Brocade Fabric OS v3.2.1

GA Release Notes v1.1

December 23, 2005

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v3.2.1 GA Release Notes v1.0	First release.	November 4, 2005
Brocade Fabric OS v3.2.1 GA Release Notes v1.1	Additional Important Note added regarding Performance Monitoring.	December 23, 2005

TABLE OF CONTENTS

About This Release

Fabric OS v3.2.1 is a maintenance release containing fixes to a number a number of defects found since the release of Fabric OS v3.2.0. Aside from these changes, this maintenance release includes the same feature set as the Fabric OS v3.2.0 release.

Overview

Fabric OS v3.2.0 contains significant enhancements in the areas of Fibre Channel long-distance support, scalability, and manageability, to name a few. In addition, several improvements since the release of Fabric OS v3.1.3 have been incorporated in this release. Major new features include:

- Additional support allows a switch running Fabric OS v3.2.0 to recognize a SilkWorm Multiprotocol Router Model AP7420 connected to the fabric

- Updated security enhancements:

    o RADIUS

    o DH-CHAP authentication

- Brocade Fabric Watch and Advanced Web Tools usability enhancements

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 v3.2.1 supports SilkWorm 3200 and 3800 switches.

Technical Support

Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To assist your support representative and 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
    - **supportShow** command output
    - Detailed description of the problem and specific questions
    - Description of any troubleshooting steps already performed and results

2. **Switch Serial Number**

    The switch serial number and corresponding bar code are provided on the serial number label, as shown here.

    FT00X0054E9

    The serial number label is located as follows:
    - SilkWorm 3200 and 3800: Back of 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 v3.2.1 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. For a list of standards conformance, visit the following Brocade web site:

http://www.brocade.com/sanstandards

Important Notes

This section lists information you should be aware of when running Fabric OS v3.2.1.

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 and which have not reached their EOL. Brocade recommends using the *latest* software release versions to get the most benefit out of the SAN.

For a list of the effective end-of-life dates for all versions of Fabric OS, visit the following Brocade Web site:

http://www.brocade.com/support/end_of_life.jsp

Standalone Switches, Directors, & Routers	General Compatibility
SilkWorm 2xxx Series	2.6.1 or later
SilkWorm 3200, 3800	3.1.2 or later
SilkWorm 325x, 385x, 3900, 12000, 24000	4.2.0 or later
SilkWorm 4100	4.4.0a or later
SilkWorm 200E, 48000	5.0.1 or later
SilkWorm Multiprotocol Router AP7420	7.3.0 or later
OEM-Specific Embedded Switches	**General Compatibility**
SilkWorm 3000	3.1.2 or later
SilkWorm 3016	4.2.1 or later
SilkWorm 4012	5.0.0 or later

General

The major features incorporated in Fabric OS v3.2.1 are summarized in the following table.

Category	Feature	Release
Manageability	Advanced Performance Monitoring - ISL monitoring (CLI only)	v3.2.0, v4.4.0
	Fabric Watch enhancements	v3.2.0, v4.4.0
	Export performance data	v3.2.0, v4.4.0
Security-Related	RADIUS support	v3.2.0, v4.4.0
	Multiple user accounts	v3.2.0, v4.4.0
	SSL/HTTPS support	v4.4.0
	SNMPv3 support	v4.4.0
	DH-CHAP authentication (switch-switch)	v3.2.0, v4.4.0
	SAN Gateway security	v3.2.0, v4.4.0
Long-Distance Enhancements	Trunking over extended fabrics (SilkWorm 3200, 3250, 3850, 3800, 3900, 12000, 24000 (all Bloom-ASIC-based platforms) is only supported at 2 Gbit/sec speed, as follows: • four links at 10 km @ 2 Gbit/sec per trunk group • three links at 25 km @ 2 Gbit/sec per trunk group • two links at 50 km @ 2 Gbit/sec per trunk group When configuring an Extended Fabrics trunk, make sure that the *vc_translation_link_init* option is set to 1 (enabled). This option can be set using the **portCfgLongDistance** command. If this option is disabled on a port, the port will not participate in a trunk; instead, it will come up as an individual Lx_Port.	v3.2.0, v4.4.0
MPRS Enhancements	Max Hop Count (FC Router) – CLI only	v3.2.0, v4.4.0
	WAN_TOV (FC Router) – CLI only	v3.2.0, v4.4.0
Scalability	Support for 1280 total ports and 34 domains with security enabled	v3.2.0, v4.4.0
Usability Improvements + RFEs	Security Management – enable/merge 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

Other Notes

The tables below list other important information you should consider about the Fabric OS v3.2.1.

Fabric OS Area	Description
Performance Monitoring	On Fabric OS v3.2.x, with only a single Arbitrated Loop Physical Address (ALPA) on a loop port, the PortShowAlpaCrc CLI command fails with error message "invalid argument." Also, with other interfaces such as FabricWatch, the CurVal of alpaPerfCRC does not change from 0 percent. Work Around: Specify port number and ALPA number as input in the single ALPA case. If there are multiple ALPAs on the loop port, there is no problem displaying each ALPA CRC

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://www.mozilla.org/releases/mozilla1.6/

- **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 2.6.x versions, no warning message is displayed.

   Workaround: The Netscape browser is not supported by Web Tools. However, if you must access the Switch Admin module from a Solaris operating system on a Fabric OS v2.6.x switch, use the Netscape v4.7.7 or later browser.

- Two Domain/Four Domain Fabric Licensing

   If your fabric includes a switch with a license for a limited number of switches in the fabric and the fabric exceeds the switch limit indicated in the license, Web Tools allows a 45-day "grace period" in which you can still monitor the switch. However, Web Tools will display warning messages periodically.

   These messages warn you that your fabric size exceeds the supported switch configuration limit and tells you how long you have before Web Tools will be disabled. After the 45-day grace period, you will no longer be able to launch Web Tools from the switch with the limited switch license if that switch is still exceeding the switch limit. Two domain/four domain fabric licensing is applicable only to 2 Gbit/sec switches.

- Advanced Web Tools browser, operating system, and Java Plug-in support is updated for Fabric OS v4.4.0. The following table identifies the supported browsers, operating systems, and Java Plug-ins for this release.

Priority	OS	Browser	Plug-in
1	Windows 2000	IE 6.0	1.4.2_03
2	Windows XP	IE 6.0	1.4.2_03
3	Windows 2003	IE 6.0	1.4.2_03
4	Solaris 2.9	Mozilla 1.6	1.4.2_03
5	Red Hat Linux 9.0	Mozilla 1.6	1.4.2_03
6	Solaris 2.8	Mozilla 1.6	1.4.2_03

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

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.
Firmware: Fabric OS v2.6.x **Operating System:** Solaris **Browser:** Mozilla	**Issue**: The Switch Admin does not launch correctly. **Workaround:** The Netscape browser is not supported by Web Tools. However, if you must access the Switch Admin on a switch running Fabric OS v2.6.x from a Solaris operating system, use the Netscape 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**: When accessing the Switch Admin, Zoning, Fabric Watch, or High Availability Admin, the browser might crash. **Workaround**: The Netscape browser is not supported by Web Tools. However, if you must access the Switch Admin, Zoning, Fabric Watch, or High Availability Admin from a Solaris operating system, use the Netscape 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 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.
	Issue: When trying to perform end-to-end monitoring (Brocade Advanced Performance Monitoring) on a SilkWorm 24000 or SilkWorm 3250, the SilkWorm 24000 or SilkWorm 3250 will be displayed as a 16-port switch. **Workaround:** For a SilkWorm 3250, ignore the extra ports. For a SilkWorm 24000, use a launch switch running Fabric OS v4.2.0 or later to perform end-to-end monitoring on the switch.
	Issue: When trying to perform zoning on a SilkWorm 24000 or SilkWorm 3250, the SilkWorm 24000 or SilkWorm 3250 will be displayed as a 16-port switch. **Workaround:** If you are running Secure Fabric OS, select a switch running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later as the primary FCS switch. If you are not running Secure Fabric OS, use a launch switch running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later to perform zoning on the switch.

Launch Switch Environment	Problems
Firmware: Fabric OS v 2.6.2, 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:** The Name Server table will not display properly for a switch running firmware versions prior to Fabric OS v2.6.2, v3.1.2, or v4.2.0. **Workaround:** If secure mode is enabled, select a switch running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later as the primary FCS switch. If secure mode is not enabled, use a launch switch running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later to access the Name Server table 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**: Netscape is not a supported browser for switches running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later. Use Mozilla browser 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 the Fabric View, the browser might crash. **Workaround**: Use a launch switch that runs Fabric OS versions v2.6.1, v3.0.x, or v4.0.x or later, so that you can use Switch Explorer (not Fabric View).

Documentation Updates

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

The most recent Fabric OS product manuals are available on Brocade Connect:

> *http://www.brocadeconnect.com/*

The Fabric OS v3.1.0 documentation set supports Fabric OS v3.2.0, supplemented with the *Brocade Fabric OS Documentation Addendum*, publication number 53-0000605-02. With the exception of the following three documents, you should use the Fabric OS v3.1.0 document set and the *Brocade Fabric OS Documentation Addendum* for Fabric OS v3.2.0 documentation support:

- *Brocade Fabric OS MIB Reference Manual* (53-0000521-08)
- *Brocade Secure Fabric OS Quick Start Guide* (53-0000352-04)
- *Brocade Secure Fabric OS User's Guide* (53-0000526-04)

The following Brocade Fabric OS v3.1.0 publications are represented in the *Brocade Fabric OS Documentation Addendum*.

Document Title	Publication Number
Brocade Advanced Performance Monitor User's Guide v3.1.0/4.1.0	53-0000514-02
Brocade Advanced Web Tools User's Guide v3.1.0	53-0000503-02
Brocade Advanced Zoning User's Guide v3.1.0/4.1.0	53-0000523-02
Brocade Diagnostic and System Error Reference User's Guide v3.1.0	53-0000511-04
Brocade Distributed Fabrics User's Guide v3.1.0/4.1.0	53-0000516-02
Brocade Fabric OS Procedures Guide v3.1.0	53-0000501-02
Brocade Fabric OS Reference v3.1.0	53-0000500-02
Brocade Fabric Watch User's Guide v3.1.0	53-0000504-02
Brocade ISL Trunking User's Guide v3.1.0/4.1.0	53-0000520-02

SilkWorm 3200 Hardware Reference Manual

(Publication number 53-0001619-06)

The *Temperature* condition in Table A-3 on page A-3 of Appendix A refers to the ambient air temperature at the air intake vents on the nonport side of the switch. You should change the *Temperature* condition within the "Condition" heading in the table to *Ambient Temperature* and also add the following note to the table:

NOTE: The temperature inside the switch can be up to 75 degrees Celsius (167 degrees F) during switch operation.

SilkWorm 3800 Hardware Reference Manual
(Publication number 53-0001576-06)

The *Temperature* condition in Table A-3 on page A-3 of Appendix A refers to the ambient air temperature at the air intake vents on the nonport side of the switch. You should change the *Temperature* condition within the "Condition" heading in the table to *Ambient Temperature* and also add the following note to the table:

NOTE: The temperature inside the switch can be up to 75 degrees Celsius (167 degrees F) during switch operation.

The following statement should be added to the Port Status LED information for when the port status is "offline" in Table 3-1, "Port Side LED Patterns During Normal Operation," on page 3-2:

"When a Port Status LED indicator light is off, another possible hardware status is offline."

Closed Defects in Fabric OS v3.2.1 GA

This table lists the defects that have been newly closed in Fabric OS v3.2.1.

Defects Newly Closed in Fabric OS v3.2.1 GA		
Defect ID	**Severity**	**Description**
DEFECT000054367	High	Summary: Tape Drive problem with Silkworm 3800s - L bit is currently depending on the Lport lock of portcfgLport. Symptom: 3rd party device does respond well to the L (Login) bit being set based on switch lock L port configuration. Solution: Loop master can set Login (L) bit in LISA frame to indicate a device login is needed. portcfglport sometimes is used to lock a port at L port and prevent a port from trying point to point. With portcfglport, the switch forces LISA frame to set the L bit (Login bit) for both public and private loop devices. Fixed code such that the Lbit setting is independent of portcfglport. Workaround: Do not Lock L port with portcfgLport Customer Impact: With a certain 3rd party tape device, the LIPA table does not show the switch to which the device is connected. Service Request# RQST00000036080 Reported in Release: V3.1.2
DEFECT000055545	High	Summary: After switchdisable/enable of all switches in a large secure fabric, some SilkWorm 3800 switches got queue overflow and rebooted. Symptom: Observed queue overflow messages and switch reboot. Solution: Adjusted scn_q and sec_q queue size to allow more time to process queued messages during large fabric configuration. Customer Impact: After switch disable/enable of all switches in a large secure fabric (a mixed large fabric with 1280 ports testing FOS 5.0.1), some SW3800's experienced queue overflows and reboot. Probability: Low Reported in Release: V3.2.0

Defects Newly Closed in Fabric OS v3.2.1 GA		
Defect ID	**Severity**	**Description**
DEFECT000057260	High	Summary: During in-house testing on large fabrics, all switches in a 30-switch fabric become isolated. Symptom: FOS 3.x principal switch stuck in a state where it does not receive any frames but keeps on transmitting ELP frames at 10 second intervals. Fabric does not come up. Solution: After the global object structure is allocated, its members are not initialized. Subsequent freeing of bad memory (structure members) caused tTransmit to be suspended and stuck in MS code. Though the receiving task is still receiving frames, the fabric can not build up. The fix is to initialize the member data structure after it is allocated in msd. Customer Impact: Due to the nature of the testing that induced this problem, it is unlikely that this would ever occur at a customer site. Probability: Low Reported in Release: V3.2.0
DEFECT000057919	High	Summary: Using Web Tools, received a pop up message "NO PERFORMANCE LICENSE " during "basic monitoring." Symptom: Using Web Tools, click PERF button, then from the "performance monitor" window, choose "performance graphs" then "basic monitoring". "port throughout" and "port error" will show no license. Solution: Make FOS3.x consistent with later release and previous release to allow basic monitoring without the Advance Performance Monitoring license. Workaround: Install Advanced Performance Monitoring license. Customer Impact: No monitoring of basic monitor service without Advance Performance Monitoring license. Service Request# RQST00000038197 Reported in Release: V3.2.0

Defects Newly Closed in Fabric OS v3.2.1 GA		
Defect ID	**Severity**	**Description**
DEFECT000058015	High	Summary: Config Upload fails with API error -83 for Silkworm3x00 with FOS3.2.x. Symptom: From Fabric Manager, the 'Save Baseline' feature reports a "Config Upload Failed" error message. Solution: In FOS 3.x, the API_MAX_CONFIG size was defined as 128KB, which is no longer big enough due to new zone database size increase in later release. Increase API_MAX_CONFIG size. Workaround: Save config database through CLI. Customer Impact: Config upload will fail on a switch supporting a larger Zone Data Base, making the total config file larger than 128k. Reported in Release: V3.2.0
DEFECT000058964	High	Summary: The CurVal of eportTXPerf did not change from 0 percentage. Solution: The current value of eportTXperf was returned as a percentage of link speed but was wrongly being converted to a kilobyte value in the eportAgentTXPerfGet() function. Since it is already a percentage, it should not be converted to a kilobyte value. Customer Impact: This is a display issue only: no major customer impact. Service Request# RQST00000039328 Reported in Release: V3.2.0
DEFECT000059155	High	Summary: Silkworm3800 running 3.2.0 panics while doing zoning changes in interop mode. Symptom: Switch panic on zone change in interop mode with a 3rd party switch. Switch panic'd after running the cfgsave command with _ipoHostPortCheck + 0x588 Solution: Zone list memory on the neighboring Silkworm 3800 is getting corrupted when a State Change Notification (SCN) is sent by another Silkworm 3800 following a "cfgSave", which leads the Silkworm3800 to a panic mode. Customer Impact: This problem occurs only when a certain 3rd party switch is connected to the Silkworm 3800. Service Request# RQST00000039382 Reported in Release: V3.2.0

Defects Newly Closed in Fabric OS v3.2.1 GA		
Defect ID	**Severity**	**Description**
DEFECT000059212	High	Summary: Silkworm 3800 is using incorrect buffer-to-buffer (BB) credits when switch BB credit is set to less than device BB credit. Symptom: Customer experienced failed tape backups/SCSI transport failure. This is caused by a Silkworm 3800 sending frames even though there are zero buffer credits. Solution: Brocade switch wrongly sets the effective BB credit to fixed number 16 if device has BB credit limit set to more than configured BB credit limit in switch. Fix the code to use configured BB credit limit in switch. Workaround: Increase the switch BB credit limit to >= device BB credit limit. Customer Impact: The problem only happens if configured switch BB credit limit is less than device BB credit limit. Probability: Low Service Request# RQST00000039498 Reported in Release: V3.1.3
DEFECT000059784	High	Summary: Switch port is too sensitive to short burst of bad primitives on the link, and causes rx_under flow error. Symptom: Customer experiencing random link failures triggered by the DWDM creating bursts of code violations. Solution: When there is a short burst of bad primitives, check if the loss of sync timeout bit is set in the lli interrupt status to extend switch tolerance on the number of bad primitives. Customer Impact: The issue is observed with a certain tape device and DWDM device. Service Request# RQST00000039083 Reported in Release: V3.2.0

Defects Newly Closed in Fabric OS v3.2.1 GA		
Defect ID	**Severity**	**Description**
DEFECT000056082	Medium	Summary: When SW3800 was rebooted, ZONEGROUPADDFAIL message is displayed.

Symptom: With 2 or more ports zoned together on the switch, customer will see "ZONEGROUPADDFAIL....." message when switch is brought online.

Solution: Fixed a race condition when multiple ports in same zone are coming up together.

Customer Impact: Problem occurs most often during switch start up or switchEnable, followed by switchDisable.

Service Request# RQST00000035448

Reported in Release: V3.2.0 |
| DEFECT000059558 | Medium | Summary: Certain vendor's E-mail from switch rejected: 501 badly formated MAIL FROM user - no "<.

Symptom: Email configured through Fabric Watch is not received on certain 3rd party mail servers.

Solution: Add "<" to the address in mail header format.

Customer Impact: Only Mail Marshall 6.0 fails.

Service Request# RQST00000038173

Reported in Release: V3.2.0 |

Closed Defects in Fabric OS v3.2.0a

This table lists the defects that were closed in Fabric OS v3.2.0a.

Defects Closed in Fabric OS v3.2.0a		
Defect ID	**Severity**	**Description**
DEFECT000048432	High	Summary: When the switch is accessed through Web Tools, the login dialog displays a warning message that the certificate load failed. Symptom: When logging into the switch via Web Tools, the login window displays "Secure Login" although there is no security license. Solution: Web Tools queries a URL page to know if the switch is secure mode enabled or disabled. When customer uses the proxy server, this URL will return the invalid page , causing Web Tools to run into exceptions. When Web Tools checks for security mode it catches the exception. Then it will by default believe that the switch has secure mode enabled. So Web Tool popped up a secure login dialog. The fix is to remove the handcraft URL with regular URL such that web tool gets the http protocol and port from the launch URL. Workaround: Do not use the proxy server Customer Impact: This only happens if the proxy server uses specific settings causing the URL page not to go through. A workaround exists for this issue. Service Request# RQST00000031210 Reported in Release: V3.1.1

Defects Closed in Fabric OS v3.2.0a		
Defect ID	**Severity**	**Description**
DEFECT000051204	High	Summary: After a 3rd party device by design bounced the link during an administrative LUN command, the host PLOGI to the device was not passed through by the switch. Symptom: The host records the PLOGI to the device, but the switch does not record the PLOGIN in the portlogdump. Solution: Offline RSCN from the bounced link device and FLogin caused a race condition in setting up Filter CAM in the ASIC driver. In FOS3.1.x/3.2, port offline SCN is received in the name server queue, which indirectly sends an ioctl to the ASIC driver to remove the Filter CAM entry. Flogin is intercepted by zoned which sends the ioctl to the ASIC driver to set up the Filter CAM entry. The cam entry setup from flogin from zoned was interfered with by the cam entry tear down from the name server daemon. The fix is to make sure that the Filter CAM is not torn down if the port is on line and the FLOGIN is processed already. Workaround: portdisable or portenable the switch port. Customer Impact: The problem is created by a link reset followed immediately by a FLOGI to the switch. This problem is only seen on a specific 3rd party storage device, which intentionally bounces the link during an administration LUNS change. Service Request# RQST00000033365 Reported in Release: V3.1.2
DEFECT000051484	High	Summary: Memory leak in name server when Get Symbolic Node Name (GSNN) command is received for a remote switch. Symptom: Switch panic CRITICAL SYS-NOMEM, 1, No memory Solution: There is a memory leak in the name server code when a Get Symbolic Node Name (GSNN) command is received for a remote device. The fix is to free the memory after the remote device returns the response. Workaround: Avoid polling the GSNN through API or any other management service until the patch is applied. Customer Impact: This has been observed when performing a GSNN poll frequently through a management service using API. The switch eventually runs out of memory and panics. Service Request# RQST00000034211 Reported in Release: V3.2.0

Defects Closed in Fabric OS v3.2.0a		
Defect ID	**Severity**	**Description**
DEFECT000052557	High	Summary: User disabled ports re-enable themselves when "L1" ports fail Symptom: A user disabled port (via portdisable, portpersistentdisable) is enabled when another port in the same quad goes offline. Solution: 1. When a port is already disabled by the user, clear the flag regarding buffer credits. Hence, the switch will only remember the user disable and will not maintain the disable state due to no buffers. 2. If the port is persistently disabled, fail the portEnable command. This behavior is consistent with FOS 4.x now. Customer Impact: During long distance configuration, a user may intentionally disable a port to allow another port in the same quad to have enough buffer credits to become a long distance port. But if the long distance port goes down, the user disabled port can become enabled due to the newly available buffers. This behavior might surprise unaware users. Service Request# RQST00000035007 Reported in Release: V3.2.0
DEFECT000055068	High	Summary: Silkworm 3800 panics due to malloc failure. Symptom: A system panic with no memory while there are unstable ports will generate many rscns. Solution: During debug process, sysmeminfo indicates there is a memory leak in the RSCN processing code path. However, a code review did not reveal a memory leak in the normal RSCN handling. Fix the memory leaks in error handling cases that were identified in the code review process. Workaround: To mitigate this condition, make sure the ports are zoned to reduce the likelihood of an unstable port generating RSCNs. Customer Impact: If the problem is encountered, the system will run out of memory and cause a switch reboot. Service Request# RQST00000036286 Reported in Release: V3.2.0

Defects Closed in Fabric OS v3.2.0a		
Defect ID	**Severity**	**Description**
DEFECT000055488	High	Summary: In PID Format 2 (Extended Edge PID Format), extend the support beyond 127 ports. Solution: In PID Format 2 (Extend Edge PID FORMAT), change max port support to 256. Customer Impact: This change does not impact PID format 1 (the most commonly used Core PID Format). It only impacts PID format 2 (Extended Edge PID), usually used in a static PID binded hosts environment to avoid host reboot during fabric migration to FOS 4.x. This does not impact the current environment but is needed for future platforms with more than 128 ports. Reported in Release: V3.2.0
DEFECT000055663	High	Summary: Neighboring switch has F/L ports stuck in Disabled state (Switch not ready for F or L ports). Symptom: F/L-ports in the fabric are disabled as shown below. 64 4 0 id N2 No_Sync Disabled (Switch not ready for F or L ports) Solution: 1) When there are two direct ISLs/trunks connecting switch A and switch B, the fabric is not fully segmented which causes an inconsistent view between fspf and the fabric domain list. FOS 4.x detects the inconsistency and disables the F/L ports. The fix is to segment the ports when the EFP frame is received before AC_PORT_SCN on FOS 3.2 if the secure mode is enabled. This will remove the inconsistent view between the fabric domain list and fspf. 2) There is also a problem that when one ISL/trunk is segmented, the trunk master still points to the segmented port. This means the domain cannot reach a confirmed state as it sends RDI frames through the segmented trunk port during fabric rebuild. This is also fixed by moving the master port to point to the alternate port, whenever the master port is either segmented or disabled. Workaround: Manually disable security mode on the 3.2 switch. Customer Impact: This defect will happen when switch A running FOS3.2 in secure mode is connected to switch B running FOS 4.x in non-secure mode, and there is more than 1 direct ISLs/trunk connection between switch A and switch B. On one of the direct ISL/trunks, one side reports fabric segmentation the other side did not segment. On the other direct ISL/trunk, there is no segmentation reported at all. When the FOS 4.x side detects the inconsistency, it will disable all ports. This is more likely to happen when FOS 4.x is a condor based platform, which can send EFP earlier, before FOS 3.2 can handle it properly. Reported in Release: V3.2.0

Defects Closed in Fabric OS v3.2.0a		
Defect ID	**Severity**	**Description**
DEFECT000050739	Medium	Summary: When memory allocation fails, Management Server sends corrupted response to remote switch. Symptom: msd sends a corrupted frame, causing a remote switch to panic. Solution: When malloc fails, the code does not set the explanation code. Thus when the response is generated, it sends a corrupted response to other switches in fabric. The fix is to set the proper explanation error code when malloc fails to send a correct response. Customer Impact: When FOS 3.x sends a bad response frame, it could cause other switches in the fabric not handling the bad frame well to panic. FOS 3.x sends the bad response frame only when experiencing a low memory condition. Service Request# RQST00000032793 Reported in Release: V3.1.2
DEFECT000051654	Medium	Summary: The RPA and RPRT is not forwarded to FOS5.0 and later versions Symptom: When local domain HBA/port information changes, the information is not propagated to domains running FOS5.0 or higher. Solution: When local domain HBA/port information changes, the information is not propagated to remote switch if remote switch has FOS 5.0 and higher due to a version comparison mistake. Fix the version check such that RPA and RPRT are propagated properly to higher version switches. Customer Impact: FOS 5.0 and above won't get RPA and RPRT updates in the fabric for FDMI. This defect does not impact the currently released product, and is now fixed for future FOS functionality. Reported in Release: V3.2.0

Defects Closed in Fabric OS v3.2.0a		
Defect ID	**Severity**	**Description**
DEFECT000053117	Medium	Summary: Web Tool "member of zones" is not listed in PID FORMAT 0 (Native PID Format) for interop with old Silkworm1000 switches. Symptom: If PID Format is set to 0, neither soft- nor hardzoning show "member of Zone" information under Web Tools. With PID Format set to 1 or 2, the zones are listed in "member of zone." Solution: Change the logic to get the areaid based on the PID format. Customer Impact: PID Format 0 is used for interop with Silkworm1000. The problem is observed on Web Tools under PID Format 0 only. CLI display is good. Service Request# RQST00000035420 Reported in Release: V3.2.0
DEFECT000054423	Medium	Summary: Can not create DCC_POLICY by using * to include port numbers beyond 127 in the DCC_POLICY Symptom: Can not create security DCC policy to include beyond 127 port numbers Solution: Adjust length definitions SEC_MEMBER_LEN and SEC_MAX_SW_PORT to handle 256 ports. Customer Impact: Security DCC policy can not include port numbers greater than 127. No impact to current product in field. Reported in Release: V3.2.0