing. These features are: 1. Variable length log size 2. Reference clock testing (only avaialble on SW12000 in factory only) 3. Loopback back plane testing mode (SW12000 and SW24000 in factory only) 4. Early yield enhancement data collection tests (SW24000, and SW3850/SW3250) 5. CP mastership toggling (SW12000 and SW24000 factory only) Customer Impact: This does not affect customer operation, it is for factory debug cleanup. Probability: Low Reported in Release: V4.2.0
DEFECT000038352	Medium	Summary: hafailover on SW24k caused port blade vacant , but the status LED on the port blade shows it is in a good state Symptom: reset microswitch or soft reboot CP caused 1 port blade out of FOS controlled Customer Impact: This problem can only come from a blade which is failing intermittently. The blade passed PCI scan on bring up, but on a subsequent warm failover during the early PCI scan, it failed with an isolated bridge indication, and was marked as removed in the PCI attach routine. The current warm recovery logic has a missing check allows a blade to be discovered as bad to end up marked as absent. It should have been marked as faulty, and it's status LED turned on. In either case it would not be used as an operational blade. The message indicating the PCI scan problem is logged on the console and is stored in the nonvolatile message area. Subsequent failovers (warm or cold), or cycling of the ejector switch, should move the blade out of the absent state to faulty or operational depending upon whether or not it fails the next scan. This was a one time failure mode. It was not reproduced. Probability: Low Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000038822	Medium	Summary: Some diag commands under "diaghelp" should be hidden in the "admin" level user Symptom: After fwdl the release build, login as "admin" level user, type "diaghelp", the following diagnostics commands should be hidden: blockcheck, cftest, cptest, fpBTrace, fpDestroy, fpDestroyPLog, fpETrace, fpEnterSymbols, fpPurgePerformance , fpPurgeSymbols, fpSample, fpShowLog, fpShowPerformance, fpShowSymbols , kerneltest, ledtest , serialtest , srctest Solution: Future firmware release will move identified commands to the "admin"level. Workaround: Do not use the following commands: blockcheck, cftest, cptest, fpBTrace, fpDestroy, fpDestroyPLog, fpETrace, fpEnterSymbols, fpPurgePerformance , fpPurgeSymbols, fpSample, fpShowLog, fpShowPerformance, fpShowSymbols , kerneltest, ledtest , serialtest , srctest Customer Impact: This defect does not impair the operation of the switch. It's only effect is to provide extraneous information to the user when accessing help. Since this defect does not alter the operation of the switch no workaround is necessary. This defect will fixed in a future release. Probability: Medium Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000039052	Medium	Summary: On PID format conversion max cfgsize limit is not enforced Solution: First, ambiguous error message, "Switch: 0, Info ZONE-TRANS_ABORT, 4, Zoning transaction aborted - Bad Zone Config" that occurs when a user changes "Core" (1) "Displaced" (2), when the zone db is maxed out will be updated. Also, additional error message will be added for the situation when user changes from "Displaced(2)" to Core (1)", and the zone db is maxed out. Workaround: No known workaround. Customer Impact: Changing from Core to Displaced PID format when zoning database size is near max, results in a non-descript error message. Changing from Displaced to Core PID format results in no error message, however this is not a recommended procedure. This test is only in lab environment. Probability: Low Reported in Release: V4.2.0
DEFECT000039318	Medium	Summary: In a 4x16 fabric with zone db size 35K,the Zone administration window opened from FM does not show all the last two zone members properly. Symptom: Using Fabric Manager 4.1.1, open the zone administration window from the primary FCS switch (12k in this case). Go to the 'config' tab and select the currently enabled config. The "Config Members" on the right hand side doesn't show the last two zone members when the window is maximized and doesn't scroll down also. When the window size is reduced, still the last member can not be seen properly. Customer Impact: It is very hard to reproduce. When the problem happened, the information was insufficient to root cause the problem. A build with extra instrumentation has been run without hitting the problem again. Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000039580	Medium	Summary: "error creating new license file" message in CLI when performing configdownload on 24k Symptom: When user tries to download a config file which has a license entry [Licenses] to a switch which does not have a license file /etc/fabos/license created, this error will show up. "error creating new license file" The operation will succeed anyway. Customer Impact: This problem produces an error message, however the action completes successfully. Message removed in future release. Service Request# RQST00000028011 Reported in Release: V4.2.0
DEFECT000040178	Medium	Summary: EMC H/W OPT 177106 : Slot 10 Faulted and did not recover while running diagnostics during a temperature cycle. Service Request# RQST00000028157 Reported in Release: V4.2.0
DEFECT000040325	Medium	Summary: Critical Error:Post Diag. Stopped, No Longer Transmitting, Counter Stuck; Blade Faulted. Service Request# RQST00000028212 Reported in Release: V4.2.0
DEFECT000040469	Medium	Summary: PID change to 2, segments legacy switches and only reports 1 out of 3 ports affected. Solution: Fix implemented, will be released in future release. Workaround: No known workaround. Service Request# RQST00000028270 Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000040611	Medium	Summary: I/O failure in fabric with Brocade switches running fw 3.0.2c & fw 4.2.0 Symptom: I/O failure in fabric with Brocade switches running fw 3.0.2c & new switches fw 3.0.2c backward compatible with 4.2.0 as listed in the OEM notes I/O failure inside fabric consisting of Brocade 3850 & 3800 switches cascaded together. Path was good for a while, then became offline to the host after some I/O run. This problem was no longer encountered after upgrading from 3.0.2c to 3.1.2_rc1 Is 3.0.2c compatible with 4.2.0? If not, the documentation needs to be changed to reflect this. Complete problem description from SUN and supportshow outputs are attached. Service Request# RQST00000027777 Reported in Release: V4.2.0
DEFECT000040747	Medium	Summary: [help page] Help pages on some commands reference the Silkworm12k in the example section. Service Request# RQST00000028370 Reported in Release: V4.2.0
DEFECT000040786	Medium	Summary: EMC S/W OPT 177484: FM Reports In The Current Status Window Power Supplies Are Not In The Correct Slots; 24K Switch Service Request# RQST00000028271 Reported in Release: V4.2.0
DEFECT000040802	Medium	Summary: (Scalabiltiy) Make cfgactvshow available on all FCS switches Symptom: cfgactvshow can only be executed from the primary FCS Switch. Solution: Make cfgactvshow available on any FCS Switch or restrict cfgshow command only to Primary FCS Switch. Workaround: However user can get the same information from cfgshow command which can be executed from any FCS switch. Reported in Release: V4.3.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000040905	Medium	Summary: Port log "disable" or "enable" entry is not logged in port log when Fabric Watch's PortLogLock alarm trigger is used to log a port log of a port. Symptom: Cannot figure out if port log is locked and nothing is showing up for a particular port by looking at port log dump data. Solution: User needs to know if and when port log is DISABLED (lock) or ENABLE (unlock). Fix available for future release. Reported in Release: V4.3.0
DEFECT000040991	Medium	Summary: When using the bladeDisable or bladeEnable command there is no output to the user to let them know whether the command failed or succeeded. Service Request# RQST00000028457 Reported in Release: V4.2.0
DEFECT000041016	Medium	Summary: If a slot is disabled using bladeDisable command, the slotShow command shows the slot as enabled, this may lead the user to incorrectly assume that the command failed. Service Request# RQST00000028464 Reported in Release: V4.2.0
DEFECT000041475	Medium	Summary: GUI HA Admin Fails To Indicate The Sync State Of CPs. Service Request# RQST00000028604 Reported in Release: V4.2.0
DEFECT000041567	Medium	Summary: SW3900 saw ENC_ERR when no cable plugged in on 4.0.2; SW3250/3850 saw same issue with 4.2 Symptom: Enc_out errors increasing on unused ports. Service Request# RQST00000027602 Reported in Release: V4.0.2

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000041678	Medium	Summary: Ethernet port failed to send MAC address after link negotiation Symptom: Ethernet interface hang. Switch could not send any packets after IP negotiation and lost connectivity. Solution: Soft reset of the EMAC when RXDE errors occurred. This eliminated the RX FIFO overflows that were occurring with the packet generator traffic and which resulted in hangs of the EMAC. Workaround: Doing an ipaddrset command clears the condition. Service Request# RQST00000028673 Reported in Release: V4.2.0
DEFECT000041851	Medium	Summary: "Do not power cycle" message does not appear in WebTools during firmwaredownload Symptom: firmwaredownload from command line will give the message "Do not power cycle" while the boot prom is being updated. SUN has discovered that the boot prom will be corrupted if the switch is power cycled during this time, and be unable to boot. firmwaredownload using WebTools does not give this message. It needs to be added to the firmwaredownload process in WebTools. We have verified this with a switch in the support lab. Service Request# RQST00000028725 Reported in Release: V4.2.0
DEFECT000042176	Medium	Summary: cfgShow page separator does not exist in 4.x code Symptom: With the 3.1.x code, when you run a "cfgshow" via a telnet session, it pauses the output a screenful at time. With the 4.x code, this is not the case. Workaround: "cfgShow | more" will give you the desired results. Customer Impact: The feature requested can be obtained by a simple workaround and is more flexible than forcing a page separator and there is no plan to fix it. Service Request# RQST00000028870 Reported in Release: V4.1.2

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000042413	Medium	Summary: Commands fanShow and sensorShow do not report FW threshold levels accordingly, should show below-minimum! Customer Impact: In a future release, basic environmental CLI commands, Webtool dispaly, fabric watch will be synced up. Reported in Release: V4.1.2
DEFECT000042433	Medium	Summary: SCALABILITY: (2 domain) Eth1 interface is not through (RX counter on CP1 is 0) which cause both CP cannot be sync up. Symptom: When doing chassisconfig 2 on the 24K switch, occasionally, after CP1 was rebooted twice and after CP1 came back, HA was out of sync. Solution: Bringing the interface down and up on CP0, seem to have solved the problem. Will continue to investigate. Reported in Release: V4.3.0
DEFECT000042504	Medium	Summary: SCALABILITY: 0x3 (fabos): Switch: 0, Warning BLOOM-TRNK_SLV_DWN, 3, S7,P73: Trunk slave port 73 goes OFFLINE in trunk group [74 75 73] during zone propagation Symptom: When doing zone propagation from one of edge on 3900, on core and edge, there was message "Warning BLOOM-TRNK_SLV_DWN" showing up. When switchshow on that port is checked, there is no indication on port offline. Solution: Currently being investigated. Workaround: No known workaround. Reported in Release: V4.3.0
DEFECT000042749	Medium	Summary: wwnhsclient and wwnhserver - can run in admin level, but marked as root level in CLI DB - which is correct?? should these two commands have help pages?? Symptom: wwnhsclient and wwnhserver command info is inconsistent. Solution: Determine whether wwnhsclient and wwnhserver should be in admin or root. Document properly. Behavior and documentation should be consistent. Reported in Release: V4.3.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000042802	Medium	Summary: Running secfcsfailover script overnight will have memory leak on the switch Symptom: Possible that one might see a memory leak running test similar to our running script secfcsfailover between silkworm 24000 and 3900. Solution: Currently under investigation. Workaround: None known. Reported in Release: V4.3.0
DEFECT000042838	Medium	Summary: wrong GE_PT sent from Meteor Symptom: When GE_PT is sent from 3900 to 24000, it is the extended format header GE_PT. The 3900 expects the same format GE_PT to come back, but for some reason it does not. Solution: Currently under investigation. Workaround: No known workaround. Reported in Release: V4.3.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000042846	Medium	Summary: mismatching between switch CLI and Command DB for following man pages Symptom: no help texts for following commands: configcommit configsslnoti diagClearError errloginfo ficoncupset ficoncupshow ficonhelp ficonMode fstovset generationset pdcp pdex perfcmd portlognvdisable portlogportdisable portlogportenable portLogPortSet portlogportshow ps_dbgcmd ps_dump pshcshow ptDataShow ptPhantomShow sbtst servicestat servicestatstart servicestatstop sysc_dprintf systemtest timelineget voltageMargin Solution: Determine which commands should be available to the user and provide help texts. Reported in Release: V4.3.0
DEFECT000042893	Medium	Summary: Webtool's Nameserver Does Not Display The Storage Array Vendor's Name Under Device Name. Service Request# RQST00000029063 Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000043050	Medium	Summary: FW-FRU_ABSENT is not reported until CP is re-inserted. Symptom: 1. Fabric Watch does not generate a FRU_ABSENT message after active CP is pulled out. 2. Fabric Watch generate FRU_ABSENT when active CP is inserted immediately or after a couple of minutes. Solution: The FRU monitoring implementation in FW was improved in 4.4 and fixed this issue Workaround: Use the slotshow command to find about whether a CP has been removed. Customer Impact: There should no customer impact since the defect has been fixed in v4.4 RC1 release. Probability: Low Service Request# RQST00000028586 Reported in Release: V4.2.0
DEFECT000043137	Medium	Summary: SCALABILITY: ECC Corr Err: BK1, Odd wd ln 1 during reboot -f after firmwaredownload with -s -f Symptom: Following successful firmware download, and reboot -f, the following error message may be seen: "ECC Corr Err: BK1, Odd wd ln 1" Solution: Currently under investigation. Workaround: None known. Reported in Release: V4.3.0
DEFECT000043160	Medium	Summary: coldstart trap is not at all received on meteor. Symptom: Customer may encounter coldstart trap not being received on 24k with all types of reboot methods. Solution: Currently believed fixed. Carrying forward to future release to verify before closing. Reported in Release: V4.3.0
DEFECT000043165	Medium	Summary: cpstatus changed and fruhistory traps are not generated while doing hafailover on 24k. Solution: Believe may be fixed. Carrying forward to future release to be verified. Reported in Release: V4.3.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000043212	Medium	Summary: Reload of switch configuration causes port to go offline Symptom: If you set almost all the ports on the side of a 12K to be persistent disable and then issue a switch reboot, upon the switch coming back up to it's normal operational state, it was identified that all the persistently disable port LED are no long flashing AMBER. Instead, they remain steady amber. Any changes to the ports from persistent disable back to enable will not reset the steady amber light. Solution: Currently under investigation. Workaround: None known. Service Request# RQST00000028942 Reported in Release: V4.1.1
DEFECT000043323	Medium	Summary: [help page] typo in the diaghelp man page Symptom: typo in the diagHelp man page in the description section Customer Impact: None. This is a documentation item. Reported in Release: V4.3.0
DEFECT000043342	Medium	Summary: Fwdl on Terminator - EMD/SNMPD panic during commit Symptom: When doing a firmware download on a 3900, EMD and SNMPD panic may occur, when upgrading firmware from 4.1x to 4.2x Solution: Solution has two components, and which are currently being worked and are targeted for a future release: 1. The EM owners shall fix the NULL pointer to avoid an emd panic regardless of the recovery failure or success. 2. The fabos startup infrastructure shall deal with a timeout or failure of recovery during a switch bootup or failover. A right message shall be printed/logged to indicate this recovery error and instruct a user to collect all information and reboot. A right place to have this enhancement is the sysctrld. Workaround: None known. Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000043444	Medium	Summary: FM: Login from FM to 4.3.0_main_bld27 switch with deleted user accnt succeeds if this account was previously used from FM Symptom: After deleting user accounts via Fabric Manager, you are still able to login into switch from FM using deleted user accounts. Solution: Currently under investigation. Workaround: Delete user accounts via CLI or Web Tools. Reported in Release: V4.3.0
DEFECT000043528	Medium	Summary: Add license fails with certain proxy-target combinations if the license key already exists in target switch Symptom: Add license fails with certain proxy-target combinations if the license key already exists in target switch. Reported in Release: V4.3.0
DEFECT000043619	Medium	Summary: SCALABILITY: Error message "0x2b6 (fabos): Switch: 1, Error FABRIC-FAB_ME_ERROR, 2, Managment Entity IPC error, -984, to inform fabric is stable. " shown on the console when switchcfgtrunk 0 executed. Symptom: When executing switchcfgtrunk 0, the following error message may be seen on the console: 0x257 (fabos): Switch: 0, Error FABRIC-FAB_ME_ERROR, 2, Managment Entity IPC error, -984, to inform fabric is stable. Solution: Fix checked in and targeted for next release. Workaround: None known. Reported in Release: V4.3.0
DEFECT000043736	Medium	Summary: IU memory holding: about 1000 active IUs are not being released in the time period window monitored, eventually the memory is released. Customer Impact: rtwr has been changed with a larger timeout value and no iu holding in kernel. Due to the risk of the change, it will be only fixed in a future release, and not back ported to a patch branch. Probability: Low Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000043799	Medium	Summary: SCALABILITY: 0x23b (fabos): Switch: 0, Critical SCN-SCNQ_OVERFLOW, 1, SCN queue overflow for process webd was shown up sometimes Symptom: When running switchdisable; cfgclear; cfgdisable; switchenable on all core switches (2 - 3900s and 1 - 24K), an error message: 0x23b (fabos): Switch: 0, Critical SCN-SCNQ_OVERFLOW, 1, SCN queue overflow for process webd occasionally occurs on the core 24K switch. Solution: Currently under investigation. Reported in Release: V4.3.0
DEFECT000043880	Medium	Summary: Update supportshow, supportshowcfgdisable, and supportshowcfgshow man pages Symptom: In the supportShow "Description" section, need to change the third sentence currently reads, "These commands are organization by groups..." to "These commands are organized by groups..." In supportShowCfgDisable, the "Synopsis" section does not include the perfmon and ficon operands in the "Operands" section. Customer Impact: This is a documentation error and will be corrected in the future release. Reported in Release: V4.3.0
DEFECT000043939	Medium	Summary: Unable to change the proxy switch IPGateway from API Symptom: Established a session to a 4.x switch successfully. Then change the proxy IPGateway by calling AddAttributes(), the IPGateway value is not changed via examing the telnet or by calling checking the IPGateway value. The value should be changed. Reported in Release: V4.3.0
DEFECT000043952	Medium	Summary: SCALABILITY: (stress) CP will reset if 100Mbps traffic is transmitted on ethernet port. Symptom: The CP resets while transmitting line speed (100Mbps) traffic into one of ethernet port. Customer Impact: This is a stress test condition and does not happen in a normal environment. Reported in Release: V4.3.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000044001	Medium	Summary: unable to execute "quietMode" under user level login Symptom: Unable to execute "quiteMode" under user login. According to help page, user should be able to display the current mode. Solution: simply updates the help page to reflect the correct access level. Workaround: none. Reported in Release: V4.3.0
DEFECT000044500	Medium	Summary: Sec Fabric: Unable to Apply or Cancel changes made to FWClassArea class when proxy is non-Primary, and modifying local switch. Symptom: Sec Fabric: Unable to Apply or Cancel changes made to FWClassArea class when proxy is non-Primary, and modifying local switch. One should be able to modify local switch when proxy is non-Primary FCS. Steps to reproduce: 1. Login to non-primary switch 2. Encode FWClassArea OID 3. Call GetObjectTemplate and ModifyObject. 4. Call AddAttributes to Apply or Cancel the changes. Actual Results: AddAttributes returns -59. Customer Impact: This is API related. Reported in Release: V4.3.0
DEFECT000044643	Medium	Summary: ASSERT - Failed expression: NULL != pubk_buf followed by secd terminated. Symptom: The SilkWorm 3850 captured an "ASSERT - Failed expression" and Call Backtrace followed by secd unexpected termination after doing following steps: 1. On a SilkWorm 24000 switch, type secmodeenable --quickmode 2. before above command completed, type switchdisable then switchenable on another telnet session of same switch 3. From the SilkWorm 3850 switch (connected to a SilkWorm 3900 which connects to a SilkWorm24000 switch in turn), the ASSERT error shown up. Reported in Release: V4.3.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000044673	Medium	Summary: WT zone admin: refresh icon keeps flashing when user saves local work instead of refreshing from switch Symptom: WT zone admin: refresh icon keeps flashing when user saves local work instead of refreshing remote zoning changes from switch. Reported in Release: V4.3.0
DEFECT000044674	Medium	Summary: WT zone admin edit/delete and edit/replace WWN don't work for WWNs added with edit/add WWN Symptom: WT zone admin edit/delete and edit/replace WWN don't work for WWNs added with edit/add WWN Reported in Release: V4.3.0
DEFECT000044698	Medium	Summary: create an user defined account using userConfig command, after firmwaredowngrade to v4.2.0, still able to login with this user defined account Symptom: create an user defined account using userConfig command, after firmwaredowngrade to v4.2.0, still able to login with this user defined account Reported in Release: V4.3.0
DEFECT000044728	Medium	Summary: Standby CP getting "Failed expression" error in rcs_ha.c Symptom: The problem happens intermittently. The last time this problem happens when both CPs are rebooted almost at the same time. A message showed up on standby CP console. The end result is that standby CP cannot sync up with the active CP. Reported in Release: V4.3.0
DEFECT000044731	Medium	Summary: create user defined account using the userconfig cmd, firmwaredowngrade to v4.2.0 then firmwareupgrade back to v4.3.0. After the upgrade, the user defined account does not exist Symptom: create user defined account using the userconfig cmd, firmwaredowngrade to v4.2.0 then firmwareupgrade back to the beta release of v4.3.x. After the upgrade, the user defined account does not exist. Reported in Release: V4.3.0
DEFECT000044768	Medium	Summary: trapReg mib variable is giving trap recipients details for SNMPv1 alone. it has to be implemented for SNMPv3 also. Symptom: trapReg mib variable is giving trap recipients details for SNMPv1 alone. It has to be implemented for SNMPv3 also. Reported in Release: V4.3.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000044774	Medium	Summary: After disabling Port Log through API and going to telnet session, doing portLogClear will enable port log ! Symptom: After disabling Port Log through API and going to telnet session, doing portLogClear will enable port log. Reported in Release: V4.3.0
DEFECT000044777	Medium	Summary: Application 'evmd'(pid 890) got exception 11 and SWD panic on evmd occurred right after coredump Symptom: Switch panic due to evmd got exception 11 caused by access to data structure without protection. Solution: Added mutex protection to data structure in API_rpcd area. Reported in Release: V4.2.0
DEFECT000044787	Medium	Summary: illegal HBA registration Symptom: HBA is allowed to register even though the originating port is not in the HBA's registered port list. Reported in Release: V4.3.0
DEFECT000044929	Medium	Summary: Heavy stress on the CUP port results in IFCCs in overnight run Symptom: When running the test program from the mainframe under heavy stress conditions (multiple LPARs, multiple paths, etc), IFCC errors are observed on the Host. The Channel sends ABTS to a CCW chain after it has timed out waiting 2 seconds for a response. There have also been missing interrupts observed under the same conditions. Reported in Release: V4.3.0
DEFECT000045014	Medium	Summary: WebTools SID/DID predefined window display "cannot open SID/DID:null" message Symptom: User will see "Failed to load SID/DID Performance Graph: null". In addition, a user could potentially see a maximum graph limitation message when there aren't any graphs. Reported in Release: V4.3.0
DEFECT000045024	Medium	Summary: device name not displayed in NS in webtools Service Request# RQST00000028983 Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000045053	Medium	Summary: https to remote switch cause webtools hangs Symptom: Using https to access a 4.2.x platform switch, and access another remote 4.2.x switch from webtools, webtools get stuck or it take long time to get into the remote switch. Reported in Release: V4.3.0
DEFECT000045059	Medium	Summary: invalid SSL certificate files cause "secure RPCd is disabled" (meaningless) Symptom: Secure RPCd is not supported on this release, but when a invalid SSL certificate file is detected, webd still print an error message: "Warnning RPCD-CERT_ERR2, 3, Invalid certificate file, secure rpcd is disabled" which is not applicable. Customer Impact: See Symptom. Reported in Release: V4.3.0
DEFECT000045067	Medium	Summary: An error occurs on a switch in the secured fabric, however SwitchSecStatus of switch object shows OK; status should be SWITCH_STATUS_SEC_ERROR Symptom: This is an API-related error. 1. At switch side, there are errors in the switches in the secured fabric and are reflected correctly when issuing "secFabricShow" command. 2. At API side, GetObjects on Switch object does not reflect the correct status (it shows as OK). SwitchSecStatus shows SWITCH_STATUS_OK. Customer Impact: See Symptom. Reported in Release: V4.3.0
DEFECT000045230	Medium	Summary: FM: Enable sec.mode via wizard fails if one of chassis switches is not populated with ports Symptom: When enabling secure mode via Fabric Access API on fabric that contains 2 domain switch, it may fail with error -17 if only one of domains is on the fabric and it is either Primary FCS or backup FCS switch. Note: It succeeded if it is a non-FCS switch but then switches segmented due to security parameters incompatibility. Solution: Root cause has been determined, fix targeted for a future release. Workaround: Secure mode on the fabric with dual-domain meteor switch can be enabled from CLI, or, move one blade with ports to another switch, so both switches will be populated with ports. Reported in Release: V4.3.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000045324	Medium	Summary: NSD panic in deleting timer. Symptom: In a fabric of mixed 16 different type of switches (core-edge) design, panic occurred either during power cylce or reboot process using one of the following procedure: 1. Power cycle all switches with diagenablepost active -Invoke diagenablepost in all switches -Power off all switches wait for 10 minutes -Power on all switches 2.Reboot all switches simultaneously with diagenablepost active -Invoke diagenablepost in all switches -Reboot all switches simultanously Solution: Fixed a NSd memory corruption in the case that standby could try to delete a timer which doesn't exist Reported in Release: V4.2.0
DEFECT000045360	Medium	Summary: SCSI Frame sent prior to target prior to ACC of FLOGI frame for target. Symptom: When creating a new hardware based wwn group for one host, some remaining hosts lose connectivity and I/Os are rejected with certain storage arrays. This can be reproduced simply by creating a new hardware wwn group while other host I/O is taking place. Solution: Changes to disable port Tx when a FLOGI is received on F-port, right before we set up the routing table. Port Tx will be re-enabled when we send out the first frame from embedded port on an active F port where port Tx was disabled. Prevent frames from leaking through switch during the window after receipt of FLOGI and before sending FLOGI Accept. Workaround: none from our switch. Service Request# RQST00000029919 Reported in Release: V4.1.1

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000045370	Medium	Summary: In Web Tools the Cancel button in Reset Allegiance dialog still performs Reset Allegiance function Symptom: When executing a Web Tools command to modify configuration data on the switch and the allegiance is owned by the Host Program, a Reset Allegiance dialog pops up. When Cancel is selected in the pop-up to cancel the Reset Allegiance operation, the operation occurs anyway. Solution: Change the Cancel button handling. Reported in Release: V4.3.0
DEFECT000045481	Medium	Summary: Currently setting monitors is not checking for duplicate entry. i.e.. if Matrixmap has ' 1' corresponds to an initiator/target pairs .....say (a,b) & (b,a) , it's observed that monitors are being set on both ports ,if resources are available for both Symptom: When setting monitors (for initiator/target pairs), duplicate entries may occur. Solution: Currently under investigation. Workaround: No known workaround. Reported in Release: V4.3.0
DEFECT000045552	Medium	Summary: FCIP issue with WWN zoning Symptom: When switch was zone using WWN, with three machine configured with IP over FC connected to the switch . When moved one of the switch port to another port on the blade that IP for the machine would stop working. Solution: WWN zoning setup no longer solely depends on device PLOGIN when device on line/offline. Service Request# RQST00000030087 Reported in Release: V4.1.2
DEFECT000045605	Medium	Summary: Fabric Watch reporting 739 Gigabytes per second Solution: RX and TX is given to FW in Bytes: the user is presented with the percentage of bandwidth used. Customer Impact: This is fixed in a future FOS release. Service Request# RQST00000029821 Reported in Release: V4.1.2

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000045671	Medium	Summary: A zone was created on a fabric and the zone was not exported through router Service Request# RQST00000029764 Reported in Release: V4.2.0
DEFECT000045713	Medium	Summary: FSSME should take on default values if fssme.conf file is corrupted or not present instead of preventing switch from bootup Symptom: Switch fails to bootup with following error message: 0x24b (fabos): Switch: 0, Critical FSSME-ERROR, 1, Internal Error: FSS port missing FSSME abnormal exit memain.c 122 Solution: If fssme.conf is corrupted, use default values instead of exiting. Customer Impact: Switch fail to bootup when configuration file is corrupted or not present, this will be fixed in a future release. Reported in Release: V4.1.0
DEFECT000045807	Medium	Summary: FM: Cryptic Error message showing up in Events table; needs to clearly indicate why the error occurred Symptom: A cryptic error message shows up in Fabric Manager Event log: "Error in function: demux_ipccb() msg:switchFmsSetRouting() failed=-1" Solution: The FICU daemon prints out an errlog message whenever it encounters an IPC call failure. This message is what was designated as cryptic. This change hides the message so that it is not displayed on the console, yet it is still stored on the NV errlog. This is ok, since the IPC failure is more of an internal error message rather than one meant for the user. Reported in Release: V4.3.0
DEFECT000045822	Medium	Summary: When number of corefiles reached limitation (10) on a switch, old corefiles should be remove to make room for new corefiles. Symptom: When number of corefile on the switch reaches limitation, no new core file will be saved. Workaround: Remove old corefiles on system manually. Customer Impact: This defect will be fixed in a future release. Reported in Release: V4.1.1

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000046020	Medium	Summary: Trunk master changed event is not received if silkworm is proxy Reported in Release: V4.3.0
DEFECT000046037	Medium	Summary: Host Failed to Write File to Switch -- GCSGID field in Read Configuration Data is incorrect Symptom: MVS can't write a file to the switch. In the read configuration command, the GCSGID field should be set to 0x02B9 according to the CUP spec. Solution: Set GCSGID in Read Configuration Data to 0x02B9 as per CUP spec. Reported in Release: V4.3.0
DEFECT000046382	Medium	Summary: Time scale in performance graph Symptom: "Time in Minutes" scale is wrongly labeled. 5 mins, 10 mins, 15mins Solution: Time scale in WT Performance line graph is wrong. Correct it by showing the right time. Customer Impact: This is fixed in a future release. Service Request# RQST00000030582 Reported in Release: V4.2.0
DEFECT000046860	Medium	Summary: MSD core dumps on overnight IRNDUP run Symptom: During overnight stress tests on the CUP port, Interface control checks were observed on the mainframe. Reported in Release: V4.3.0
DEFECT000046925	Medium	Summary: WT: FM needs to show switch name in PDCM table that is open from Port Address Config -> Active menu Solution: Add switch name to PDCM dialog title, Avoid the replicate columns when refresh Reported in Release: V4.3.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000047021	Medium	Summary: In Web tool pop up window for Frus, GUI displays wrong switch type information. Symptom: Web Tool pop-up windows for Power, Temp, and Fan does not display the proper switch type. When these buttons are clicked, the pop-up window's title displays "Detailed ... States for Silkworm12000" while the switch is of another silkworm product model. Solution: For chassis switch, FRUs belong to chassis and is shared between two domains. Showing switch name to FRU window title does not make sense. So it's changed to uses chassis name to identify FRU windows. All FRUs windows: Fan, Power, Temp show Chassis Name on Window Title; Other windows: Event, Port Info, Switch Info, Switch Status, Perf, Admin, Watch show Switch Name on Window Title. For pizza box switch, WebTools always shows switchname to those FRU windows. Service Request# RQST00000029894 Reported in Release: V4.2.0
DEFECT000047025	Medium	Summary: Refresh button in Port Connectivity adds additional set of ports in the column display Solution: Add switch name to PDCM dialog title, Avoid the replicate columns when refresh Reported in Release: V4.3.0
DEFECT000047083	Medium	Summary: ipaddrset generates segmentation error when set hostname too long. Symptom: When change switch name via ipaddrset, gets a "Segmentation fault" error message when the name is beyond 16 bytes. Solution: For the cli command ipaddrset, validate the input hostname length before accepting. Service Request# RQST00000030814 Reported in Release: V4.2.0

Defects Closed Since Last GA Release		
Defect ID	**Severity**	**Description**
DEFECT000047668	Medium	Summary: Fan, Temp and Power buttons shows no data if FabricWatch license is not installed. Symptom: Fan, Temp and Power buttons on WebTools do not work if FabricWatch is not installed on a switch. Solution: If fabric watch license is not installed, webtool will get data from EM module directly. Service Request# RQST00000031247 Reported in Release: V4.2.2
DEFECT000049909	Medium	Summary: After switch install, thrid party I/O Module management software did not show the last letter of a patch revision number. Symptom: Vital Product Data (VPD) will not show software revision suffix when doing a install of a "patch" release. Solution: Add the version suffix to the release file during factory install. Workaround: Execute a firmwaredownload to recreate the release file. Customer Impact: The VPD data will show incomplete firmware version string when a patch release is installed. Reported in Release: V4.2.1