



# Brocade Fabric OS v3.2.0a Release Notes\_v1.0

April 27, 2005

## *Document History*

<b>Document Title</b>	<b>Summary of Changes</b>	<b>Publication Date</b>
Brocade Fabric OS v3.2.0a Release Notes v1.0	First release.	April 27, 2005

Copyright © 2005, Brocade Communications Systems, Incorporated.

ALL RIGHTS RESERVED.

BROCADE, the Brocade B weave logo, Brocade: the Intelligent Platform for Networking Storage, SilkWorm, and SilkWorm Express, are trademarks or registered trademarks of Brocade Communications Systems, Inc. or its subsidiaries in the United States and/or in other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

FICON® is a registered trademark of IBM Corporation in the US and other countries.

Notice: The information in this document is provided “AS IS,” without warranty of any kind, including, without limitation, any implied warranty of merchantability, noninfringement or fitness for a particular purpose. Disclosure of information in this material in no way grants a recipient any rights under Brocade's patents, copyrights, trade secrets or other intellectual property rights. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

Notice: The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find-out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

Export of technical data contained in this document may require an export license from the United States Government.

## TABLE OF CONTENTS

Document History.....	1
About This Release.....	4
Overview .....	4
Supported Switches .....	4
Technical Support.....	4
Standards Compliance .....	5
Important Notes.....	5
OS Requirements.....	5
General .....	6
Advanced Web Tools Updates .....	7
Documentation Updates .....	10
SilkWorm 3200 Hardware Reference Manual.....	10
SilkWorm 3800 Hardware Reference Manual.....	10
Closed Defects in Fabric OS v3.2.0a.....	11

## About This Release

Fabric OS v3.2.0a is a patch release containing fixes to a number of defects found since the release of Fabric OS v3.2.0. Aside from these changes, this patch 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:
  - RADIUS
  - 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 v3.2.0 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.



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 v3.2.0a 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 v3.2.0.

## 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 out of the SAN.

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 starting February 2004.

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.

	<b>SilkWorm 2000 Series</b>	<b>SilkWorm 3200 &amp; 3800</b>	<b>SilkWorm 3016, 3250, 3850, 3900, 12000, &amp; 24000</b> <sup>1</sup>	<b>SilkWorm 4100</b> <sup>2</sup>	<b>Fabric Manager</b>
General compatibility	v2.6.1 or later	v3.1.0 or later	v4.1.0 or later	v4.4.0b 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	v4.4.0b or later	3.0.2c or later
Recommended software versions	v2.6.2	v3.2.0	v4.4.0b or later	v4.4.0b or later	4.1.1 or later

- <sup>1</sup> SilkWorm 3016 is supported by Fabric OS v4.2.1x and v4.4.0b 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.
- <sup>2</sup> SilkWorm 4100 is supported by Fabric Manager 4.4.0 or later.

## General

The major features incorporated in Fabric OS v3.2.0a are summarized in the following table.

Category	Feature	Release
<b>Manageability</b>	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
<b>Security-Related</b>	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
<b>Long-Distance Enhancements</b>	<p>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:</p> <ul style="list-style-type: none"> <li>▪ four links at 10 km @ 2 Gbit/sec per trunk group</li> <li>▪ three links at 25 km @ 2 Gbit/sec per trunk group</li> <li>▪ two links at 50 km @ 2 Gbit/sec per trunk group</li> </ul> <p>When configuring an Extended Fabrics trunk, make sure that the <i>vc_translation_link_init</i> option is set to 1 (enabled). This option can be set using the <b>portCfgLongDistance</b> 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.</p>	v3.2.0, v4.4.0
<b>MPRS Enhancements</b>	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
<b>Scalability</b>	Support for 1280 total ports and 34 domains with security enabled	v3.2.0, v4.4.0
<b>Usability Improvements + RFEs</b>	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

## 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 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
<p><b>Firmware:</b> Fabric OS v3.1+ or v4.1+</p> <p><b>Operating System:</b> any supported operating system (with supported browser)</p> <p><b>Browser:</b> any supported browser (on supported operating system)</p>	<p><b>Issue:</b> 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.</p> <p>Web Tools v3.1.0+ and v4.1.0+ includes a Print button in the Fabric Topology window. Earlier versions do not.</p> <p><b>Workaround:</b> 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.</p>

Launch Switch Environment	Problems
<p><b>Firmware:</b> Fabric OS v2.6.x</p> <p><b>Operating System:</b> Solaris</p> <p><b>Browser:</b> Mozilla</p>	<p><b>Issue:</b> The Switch Admin does not launch correctly.</p> <p><b>Workaround:</b> 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.</p>
<p><b>Firmware:</b> version <i>prior</i> to Fabric OS v2.6.2, v3.1.2, or v4.2.0 with secure mode enabled</p> <p><b>Operating System:</b> Solaris</p> <p><b>Browser:</b> Mozilla</p>	<p><b>Issue:</b> When accessing the Switch Admin, Zoning, Fabric Watch, or High Availability Admin, the browser might crash.</p> <p><b>Workaround:</b> 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.</p>
<p><b>Firmware:</b> version <i>prior</i> to Fabric OS v2.6.2, v3.1.2, or v4.2.0</p> <p><b>Operating System:</b> any supported operating system (with supported browser)</p> <p><b>Browser:</b> any supported browser (on supported operating system)</p>	<p><b>Issue:</b> 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.</p> <p><b>Workaround:</b> Use a launch switch running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later to access the switch.</p>
	<p><b>Issue:</b> 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.</p> <p><b>Workaround:</b> 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.</p>
	<p><b>Issue:</b> 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.</p> <p><b>Workaround:</b> 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.</p>
<p><b>Firmware:</b> Fabric OS v 2.6.2, v3.1.2, or v4.2.0</p> <p><b>Operating System:</b> any supported operating system (with supported browser)</p> <p><b>Browser:</b> any supported browser (on supported operating system)</p>	<p><b>Issue:</b> 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.</p> <p><b>Workaround:</b> 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.</p>

Launch Switch Environment	Problems
<p><b>Firmware:</b> version <i>prior</i> to Fabric OS v2.6.2,v3.1.2, or v4.2.0</p> <p><b>Operating System:</b> Solaris</p> <p><b>Browser:</b> Netscape</p>	<p><b>Issue:</b> Any switches running Fabric OS v2.6.2, v3.1.2, or v4.2.0 or later are unsupported through Netscape.</p> <p><b>Workaround:</b> 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.</p>
<p><b>Firmware:</b> version <i>prior</i> to Fabric OS v2.6.1, v3.0.x, or v4.0.x</p> <p><b>Operating System:</b> Windows</p> <p><b>Browser:</b> Internet Explorer</p>	<p><b>Issue:</b> When you are trying to run the Fabric View, the browser might crash.</p> <p><b>Workaround:</b> 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).</p>

## 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
<i>Brocade Advanced Performance Monitor User's Guide v3.1.0/4.1.0</i>	53-0000514-02
<i>Brocade Advanced Web Tools User's Guide v3.1.0</i>	53-0000503-02
<i>Brocade Advanced Zoning User's Guide v3.1.0/4.1.0</i>	53-0000523-02
<i>Brocade Diagnostic and System Error Reference User's Guide v3.1.0</i>	53-0000511-04
<i>Brocade Distributed Fabrics User's Guide v3.1.0/4.1.0</i>	53-0000516-02
<i>Brocade Fabric OS Procedures Guide v3.1.0</i>	53-0000501-02
<i>Brocade Fabric OS Reference v3.1.0</i>	53-0000500-02
<i>Brocade Fabric Watch User's Guide v3.1.0</i>	53-0000504-02
<i>Brocade ISL Trunking User's Guide v3.1.0/4.1.0</i>	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 v3.2.0a

Defects Closed in Fabric OS v3.2.0a		
Defect ID	Severity	Description
DEFECT000048432	High	<p>Summary: When the switch is accessed through Web Tools, the login dialog displays a warning message that the certificate load failed.</p> <p>Symptom: When logging into the switch via WEBTOOLS , the login window displays "Secure Login" although there is no security license.</p> <p>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.</p> <p>Workaround: Don't not use proxy server</p> <p>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.</p> <p>Service Request# RQST00000031210</p> <p>Reported in Release: V3.1.1</p>

Defects Closed in Fabric OS v3.2.0a		
Defect ID	Severity	Description
DEFECT000051204	High	<p>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.</p> <p>Symptom: The host records the PLOGI to the device, but the switch does not record the PLOGIN in the portlogdump.</p> <p>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.</p> <p>Workaround: portdisable or portenable the switch port.</p> <p>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.</p> <p>Service Request# RQST00000033365</p> <p>Reported in Release: V3.1.2</p>
DEFECT000051484	High	<p>Summary: Memory leak in name server when Get Symbolic Node Name (GSNN) command is received for a remote switch.</p> <p>Symptom: Switch panic CRITICAL SYS-NOMEM, 1, No memory</p> <p>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.</p> <p>Workaround: Avoid polling the GSNN through API or any other management service until the patch is applied.</p> <p>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.</p> <p>Service Request# RQST00000034211</p> <p>Reported in Release: V3.2.0</p>

Defects Closed in Fabric OS v3.2.0a		
Defect ID	Severity	Description
DEFECT000052557	High	<p>Summary: User disabled ports re-enable themselves when "L1" ports fail</p> <p>Symptom: A user disabled port (via portdisable, portpersistentdisable) is enabled when another port in the same quad goes offline.</p> <p>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.</p> <p>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.</p> <p>Service Request# RQST00000035007</p> <p>Reported in Release: V3.2.0</p>
DEFECT000055068	High	<p>Summary: Silkworm 3800 panics due to malloc failure.</p> <p>Symptom: A system panic with no memory while there are unstable ports will generate many rscns.</p> <p>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.</p> <p>Workaround: To mitigate this condition, make sure the ports are zoned to reduce the likelihood of an unstable port generating RSCNs.</p> <p>Customer Impact: If the problem is encountered, the system will run out of memory and cause a switch reboot.</p> <p>Service Request# RQST00000036286</p> <p>Reported in Release: V3.2.0</p>

Defects Closed in Fabric OS v3.2.0a		
Defect ID	Severity	Description
DEFECT000055488	High	<p>Summary: In PID Format 2 (Extended Edge PID Format), extend the support beyond 127 ports.</p> <p>Solution: In PID Format 2 (Extend Edge PID FORMAT), change max port support to 256.</p> <p>Customer Impact: This change does not impact PID format 1 (the most common 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.</p> <p>Reported in Release: V3.2.0</p>
DEFECT000055663	High	<p>Summary: Neighboring switch has F/L ports stuck in Disabled state (Switch not ready for F or L ports).</p> <p>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)</p> <p>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 inconstancy 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.</p> <p>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.</p> <p>Workaround: Manually disable security mode on the 3.2 switch.</p> <p>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 connections 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.</p> <p>Reported in Release: V3.2.0</p>

Defects Closed in Fabric OS v3.2.0a		
Defect ID	Severity	Description
DEFECT000050739	Medium	<p>Summary: When memory allocation fails, Management Server sends corrupted response to remote switch.</p> <p>Symptom: msd sends a corrupted frame, causing a remote switch to panic.</p> <p>Solution: When malloc fails, the code does not set the explanation code. Thus when the response is generated, it sends an 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.</p> <p>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.</p> <p>Service Request# RQST00000032793</p> <p>Reported in Release: V3.1.2</p>
DEFECT000051654	Medium	<p>Summary: The RPA and RPRT is not forwarded to FOS5.0 and later versions</p> <p>Symptom: When local domain HBA/port information changes, the information is not propagated to domains running FOS5.0 or higher.</p> <p>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.</p> <p>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.</p> <p>Reported in Release: V3.2.0</p>

Defects Closed in Fabric OS v3.2.0a		
Defect ID	Severity	Description
DEFECT000053117	Medium	<p>Summary: Web Tool "member of zones" is not listed in PID FORMAT 0 (Native PID Format) for interop with old Silkorm1000 switches.</p> <p>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."</p> <p>Solution: Change the logic to get the area id based on the PID format.</p> <p>Customer Impact: PID Fomat 0 is used for interop with Silkorm1000. The problem is observed on Web Tools under PID Format 0 only. CLI display is good.</p> <p>Service Request# RQST00000035420</p> <p>Reported in Release: V3.2.0</p>
DEFECT000054423	Medium	<p>Summary: Can not create DCC_POLICY by using * to include port numbers beyond 127 in the DCC_POLICY</p> <p>Symptom: Can not create security DCC policy to include beyond 127 port numbers</p> <p>Solution: Adjust length definitions SEC_MEMBER_LEN and SEC_MAX_SW_PORT to handle 256 ports.</p> <p>Customer Impact: Security DCC policy can not include port numbers greater than 127. No impact to current product in field.</p> <p>Reported in Release: V3.2.0</p>