Brocade Fabric OS v5.0.2 Release Notes v1.1

November 23, 2005

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v5.0.2 Release Notes v1.0	First release.	November 16, 2005
Brocade Fabric OS v5.0.2 Release Notes v1.1	Revised SFP compatibility information and added note regarding Blade Server running Linux.	November 23, 2005

TABLE OF CONTENTS

About This Release

Fabric OS v5.0.2 is a maintenance release that includes the same feature set as Fabric OS v5.0.1 and support for the SW4020 platform. Defects fixed in the release since 5.0.1 are listed below. Known defects open in 5.0.2 are also listed. For the list of known issues not fixed in 5.0.2, refer to the 5.0.1 release note.

Overview

Brocade Fabric OS v5.0.2 supports one new platform: the SilkWorm 4020 20-port switch for use with IBM® BladeCenter™ and IBM OEM Partners.

SilkWorm 4020

The Brocade SilkWorm 4020 switch is designed for use with IBM eServer BladeCenter™ and IBM OEM Partners; this switch is also called the Brocade® 4Gb SAN Switch Module for IBM eServer BladeCenter. The Brocade 4Gb SAN Switch Module for IBM eServer BladeCenter is an embedded 20-port Fibre Channel switch that simplifies the integration of a standard network environment with a SAN-switched storage solution through its inclusion in the IBM eServer BladeCenter ecosystem of products

Fabric OS v5.0.2 contains all of the features in v5.0.1 including basic switch and fabric support software as well as optionally licensed software that is enabled via license keys. It comprises two major software components: firmware, which initializes and manages the switch hardware, and diagnostics.

Included in every switch:

- **Brocade Advanced Zoning** segments a fabric into virtual private SANs.
- **Brocade Web Tools** enables administration, configuration, and maintenance of fabric switches and SANs.

Optionally licensed products include:

- **Brocade Extended Fabrics** provides up to 230 km of switched-fabric connectivity at full bandwidth over long distances.
- **Brocade ISL Trunking** provides the capability to combine up to 3 ISL's into one logical 12 Gbit/sec "trunk" optimizing performance and simplifying management.
- **Brocade Fabric Manager** enables administration, configuration, and maintenance of fabric switches and SANs with host-based software.
- **Brocade Advanced Performance Monitoring** enables performance monitoring of networked storage resources.
- **Brocade Fabric Watch** monitors mission-critical switch operations.
- **Ports on Demand** offers instant, non-disruptive scalability to increase the number of ports in 5, or 10 port increments.

Supported Switches

Brocade Fabric OS v5.0.2 is specific to the SilkWorm 4020. Attempts to load this software release on Brocade switches other than the SilkWorm 4020 will result in File-Not-Found errors. At the same time, the SilkWorm 4020 is not supported by any previous versions of Brocade Fabric OS, including v5.0.1x. Attempts to load any release prior to Brocade Fabric OS v5.0.2 on a SilkWorm 4020 will result in File-Not-Found errors.

Technical Support

Contact your switch supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information immediately available:

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, 4012, and 4020—Side of switch module
   - SilkWorm 200E—Nonport side of the chassis
   - SilkWorm 3250, 3850, and 3900—Bottom of the chassis
   - SilkWorm 4100—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, 24000, and 48000 directors—Inside front of the chassis, on the wall to the left of the 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 200E, 3016, 3250, 3850, 3900, 4012, 4020 and 4100 switches and SilkWorm 12000, 24000, and 48000 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—Provide the switch WWN. Use the **wwn** command to display the switch WWN.

Standards Compliance

Brocade Fabric OS v5.0.2 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 this Brocade Web site:

http://www.brocade.com/sanstandards

OS Requirements

The following table summarizes the earliest versions of Brocade software that is supported in 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.

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

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

	General Compatibility	With Secure Fabric OS Enabled	Recommended Software Versions
SilkWorm 4020	v5.0.2[1] or later	v5.0.2[1] or later	v5.0.2[1] or later
SilkWorm 4012	v5.0.0 or later	v5.0.0 or later	v5.0.1b or later
SilkWorm 2000 series	v2.6.1 or later	v2.6.1 or later	v2.6.2d
SilkWorm 3200 and 3800	v3.1.0 or later	v3.1.2 or later	v3.2.0a
SilkWorm 3016, 3250, 3850, 3900, 12000, and 24000	v4.1.0 or later	v4.2.0 or later	v5.0.1b or later
SilkWorm 200E and 48000	v5.0.1 or later	v5.0.1 or later	v5.0.1b or later
SilkWorm 4100	v4.4.0c or later	v4.4.0c or later	v5.0.1b or later
Fabric Manager	4.1.1 or later	4.1.1 or later	5.0.0a or later

1. Fabric OS 5.0.2 is supported only on the SilkWorm 4020. Attempts to load this software release on Brocade switches other than the SilkWorm 4020 will result in File-Not-Found errors.

Important Notes

This section lists information that you should consider when running Fabric OS v5.0.2.

As of May 15, 2005, Brocade no longer includes a PKI Certificate as part of the installed Secure Fabric OS. If you wish to activate Secure Fabric OS on a supported director or switch, you must contact Brocade to obtain a PKI certificate.

Refer to the *Secure Fabric OS Administrator's Guide*, Chapter 2, "Adding Secure Fabric OS to the Fabric," for a description of how to obtain certificates from the Brocade Certificate Authority.

General

The major new features incorporated in Fabric OS v5.0.2 are summarized in the following sections.

SilkWorm 4020 Platform Support

The SilkWorm 4020 is a 4 Gbit/sec, 20-port embedded Fibre Channel switch using the Brocade Goldeneye ASIC. Fabric OS v5.0.2 supports the SilkWorm 4020, including thePorts-on-Demand (POD) feature. Ports-on-Demand delivers 15 or 20 ports in 5 or 10 port increments from the base configuration of 10 ports. The Brocade 4Gb SAN Switch Module offers the following capabilities:

- Support for the integrated SilkWorm 4020 switch embedded into the IBM eServer BladeCenter enterprise chassis and IBM eServer BladeCenter T chassis.
- Protects existing investments by providing 4 Gbit/sec technology with auto-sensing capabilities to recognize 1 and 2 Gbit/sec devices
- Supports full 4 Gbit/sec operations at distances up to 57 kilometers (or 230 kilometers at 1 Gbit/sec) for cost-effective business continuance operations

- Increases network performance with enhanced Brocade Inter-Switch Link (ISL) Trunking, which enables a high-speed data path up to two, three port trunk groups for an aggregate bandwidth of 24 Gbit/sec
- Supports 1, 2 and 4Gps (full duplex) performance with an aggregate bandwidth of 80 Gbit/sec
- Implements Ports-on-Demand (POD) on the SilkWorm 4020 instead of the two-domain, and full fabric (VL2/FF) as used on the SilkWorm 3016. POD activates up to 10 additional ports on the Brocade 10-Port 4 Gb SAN Switch Module. The VL2/FF implementation will continue to be used for the SilkWorm 3016.

Changes Unique to the SilkWorm 4020

Changes to Web Tools

WebTools in BladeCenter Enterprise Chassis:

- New graphic showing 14 internal ports and 6 external ports
- Switch Info button has been removed
- Switch Info is located on initial WebTool page
- No power or fan information
- Bay location added
- New column “Licensed Ports” added to Admin Ports panel. Unlicensed ports are grayed-out and can be configured but not enabled

WebTools in eServer BladeCenter T Chassis:

- New Telco Graphic showing only 8 internal ports and 6 external ports
- Switch Info button has been removed
- Switch Info is located on initial WebTool page
- No power or fan information
- Persistent Disable setting for ports 9-14 is automatic in the Telco chassis
- New column “Licensed Ports” added to Admin Ports panel. Unlicensed ports are grayed-out and can be can be configured but not enabled

Note that ports 1 through 14 and the associated status indicators represent ports internal to eServer BladeCenter that connect to the 14 server slots. Ports 0 and 15 through 19 represent ports external to eServer BladeCenter.

The switch icon for the Brocade SilkWorm 4020 switch consists of the following:

- External ports and status LEDs
- Internal ports and status indicators
- Switch status LEDs

Refer to the *SilkWorm 4020 Hardware Reference Manual* (Publication Number 53-0000688-01) for detailed information.

Port Info Tab

The **Port Info** tab displays 20 port tabs (0 through 19) for the SilkWorm 4020 switch. In the Telco chassis, ports 9 through 14 are persistently disabled.

The **SFP** subtab on the **Port Info** dialog displays “NO SFP INFO AVAILABLE” for the 14 internal ports of the Brocade SilkWorm 4020 switch.

The **Loop** subtab on the **Port Info** dialog displays “NO LOOP INFO AVAILABLE” for the 14 internal ports of the Brocade SilkWorm 4020 switch.

Changes to ISL Trunking

If your SilkWorm 4020 switch is licensed for the optionally licensed Brocade ISL Trunking feature, up to three external ports can be used to build a trunk. A total of two trunk groups can be built to join a trunking group on another SilkWorm switch that supports ISL Trunking. Refer to the *Brocade Fabric OS Administrator's Guide* (Publication Number 53-0000518-09) for more information.

Extended Fabric/Long-Distance Changes

The SilkWorm 4020 provides the same L0 mode support as the SilkWorm 200E. See Table 1 for approximate distance for L0 mode.

Table 1 Maximum supported distance in L0 mode

Platform	Speed: 1 Gig	Speed: 2 Gig	Speed: 4 Gig
Non-Goldeneye platforms	10 km	5 km	2.5 km
Goldeneye-based platforms	6 km	3 km	1.5 km

Table 2 specifies the maximum number of LE ports (LE mode supports distance of 10km) that can be configured on the SilkWorm 4020 without causing other ports to become "buffer-limited".

Table 2 Maximum number of LE ports

Speed	Maximum number of LE ports	Maximum number of "buffer-limited" ports
1G	6	0
2G	6	0
4G	6	0

Table 3 Shows the maximum distance supported for a given number of LD ports, at the specified speed. Table 4 assumes that non-LD ports are either not being used, or are attached to a host, or target using F_Port.

Table 3 Maximum supported distance

	1 LD Port	2 LD Port	3 LD Port	4 LD Port	5 LD Port	6 LD Port
4G	57.5km	29.5 km	20.1 km	15.5 km	12.7 km	10.8 km
2G	115 km	59 km	40.3 km	31 km	25.4 km	21.6 km
1G	230 km	118 km	80.6 km	62 km	50.8 km	43.3 km

The average buffer allocation, and extended ISL distance supported will vary for switches that have the Goldeneye ASIC. The following information is intended for the SilkWorm 4020.

Enhanced extended ISL modes for SilkWorm 4020, on a per port basis, is summarized in Table 4

Table 4 Extended ISL Modes: SilkWorm 4020 with Goldeneye ASIC

Mode	Buffer Allocation			Distance @ 1 Gbit/ sec	Distance @ 2 Gbit/ sec	Distance @ 4 Gbit/ sec	Earliest Fabric OS Release	Extended Fabrics License Required?
	1 Gbit/ sec	2 Gbit/ sec	4 Gbit/ sec					1 Gbit/ sec
L0	3 (17)[a]	3 (17)	3 (17)	6 km	3 km	1.5 km	v5.0.2	No
LE	10	15	25	10 km	10 km	10 km	v5.0.2	No
L0.5	18	30	55	25 km	25 km	25 km	v5.0.2	Yes
L1	30	55	105	50 km	50 km	100 km	v5.0.2	Yes
L2	55	105	0	100km	100 km	0	v5.0.2	Yes
LD	Auto[b]	Auto	Auto	Auto	Auto	Auto	v5.0.2	Yes

a. For each data channel (in this case, there are 4) there are 3 credits, plus 5 used for VC overhead.

b. The dynamic long-distance mode (LD) automatically configures the number of buffer credits required, based on the actual link distance.

For dynamic long distance links, you can approximate the number of buffer credits using the following formula:

*Buffer credits = [(distance in km) * (data rate) * 1000] / 2112*

The data rate is 1.0625 for 1 Gbit/sec, 2.125 for 2 Gbit/sec, and 4.25 for 4 Gbit/sec and Fibre Channel. This formula provides the minimum number of credits that will be allocated to a given port; the actual number will likely be higher.

Changes to Fabric Licensing

The SilkWorm 4020 ships in two versions. The first version is called the Brocade® 10-Port Model. This switch ships with 7 active internal ports and 3 active external ports.

The second version is the Brocade® 20-Port Model. This switch ships with 14 Internal Ports active, and 6 External Ports active.

Refer to the *SilkWorm 4020 Hardware Reference Manual* (Publication Number 53-0000688-01) for more information.

Changes to Fabric Manager

Fabric Manager v5.0.0 supports the SilkWorm 4020.

Reliability

This release of Fabric OS features RSCN suppression: the ability to control RSCNs originating from hosts on a port-by-port basis.

Enhanced RAS Log Messages

New with Fabric OS v5.0.1 are Zoning Audit messages. These messages record information about the type of zoning change made (including such tasks as **cfgenable** and **cfgdisable**) and the role level and user name making the changes. The messages are recorded in the RASlog whether change was made through the CLI or Web Tools. Note that occasional redundant entries are possible due to an extra HTTP entry when zoning changes are performed through the CLI.

Scalability

Fabric OS v5.0.2 supports the same fabric scalability as Fabric OS v4.4.0 (2,650 ports with 56 domains).

Problem Determination

Fabric OS v5.0.2 includes the **FcPing** command, which provides the ability to check Fibre Channel connectivity between any two nodes in a fabric.

Security-Related Enhancement

A new role-based access control role, switch administrator, allows an administrator to control a switch but not modify any fabric-wide configuration such as security, zoning, or user configuration (see the **userConfig** command).

Merging Zones

Before linking two switches together, it is important that you know the zone database limit of adjacent switches. For example, when switches running Fabric OS v3.2, v4.4.0, or v5.x discover that the zone merge database is larger than its pre-determined zone database size limit, they issue a reject notification before symmetrically segmenting their own ends of the ISL, thereby preventing the new switch from joining the fabric.

Symmetrical segmentation occurs when both ends of an ISL are shut down. Subsequently, no frames are exchanged between those two switches.

Asymmetrical segmentation not only prevents frames from being exchanged between switches, but also causes routing inconsistencies.

The best way to avoid either type of segmentation is to know the zone database size limit of adjacent switches. The following tables provide the expected behavior based on different database sizes after a zone merge is specified.

Table 1 Resulting Database Size: 0 to 96K

Receiver / Initiator	FOS v2.6	FOS v3.1	FOS v3.2	FOS v4.0/ v4.1/v4.2	FOS v4.3/ v4.4.0	FOS v5.0.0/ v5.0.1	Fibre Channel Router	XPath v7.3
FOS v2.6/v3.1	Join	Join	Join	Join	Join	Join	Join	Join
FOS v3.2	Join	Join	Join	Join	Join	Join	Join	Join
FOS v4.0/v4.1/ v4.2	Join	Join	Join	Join	Join	Join	Join	Join
FOS v4.3/v4.4.0	Join	Join	Join	Join	Join	Join	Join	Join
FOS v5.0.0/v5.0.1	Join	Join	Join	Join	Join	Join	Join	Join
Fibre Channel Router	Join	Join	Join	Join	Join	Join	Join	Join
XPath v7.3	Join	Join	Join	Join	Join	Join	Join	Join

Table 2 Resulting Database Size: 96K to 128K

Receiver / Initiator	FOS v2.6	FOS v3.1	FOS v3.2	FOS v4.0/ v4.1/v4.2	FOS v4.3/ v4.4.0	FOS v5.0.0/ v5.0.1	Fibre Channel Router	XPath v7.3
FOS v2.6/v3.1	Segment	Segment	Segment	Segment	Segment	Segment	Join	Segment
FOS v3.2	Segment	Segment	Join	Join	Join	Join	Join	Join
FOS v4.0/v4.1/ v4.2	Segment	Segment	Segment	Join	Join	Join	Join	Join
FOS v4.3/v4.4.0	Segment	Segment	Join	Join	Join	Join	Join	Join
FOS v5.0.0/v5.0.1	Segment	Segment	Join	Join	Join	Join	Join	Join
Fibre Channel Router	Join	Join	Join	Join	Join	Join	Join	Join
XPath v7.3	Segment	Segment	Segment	Join	Join	Join	Join	Join

Table 3 Resulting Database Size: 128K to 256K

Receiver / Initiator	FOS v2.6	FOS v3.1	FOS v3.2	FOS v4.0/ v4.1/v4.2	FOS v4.3/ v4.4.0	FOS v5.0.0/ v5.0.1	Fibre Channel Router	XPath v7.3
FOS v2.6/v3.1	Segment	Segment	Segment	Segment	Segment	Segment	Join	Segment
FOS v3.2	Segment	Segment	Join	Segment	Join	Join	Join	Segment
FOS v4.0/v4.1/ v4.2	Segment	Segment	Segment	Segment	Segment	Segment	Segment	Segment
FOS v4.3/v4.4.0	Segment	Segment	Join	Segment	Join	Join	Join	Segment
FOS v5.0.0/v5.0.1	Segment	Segment	Join	Segment	Join	Join	Join	Segment
Fibre Channel Router	Join	Join	Join	Segment	Join	Join	Join	Segment
XPath v7.3	Segment	Segment	Segment	Segment	Segment	Segment	Segment	Segment

Table 4 Resulting Database Size: 256K to 1M

Receiver / Initiator	FOS v2.6	FOS v3.1	FOS v3.2	FOS v4.0/ v4.1/v4.2	FOS v4.3/ v4.4.0	FOS v5.0.0/ v5.0.1	Fibre Channel Router	XPath v7.3
FOS v2.6/v3.1	Segment	Segment	Segment	Segment	Segment	Segment	Segment	Segment
FOS v3.2	Segment	Segment	Segment	Segment	Segment	Segment	Segment	Segment
FOS v4.0/v4.1/ v4.2	Segment	Segment	Segment	Segment	Segment	Segment	Segment	Segment
FOS v4.3/v4.4.0	Segment	Segment	Segment	Segment	Segment	Segment	Segment	Segment
FOS v5.0.0/v5.0.1	Segment	Segment	Segment	Asymmetrical Segment	Segment	Join	Join	Segment
Fibre Channel Router	Segment	Segment	Segment	Segment	Segment	Join	Join	Segment
XPath v7.3	Segment	Segment	Segment	Segment	Segment	Segment	Segment	Segment

Web Tools

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 v2.6.x versions, no warning message is displayed.

Workaround: Use Netscape 4.7.7 or later.

The added supported browsers, operating systems, and Java Plug-ins introduce the following limitations when using mixed OS versions in Web Tools v5.0.1, as identified in the following table.

Web Tools Compatibility Limitations

Launch Switch Environment	Problems
Firmware: Fabric OS v3.1.0+, v4.1.0+, or v5.0.1+ **Operating System**: Any supported operating system (with supported browser) **Browser**: Any supported browser (on supported operating system)	**Issue**: When viewing the topology from Web Tools, if your initial login was a v3.1.0+, v4.1.0+, or v5.0.1+ 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+, v4.1.0+, and v5.0.1+ include a Print button in the Fabric Topology window; earlier versions do not. **Workaround**: If the Fabric Topology window does not include a Print button, 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 Switch Admin using Fabric OS v2.6.2 on a Solaris operating system with a Mozilla browser, a warning message is displayed, telling you to use the Netscape browser. • If you try to launch 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 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 v4.2.0a **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 (Brocade 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 or later.
Firmware: Fabric OS v5.0.1+ **Operating System**: Any supported operating system (with supported browser) **Browser**: Internet Explorer and Mozilla	**Issue:** If you upgrade from Fabric OS v4.x to v5.x, you must upgrade your Java plug-in version to v1.4.2_06 from any prior version installed on your system. **Workaround:** For Internet Explorer, before launching Web Tools, check your Java plug-in version. If you have a version lower than 1.4.2_06, then you must uninstall it. When you launch Web Tools and you see a warning about a missing plug-in, follow the prompts. This procedure will make sure that the correct plug-in version is actually installed. For Mozilla, follow the Mozilla Java plug-in installation instructions to install Java v1.4.2_06.

Other Notes

The tables below list other important information you should consider about the SilkWorm 4020 and Fabric OS v5.0.2.

SilkWorm 4020	Description
Chassis	The Brocade SilkWorm 4020 blade is a Fibre Channel switch that supports link speeds up to 4 Gbit/sec. It is designed to work in an IBM® BladeCenter™ and BladeCenter™ Telco chassis.
SWL SFP	Please check the IBM ServerProven® Compatibility website for the latest supported SFP here: http://www-03.ibm.com/servers/eserver/serverproven/compat/us/blade/8720.html Or here: http://www-1.ibm.com/support/docview.wss?rs=1201&uid=psg1SCOD-3ZVQ5W&loc=en_US&cs=utf-8&lang=en ftp://ftp.software.ibm.com/pc/pccbbs/pc_servers_pdf/cog.pdf
LED	There are several important differences between Brocade SilkWorm 4020 and other Goldeneye-based platforms. • SilkWorm 4020 does not use bicolor LEDs. The OK and FAULT pair would be a single bicolor LED on other platforms, as would STATUS and DIAGNOSTICS. • The FAULT LED never blinks—it is either steady on or steady off. • The OK LED only blinks during initialization and diagnostics—it is either steady on or steady off at all other times. • The single SPEED LED can only represent two speed states: 4 Gbps versus 1 Gbps or 2 Gbps. This LED will be green for 4 Gbps and off for other speeds.

Fabric OS Area	Description
Advanced Performance Monitor	Adding Advanced Performance Monitor (**perfAddUserMonitor**) without zoning enabled at the same time will stop all frame traffic. The only frames that can go through are those that match the definitions in the **perfAddUserMonitor** command, in most cases, a very narrow definition. The result is that almost all traffic is blocked. Add Advanced Performance Monitor only when zoning is also enabled.
Nondefault operands	**IMPORTANT:** The use of nondefault operands for diagnostic commands is recommended for advanced users and technical support only.

Fabric OS Area	Description
Zoning	With AUDIT logging enabled, while performing zoning changes via CLI, an additional audit log from HTTP may also appear along with the audit logs from zoning. This message does not always appear, and when it does, it represents redundant reporting by the CAL layer.
Loss of sync between Emulex HBA and Brocade 4Gb/sec switch	**Issue:** If there is a loss of sync forcing a link to be re-esatablished, it is possible that links between Emulex HBAs and 4Gb Brocade switches may not automatically be re-established. This issue could occur after an error that has forced the switch and HBA to re-establish link initialization such as a cold switch reboot. **Workaround:** Use the command ***portCfgGPort*** to congfigure the switch port in point-to-point only mode, also known as G port mode. To configure the HBA to point-to-point mode, please refer to Emulex HBAnyware™ documentation. To re-establish the link on the affected port without traffic disruption on other ports, issue the comands ***portDisable*** and ***portEnable*** commands on the affected port.
Blade Server running Linux OS will log into SilkWorm 4020	**Issue:** Blades running Linux (RH4, SLES9, RH3U5PPC) will not log into the SilkWorm 4020. Driver versions used are: 2.4 kernel- 7.07.00 2.6 kernel- 8.01.00 **Workaround:** Set the HBA Driver to “Point-to-Point” instead of “loop preferred”.

Documentation Updates

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

Refer to the Fabric OS v5.0.1 documentation suite on Brocade Connect for Fabric OS v5.0.2 support. The documentation updates for Fabric OS v5.0.1 are available in the most recent Fabric OS v5.0.1 release notes on Brocade Connect:

http://www.brocadeconnect.com/

SilkWorm 4020 Hardware Reference Manual
(Publication number 53-000688-01)

Add the following text at the end of the first paragraph under the heading "Interpreting SilkWorm 4020 LEDs" on page 4-2:

Note: The blinking rate for RX/TX LED and the internal LED is slower than the physical switch when I/O activity is present.

Choosing an Extended ISL Mode

The average buffer allocation, and extended ISL distance supported will vary for switches that have the Goldeneye ASIC. The following information is intended for the SilkWorm 4020.

Enhanced extended ISL Modes for SilkWorm 4020 is summarized in Table xx-x.

Table xx-x Extended ISL Modes: SilkWorm 4020 with Goldeneye ASIC

Mode	Buffer Allocation			Distance @ 1 Gbit/ sec	Distance @ 2 Gbit/ sec	Distance @ 4 Gbit/ sec	Earliest Fabric OS Release	Extended Fabrics License Required?
	1 Gbit/ sec	2 Gbit/ sec	4 Gbit/ sec					1 Gbit/ sec
L0	4 (17)[a]	4 (17)	4 (17)	10 km	4 km	2 km	v5.0.2	No
LE	5	10	31	10 km	10 km	10 km	v5.0.2	No
L0.5	18	30	0	25 km	25 km	0	v5.0.2	Yes
L1	30	55	0	50 km	25 km	0	v5.0.2	Yes
L2	56	0	0	100km	0	0	v5.0.2	Yes
LD	Auto[b]	Auto	Auto	Auto	Auto	Auto	v5.0.2	Yes

a. For each data channel (in this case, there are 4) there are 4 credits, plus 1 extra credit.

b. The dynamic long-distance mode (LD) automatically configures the number of buffer credits required, based on the actual link distance.

For dynamic long distance links, you can approximate the number of buffer credits using the following formula:

*Buffer credits = [(distance in km) * (data rate) * 1000] / 2112*

The data rate is 1.0625 for 1 Gbit/sec, 2.125 for 2 Gbit/sec, and 4.25 for 4 Gbit/sec and Fibre Channel. This formula provides the minimum number of credits that will be allocated to a given port; the actual number will likely be higher.

Trunking Distances

Enhanced trunking support for the SilkWorm 4020 (Goldeneye ASIC) is summarized in Table xx-x.

Table xx-x Trunking Support for the SilkWorm 4020 (Goldeneye ASIC)

Mode	Distance	Number of 2Gbit/sec ports	Number of 4 Gbit/sec ports
LE	10 km	6 (two 3-port trunk)	6 (two 3-port trunk)
L0.5	25 km	3 (one 3-port trunk)	2 (one 2-port trunk)
L1	50 km	2 (one 2-port trunk)	0
L2	100 km	1 (one 1-port trunk)	0
LD	200 km	0	0
LD	250 km	0	0
LD	500 km	0	0

Open Defects for Fabric OS v5.0.2 GA

The following table of open defects lists those defects that, while still formally "open," are unlikely to impede Brocade customers in their deployment of Fabric OS v5.0.2 GA.

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 v5.0.2 GA but were initially reported against an earlier XPath 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.

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000059548	High	Summary: If a switch fails in a fabric that has blocked FSPF traffic, the neighboring core switch loses links and appears to hang. All links remain online. Symptom: After an AP7420 reported a parity error on a hardware component, the FOS switch topologyshow and portregshow indicated 2 connected domains lost the route to each other. Solution: Fabric Shortest Path First (FSPF) maintains a bi-directional Link State Record (LSR) database about links in the fabric and uses it to dynamically compute the shortest path from a local domain to all other domains in the fabric. When an ISL has only a 1-directional communication mode available, the 1-directional LSR causes the FSPF shortest path computation to remove the wrong route. The fix is not to remove the route that was just added if the bi-directional communication is no longer available for an ISL. Also validate the domain during the route calculation. Workaround: Identify and portdisable the problematic ISL port. Customer Impact: This unlikely event results in losing some routes in the fabric, and the host-to-target traffic is impacted. Probability: Low Service Request# RQST00000039984 Reported in Release: V4.2.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000060267	High	Summary: On condor ASIC based platform, port fault due to busy buffer stuck error on switch ISL with a 3rd party storage device. Symptom: CDR-1002: Port 27 chip faulted due to internal error which took down ISLs on Silkworm 4100. Solution: The problem was that a remote device sent a PLOGI to a non-existent loop device. The filter message that name server daemon received has to be released when it detects the loop device is no longer there. But the port number passed to filter resource release code is incorrect caused the resource not being freed and receive buffer being tied up. The fix is to pass the correct port number so filter resource is release correctly. Customer Impact: The issue is observed with a 3rd party storage controller during controller failover test: when one controller takes over for another, it appears to the Hosts that one of the PL devices simply moved ports which introduce the scenario of Plogin to a loop device that disappeared. Probability: Low Service Request# RQST00000040731 Reported in Release: V5.0.1
DEFECT000056317	Medium	Summary: Two MPRs setup as switches; when creating a new zone and using the domain port tab, only see the first 15 ports and the rest of the blades are missing Symptom: Occurs when a router is run as a switch in the fabric. If there is a router in the fabric, only 15 ports on the SW24000 are seen. Without the router, all the ports are seen. Customer Impact: Usability issue with 4.4.0 version of Web Tools and fabrics that contain more then 1 AP7420 operating as backbone switches. Probability: Medium Service Request# RQST00000034954 Reported in Release: V4.4.0

Open Defects		
Defect ID	**Severity**	**Description**
DEFECT000062401	Medium	Summary: Can set Domain ID to 238 in Interopmode causing a POST error Symptom: If Interopmode is turned on and then the Domain ID is configured to an invalid number (> 127), the switch will fail to initialize properly after a reboot and the switch will be faulted. Workaround: To avoid this symptom, always follow the recommendation from the "interopMode" command and reboot after changing the mode. This will allow the switch to readjust the domain ID validation limits for Interop Mode such that the user will not be able to configure the domain ID to an invalid number. If this symptom has already occurred and the switch is in a non-functioning state, a valid configuration can be re-established by requesting a reboot with "Restore Factory Configuration" option. Customer Impact: Switch will fail to initialize properly after a reboot and customer will have to Restore Factory Default to recover the switch. Reported in Release: V5.0.2
DEFECT000062793	Medium	Summary: PCI errors are reported while POST is running Symptom: It is possible that if enough recoverable PCI errors occur during diagnostic POST, the switch may be classified as Faulted. Workaround: Two possible workarounds: 1) Reboot the switch. This might result in a successful POST. OR 2) Use "diagDisablePost" to avoid the false POST failure. Customer Impact: This symptom could lead to a functional switch being removed from operation due to a reported POST failure. Reported in Release: V5.0.2

Closed Defects in Fabric OS v5.0.2 GA

The following tables include defects that have been fixed with code changes.

Closed Defects		
Defect ID	**Severity**	**Description**
DEFECT000054120	High	Summary: SNMP walk on MIB-2 increases the memory usage of SNMP daemon Symptom: Frequent repeated SNMP poll on switch entPhysicalTable will eventually cause an out-of-memory panic and a switch reboot. Solution: Fixed memory leaks in a function that retrieves SNMP MIB2 entPhysicalTable for switch physical attribute. Customer Impact: Continuous walk on MIB-2 exposes this memory leak. A 3rd party storage application can also expose this problem when polling the entPhysicalTable. Probability: Medium Reported in Release: V5.0.0
DEFECT000055410	High	Summary: API returns error intermittently when trying to establish a session with the proxy switch when FM tries to retrieve Port Stats and End-to-End Monitoring. Symptom: When Fabric Manager uses API, it returns -21 error code when the FabAPI_EstablishFabricSessionEx call is being made. Solution: To avoid potentially locking up the local switch, ensure that only one thread or process at a time gets access to the shared memory area used by SAPI library to pass management data to the target switch. Customer Impact: PM/APM features are not guaranteed to gather data at every 5-minute interval. Workaround exists for creating CM profile: re-create the profile. But there is no workaround when an existing CM profile is scheduled to be run. Reported in Release: V5.0.0

Closed Defects		
Defect ID	**Severity**	**Description**
DEFECT000060679	High	Summary: Blade/Brocade 4GB: (20PT) third party 4GB HBA daughter card not working with third party switch chassis. Symptom: Third party HBA configuration utility (invoked by Control-Q) will not see any HDD on either port of third party chassis. Solution: There is an issue with speed negotiation between the SW4020 and the server blade in the third-party chassis. The server reboot time exceeded the driver/switch FC speed auto-negotiation time limits. Solution was to increase the amount of time the switch will spend attempting to complete the speed auto-negotiation phase. Customer Impact: Customer will not be able to use storage devices from a Server Blade that has a certain third party HBA installed. Reported in Release: V5.0.2

Closed Defects in Fabric OS v5.0.1c and Closed in 5.0.2

Defects Closed in Fabric OS v5.0.1c		
Defect ID	**Severity**	**Description**
DEFECT000059855	High	Summary: rpcd coredump caused switch panic or failover. Symptom: rpcd0 core dump with signal 11, Segmentation fault, but no stack back trace can be generated on the panic thread. Solution: Fixed an error code handling path of secure connection, where RPCd has a pointer defined as local variable and located on stack, and same pointer is also inserted to a global list. At some point when the function exits, these pointers could be no longer valid, but still accessed through global list. As the stack being overwritten, it could cause rpcd to crash. Customer Impact: Switch may panic if the stack is badly corrupted and accessed. This problem is only observed when there is security scan application running. Probability: Low Service Request# RQST00000040243 Reported in Release: V4.4.0

Closed Defects in Fabric OS v5.0.1b and Closed in 5.0.2

Defects Closed in Fabric OS v5.0.1b		
Defect ID	**Severity**	**Description**
DEFECT000059540	Critical	Summary: SW24000 dropping frames and causing IFCCs (Interface Control Checks - FICON) Symptom: After placing the fabric into a long distance mode, and adding a SW24000 into a fabric and reconfiguring the fabric, devices attached to the SW24000 that were cascaded to other switches started getting IFCCs (Interface Control Checks). Solution: Corrected programming of back-end port VC mapping while the fabric is programmed in a long distance fabric mode setting. Customer Impact: Interface Control Checks blocking access to some devices. This has only been observed in a FICON environment. Probability: High Reported in Release: V5.0.1

Defects Closed in Fabric OS v5.0.1b		
Defect ID	**Severity**	**Description**
DEFECT000058000	High	Summary: When a disk drive on a loop is replaced, the Nameserver still shows the WWN of the old drive. Symptom: During JBOD drive replacement testing, the new drive WWN information is not listed in the switch name server table. The portloginshow command displays the correct WWN of the drive, but the old wwn shows up in the name server table. Solution: When one of the loop devices is hot swapped, NS receives a UPD_AREA SCN indicating same device PID with different WWNs. To be able to support this behavior, NS is changed to treat this as the old device offline and new device with same PID online. The zone enforcement CAM is also updated accordingly. Workaround: After swapping the device, portdisable and portenable will correct the portwwn in the NS database. Customer Impact: After hotswapping a disk drive, the user sees the WWN of the old disk drive, instead of the WWN of the new disk drive. Service Request# RQST00000038373 Reported in Release: V4.4.0
DEFECT000058011	High	Summary: Switch does not pass traffic in interop mode with Windows host when a zone change is performed without switch reboot Symptom: FC trace showed FOS 4.4 switch rejecting a GPN_ID with the error port ID not in register. Solution: The fix is to change zoning to set the proper zone type before pushing down the new zone configuration to the Name Server. Workaround: Reboot the switch. Customer Impact: Switch must be rebooted after the zone change. Probability: High Service Request# RQST00000038307 Reported in Release: V4.4.1

Defects Closed in Fabric OS v5.0.1b		
Defect ID	**Severity**	**Description**
DEFECT000058281	High	Summary: SW48000: False RLIRs on 1Gig channels on system resets Symptom: When a System Reset Clear is issued to the mainframe operators console the SW48000 detects false link incidents on the 1Gig channels. Solution: Primitive is now read in top half and saved. Later, if there is rx_fifo, the saved primitive will be checked to see if OLS was received. Probability: High Reported in Release: V5.0.1
DEFECT000058396	High	Summary: Switch panic on FOS4.4.x with zoned assert on invalid interface identifier. Symptom: Zone panic with assert at merge/zn_merge_dbg.c:453, with call from zoneDomain_portsIfId. Solution: The fix is to recover if_id for all online ports during failover. Customer Impact: The problem is only likely to happen during upgrade from 4.2.x to 4.4.x when the switch is in interop mode. The switch may also assert when there is no effective CFG enabled in non-interopmode. Once the switch is upgraded to 4.4 and rebooted, the problem should not recur. Probability: Medium Service Request# RQST00000038732 Reported in Release: V4.4.0
DEFECT000058556	High	Summary: SW200E Firmwaredownload problems Symptom: Firmwaredownload problems while performing multiple downloads with Fabric Manager and 2 of the 4 SW200Es failed with "unable to download ROM". Solution: This issue is caused by firmwaredownload not being able to install a RPM package after the package is downloaded from the network. The solution is to retry the install command for maximum of 4 times when the install command fails. If the install still fails after 4 retries, display a message "Fails to install RPM package". Service Request# RQST00000038947 Reported in Release: V5.0.1

Defects Closed in Fabric OS v5.0.1b		
Defect ID	**Severity**	**Description**
DEFECT000058745	High	Summary: FICON CUP overnight test run stopped with ABTs Symptom: Unable to bring FICON CUP Port back online Solution: Fix the overflow condition by making sure that the reference count for FICON CUP field descriptor is recovered after HA. Remove FICON CUP filter when port is offline. And only update the reference count if it's none zero. Customer Impact: Loss of access to CUP Port Probability: High Reported in Release: V5.0.1
DEFECT000058836	High	Summary: SW24000 panic when multiple changes take place without Reliable Commit Service (RCS) Symptom: Zone daemon causes switch panic (zoned ASSERT when trans_in_progress is detected) . Solution: Avoid the ASSERT in case multiple transactions are initiated at the same time when RCS is disabled in the fabric. Workaround: Enable RCS, avoid multiple transactions initiated in parallel. Customer Impact: In a fabric not running RCS, multiple transactions can occur in the fabric. The Zone daemon can process only one transaction at a time and could hit a race condition and cause a switch panic. The probability of this actually happening is low due to the small race condition window. Probability: Low Service Request# RQST00000039208 Reported in Release: V4.2.2

Defects Closed in Fabric OS v5.0.1b		
Defect ID	**Severity**	**Description**
DEFECT000059048	High	Summary: Multiple hosts lose IO, fcping to storage drops frames on certain switches in fabric Symptom: While running tests that disabled ISL between a SW200E and a SW48000, and on the SW48000 running a slotpoweroff / slotpoweron script, caused multiple hosts to be unable to query their respective storage volumes even though the name server and zone database looked OK. When performing an fcping between a host and storage port, frames were dropped on multiple switches in the fabric. Hafailovers on dual CP switches did not solve the problem. A reboot of two affected switches allowed the host to query its storage volumes even though an fcping between the two continues to drop frames on multiple switches in the fabric. A switchdisable/switchenable seemed to clear unstable fabric. Solution: This issue happens only when POST is run on a CP/port blade. The solution is to suppress the rebalance operations when diagnostics are running. Workaround: Disable POST temporarily while removing or inserting a port or CP blade. Customer Impact: There may be some missing internal routes due to this defect. Service Request# RQST00000039426 Reported in Release: V5.0.0
DEFECT000059285	High	Summary: Firmware v5.0.1 - switch does not display status "MARGINAL" when the fan is disabled. Setting for SwitchStatusPolicy - Fans: Down 2, Marginal 1. Symptom: Switch does not display status "MARGINAL" when the fan is disabled using the fandisable command. Setting for SwitchStatusPolicy - Fans: Down 2, Marginal 1. Solution: Changing switch status even when the fan FRU state is OFF due to disabling the fan. Customer Impact: Disabled Fan did not contribute to the switch status due to this the customer would not see the switch status change; i.e., from HEALTHY to MARGINAL. Service Request# RQST00000039509 Reported in Release: V5.0.1

Defects Closed in Fabric OS v5.0.1b		
Defect ID	**Severity**	**Description**
DEFECT000059393	High	Summary: No way for a customer to change if webtools.basicuser.enabled other than as root Symptom: If a user uses the Web Tools EZ on a SW200E that had been set for standard webtools, the webtools.basicuser.enabled will be set and will not allow the user to return to the use of the standard webtools interface. To undo this problem requires root access to the switch. This may be an issue as most OEM-provided switches are not provided with a root password. Solution: In the "configure" command, add a new field for basic user mode. User can telnet to switch and login as admin, disable the Basic User Mode through the "configure" command Service Request# RQST00000039684 Reported in Release: V5.0.1
DEFECT000059437	High	Summary: Switch blade insertion causes FICON I/O disruption. Symptom: In a fully populated switch, inserting a switch blade causes numerous Interface Control Checks (IFCC) on mainframe channels. Mainframe will try to recover from these errors. These will also cause CALL HOME to support. Solution: The fix is to not do the rebalance operation when a new blade is inserted while running in a FICON environment. Customer Impact: There could be disruption to the existing traffic flows. Reported in Release: V5.0.1
DEFECT000059443	High	Summary: MVS System reports Interface control checks on CP removal Symptom: Interface errors during repair action involving removal of a CP in a FICON Environment Solution: Closed as a duplicate of 59048. Customer Impact: There may be some missing internal routes due to this defect. Probability: High Reported in Release: V5.0.1

Defects Closed in Fabric OS v5.0.1b		
Defect ID	**Severity**	**Description**
DEFECT000059454	High	Summary: In the FICON CUP tab in Webtools the "Device Based Routing" option needs to be changed to "Port Based Routing". Symptom: Enhancement request to change Device Based Routing to Port Based Routing in FICON environments. Solution: Changed behavior of button to enable Port Based Routing. Reported in Release: V5.0.1
DEFECT000059533	High	Summary: FSPF segment fault in de-reference a NULL lsdbe during sending RTE domain unreachable update Symptom: In a disruptive fabric environment, where domain is added and removed from the fabric, segment fault in FSPFd may occur which will trigger an HA failover. Solution: check for null pointer before de-reference link-state record in domain unreachable update to RTE. Reported in Release: V5.0.1
DEFECT000059539	High	Summary: SW4012 becomes unresponsive to enclosure requests to arbitrate loop through the I2C bus controller Symptom: If diagnostic post is enabled, SW4012 will stop responding to arbitration requests for the enclosure-to-switch communication path after the first diagnostic step is executed. Solution: Correct the algorithm designed to handle the case where the I2C device has been reset by the POST diagnostics. Workaround: Disabling diagnostic POST will allow the arbitration logic to function without disruption. Reported in Release: V5.0.1
DEFECT000059616	High	Summary: SW48000 displayed ASSERT - Failed expression: rg->rg_paths[snode->n_id.n_inst][dnode->n_id.n_inst] == 0 and OOPs after slotpoweroff either a port blade(either C16 or C32) Symptom: Upon execution of a number of actions on SW48000 with traffic running, like remove/reinsert standby CP, turn on/off trunking, disable/enable switch, hafailover, and finally when slotpower off on a port blade(either C16 or C32), get ASSERT error on RTE. Following the ASSERT failure, the switch rebooted and Oops occurs constantly. Solution: To ensure iod remains set through rapid multiple failovers. Reported in Release: V5.0.1

Defects Closed in Fabric OS v5.0.1b		
Defect ID	**Severity**	**Description**
DEFECT000059649	High	Summary: Model Number in Sense ID data not correct Symptom: MVS errors with I/O Ops. commands Solution: Modified the code which was computing the Model Number to handle switches with more than 128 ports Probability: High Reported in Release: V5.0.1
DEFECT000059694	High	Summary: Read Port Descriptors command (FICON) does not return bit zero set to "1" on all unimplemented ports Symptom: Unit checks from CUP Device on MVS System IPL Solution: Fixed the code so that all unimplemented ports, starting from the port number above the maximum to port number 256, will have bit zero set to "1". Customer Impact: Some MVS I/O Ops commands on the CUP Port fail Probability: Low Reported in Release: V5.0.1
DEFECT000058928	Medium	Summary: Port 23 on slot 10 shows non-trunking config on "portcfgshow" Symptom: Port 23 on slot 10 shows up as non-trunking when running "portcfgshow". Running a "configshow" shows duplicate ports for 246 (slot 10/port 22) and no entry for port 247 (slot 10/port 23). After setting trunk on port using "portcfgtrunkport 1", the correct port (247) will show up again under "configshow" Solution: There was a typo in default table which missed port 247 and instead contains two entries for 246. Fix is to just correct this one. The default values do not affect any changes to the values to port 247, which will be written as a correct entry. Service Request# RQST00000039284 Reported in Release: V5.0.1

Defects Closed in Fabric OS v5.0.1b		
Defect ID	**Severity**	**Description**
DEFECT000059561	Medium	Summary: DLS change is not synced over to standby CP. This causes reroute and frame drop on existing ports when adding a new host with DLS turned off. Symptom: The "new" setting of DLS/IOD is not synced over to the standby CP. So, when there is a failover (due to "hafailover" or active CP plug-out), the new active CP would NOT have the new setting change that was made earlier. The result is that even DLS is set as OFF, disable/enable an F port still causes traffic reroute for all ports in the switch. Solution: Process IOD and DLS change management preparation on the standby CP even if there is no change to the routing policy. Reported in Release: V5.0.1
DEFECT000059618	Medium	Summary: WT EZ does not recognize the factory default zoning for SW 200E switch. Symptom: EZSwitchSetup states it is not configured for default zoning after it has just been instructed to restore defaults. Solution: Changed the warning message that pops up when user clicks on restore to factory default zoning to inform the user that this action will restore factory default zoning and that it will overwrite any previous zoning modifications done. The new message is "You have chosen to restore default Fixed zoning, which means that current zoning will be overwritten. Do you want to continue?" Reported in Release: V5.0.1

Closed Defects in Fabric OS v5.0.1a and Closed in 5.0.2

Defects Closed in Fabric OS v5.0.1a		
Defect ID	**Severity**	**Description**
DEFECT000057565	Critical	Summary: Oops: kernel access of bad area, sig: 11 Symptom: With a SW4012 running 5.0.0_beta code and ISLs connected to an embedded storage switch, run ACU for SSP and then run traffic. Run ACU again to make more LUN allocation, the SW4012 may panic. Solution: A null function pointer was called when an unexpected error happened during autonegotiation. The null pointer has been replaced with valid function call which does nothing and the error is handled properly. Customer Impact: This problem has a greater chance of occurrence only in SW 4012 because its internal ports constantly do autonegotiation until a server is attached. On other switches, this is not the case. Probability: Low Service Request# RQST00000038087 Reported in Release: V5.0.0
DEFECT000058603	Critical	Summary: When a PDCM matrix save fails no indication of location of error Symptom: If a port address name is invalid there is no indication of which port has an invalid name and must be corrected before the PDCM matrix maybe saved. Solution: When there is no change in name of a port, the FABOS returns a positive error code which should be ignored. Workaround: Manually clear all port address names and replace with valid names. Customer Impact: Could result in customer re-entering port address names. Probability: Medium Reported in Release: V5.0.1

Defects Closed in Fabric OS v5.0.1a		
Defect ID	**Severity**	**Description**
DEFECT000057037	High	Summary: Memory corruption when management software sends fabric slot information request through msd, which causes a switch panic. Symptom: kSWD kill of msd, portlogdump has following entry earlier: msd msRemQ 255 f004 00fffc7b,00fffc2c,10000060,69805fe1 <-- GSLOTD Solution: The response payload is larger than the allocated memory space, causing memory corruption when data is copied. The fix is to allow the correct length during copy of the response. Customer Impact: This problem occurs when FM is in the fabric with multiple switch views open and a fabric slot information request is performed. Probability: Low Service Request# RQST00000037753 Reported in Release: V4.2.2
DEFECT000057631	High	Summary: DCC policy is not enforced properly after failover/reboot/fastboot. Symptom: DCC_POLICY is not enforced if only 1 CP is rebooted or fastbooted during either cold or warm recovery. Rebooting or fastbooting both CPs does not show any error. Solution: DCC policies were not being converted from file to shared memory on standby. The solution is to update the shared memory after the failover before attempting to push the DCC policies down to the kernel, such that the policies are converted from file to shared memory again when the switch becomes active. Workaround: Issue a subsequent secpolicyactivate after the reboot/fastboot completes to reestablish the DCC policy. Customer Impact: The DCC policy is incorrect, and the user will have to establish the correct one by issuing a subsequent secpolicyactivate after the reboot/fastboot completes. Probability: High Reported in Release: V4.4.0

Defects Closed in Fabric OS v5.0.1a		
Defect ID	**Severity**	**Description**
DEFECT000057675	High	Summary: CUP Port returns F-Reject not available to PLOGI Symptom: CUP Port goes offline and not able to vary back online Solution: Fix is to cache the 'ficu_licensed' during warm recovery instead of relying on SW_ONLINE SCN. Probability: Medium Reported in Release: V5.0.1
DEFECT000058208	High	Summary: A memory leak causes out of memory (OOM) kill of evmd if Fabric Manager opens sessions with event listener through API during end-to-end performance monitoring. Symptom: Observe [EVMD-5000] when FM open event listener and switch panic with Out of Memory: Killed process 653 (evmd0). VM size = 86684 KB, Runtime = 84379 minutes, CPU time = 1 sec. Solution: When Fabric Manager (FM) performs end-to-end performance monitoring through a FOS 4.4 switch, an event session is being opened by the API library every time a new API session is created by FM. There is a 1/2 k byte leak for every session opened. Workaround: Do not enable any periodically scheduled API based operations from Fabric Manager (for example: PM/APM, Change Management snapshots). Turn off APM in Fabric Manager by simply selecting "Off" radio button and "Save." Turn off change management by clicking "Manage Profiles" menu item (Tools -> Change Management -> Manage Profiles menu in Fabric Manager) and edit profiles. Customer Impact: With FM opening event session through API, a small amount of memory leak occurs for that session. This happens between FM4.2/4.4 and FOS4.4 when FM pulls end-to-end performance data or performs change management periodically. This defect does not apply to releases prior to FOS4.4.0. Service Request# RQST00000038385 Reported in Release: V4.4.0

Defects Closed in Fabric OS v5.0.1a		
Defect ID	**Severity**	**Description**
DEFECT000058340	High	Summary: Channel errors on FICON Channels during concurrent firmware install. Symptom: Many channel errors during firmware upgrade Solution: "Inconsistent FICON CUP filter setup" problem was encountered. This is one of the two known Zoning/Filtering problems. The fixes for these two zoning/filtering problems are in some common code areas and should be fixed together: 1) hafailover generates "Inconsistent FICON CUP filter setup" messages for all the offline ports. 2) I/O stops when a perfAddUserMonitor command is set up. Workaround: Don't do a firmware install while traffic is running through the switch. Customer Impact: High volume of error messages and possible job appends. Probability: High Reported in Release: V5.0.1
DEFECT000058587	High	Summary: SW3016 "configsave -restore" function no longer works because "configsave -factory" is broken Symptom: The SW3016 Restore Factory Configuration operation will not work properly because of a problem in the algorithm that is used to save the factory configuration at the time the unit is manufactured. Solution: The function responsible for saving the factory defaults has been updated to handle a new format of the control file. Customer Impact: This defect does not affect SW3016 units already in the field. This defect only affects future units that would have been manufactured using 5.0.1 as the base software release. SW3016 units manufactured with 5.0.1 do not successfully save the factory values for the configuration files. Probability: High Reported in Release: V5.0.1
DEFECT000058824	High	Summary: Found memory leak in proxy switch ARR when target switch does not have IP connectivity. Symptom: the arr process virtual memory usage will slowly increase and eventually take up memory and eventually cause the switch to reboot Solution: The fix was to free memory that previously had not been freed Probability: Low Reported in Release: V4.4.0

Defects Closed in Fabric OS v5.0.1a		
Defect ID	**Severity**	**Description**
DEFECT000058864	High	Summary: Interface Control Checks when the PCDM Matrix is changed with traffic running Symptom: Interface Control Checks running I/O Ops. program to modify the PDCM Matrix. Solution: When PDCM is changed, NS or Zoning would reprogram the affected port's CAM. The current code misses disable zoning before reprogramming. This would cause IO traffic disruption when CAM is reprogrammed. The fix is to disable zoning before reprogramming ports and after all the affected ports are reprogrammed enable the zoning. Fix is done in both Zoning and NS areas. Customer Impact: Intermittent loss of frames giving Interface Control Checks in FICON environment. Probability: High Reported in Release: V5.0.1
DEFECT000059324	High	Summary: SW4012 returns wrong value for SNMP cpqRackNetConnectorModel field Symptom: SNMP request for cpqRackNetConnectorModel will see value "BRD0000CA" instead of "Brocade 4Gb SAN Switch." Solution: Change string value to "Brocade 4Gb SAN Switch." Customer Impact: Without this change, customer will see "BRD0000CA" instead of "Brocade 4Gb SAN Switch for HP p-Class BladeSystem;" however, system will function correctly in all other respects Reported in Release: V5.0.1
DEFECT000057932	Medium	Summary: Refresh operations in Web Tools Switch View, Name Server, Switch Events, and Fabric Events not reflected in "Last Updated" status messages Symptom: The timestamp updates automatically at 60-second intervals, irrespective of user- or system-generated refresh events, when every invocation of a refresh operation, either manual or timed auto-refresh, should update the timestamp displayed in the "Last Updated" status message. Solution: Correct a merge error. Customer Impact: Inaccurate or misleading information about the last refresh time is displayed for Name Server, Switch Events, and Fabric Events. Probability: High Reported in Release: V5.0.1

Defects Closed in Fabric OS v5.0.1a		
Defect ID	**Severity**	**Description**
DEFECT000058419	Medium	Summary: Firmware upgrade from 5.0.1 'main' to GA build fails, Standby CP not accessible for upgrade Symptom: Customer cannot upgrade the firmware to GA release v5.0.1 without doing a "firmwareupgrade -s" on each CP which upgrades the primary partition first not the secondary or backup partition. Also, when using the "-s" option, the remote CP will upgrade the primary partition first. Solution: Modify standby CP logic to update our packet filter when IP address is changed. Customer Impact: After changing the IP address of the standby CP, the CP will lose external IP access until it's rebooted or becomes the active CP due to HA failover. Service Request# RQST00000038765 Reported in Release: V5.0.1
DEFECT000059227	Low	Summary: RNIDS vanish on display Symptom: Missing RNIDS on Ports display if FMSMode is disabled on the switch Solution: FOS must return the RNIDS when the FMSMODE is disabled on the switch. Customer Impact: FOS will fail to return RNID information after the FMSMODE is disabled, but FICON devices continue to operate on the switch. Reported in Release: V5.0.0