BROCADE

Brocade Fabric OS v5.3.0
Release Notes v3.0

July 13, 2007

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v5.3.0 Release Notes v1.0	First release	June 15, 2007
Brocade Fabric OS v5.3.0 Release Notes v2.0	Corrected references to Brocade 7600	June 18, 2007
Brocade Fabric OS v5.3.0 Release Notes v3.0	Edits to the Fabric Scalability Section. Updated defect tables. Added update for Web Tools Administrator's Guide	July 13, 2007

Contents

Overview

Brocade Fabric OS v5.3.0 supports two new hardware blades for the Brocade 48000 director: FC10-6 Fibre Channel port blade and FA4-18 application blade. In addition, Fabric OS v5.3.0 supports a new application platform, the Brocade 7600.

- The Brocade FC10-6 blade is the new 6-port 10 Gbit Fibre Channel port blade designed for the Brocade 48000 director. This blade is designed to extend the value of the FC infrastructure to include 10 Gbit/sec FC and DWDM connected SANs. The Brocade FC10-6 blade provides the same high availability features that exist in the Brocade 48000 director today, satisfying the stringent requirements expected of an enterprise-class director.
- The Brocade FA4-18 application blade is an advanced FC director blade that is capable of enabling fabric intelligence by hosting storage management applications that provide storage virtualization, data mobility, and data protection functionality. The FA4-18 is designed for the Brocade 48000 Fibre Channel director and provides the same high availability and RAS features that exists in a Brocade 48000 director and which are expected in an enterprise class SAN.
- The Brocade 7600 application platform is a fixed configuration, 1U high chassis that is capable of enabling fabric intelligence by hosting storage applications that provide storage virtualization, data mobility, and data protection functionality. The Brocade 7600 is designed to provide the same high availability and RAS features that exist in all Brocade platforms utilized in an enterprise class SAN.
- The Brocade 200E now supports deployment as an Access Gateway. This innovative technology from Brocade allows simplified, interoperable fabric expansion through the use of NPIV, and was previously only available for embedded blade server switches. With support on the 200E, environments that wish to deploy stand-alone switches can now take advantage of the benefits of Access Gateway.

Fabric OS v5.3.0 supersedes Fabric OS v5.2.0, v5.2.1 and v5.2.2. All users are strongly encouraged to upgrade to v5.3.0 as soon as they have access to it.

New Fabric OS Features

The new features in the Fabric OS v5.3.0 release are summarized below;

- IPv6 support for the management ports
- Firmware download enhancements
  - Support for SCP (Secure Copy)
  - Support for passive FTP
- iSCSI blade – FC4-16IP enhancements
  - Support for iSCSI re-direction
  - Support for CHAP binding
  - Support for LUN delete from a virtual target
- Access Gateway mode support on the Brocade 200E
- Access Gateway enhancements:
  - Web Tools support
  - Fabric Manager support
  - NPIV on F_Ports
- Fibre Channel Routing enhancements
- IP Broadcast zone support
- IP over FC also via FCR
- IP Filter support (formerly MAC and Management port ACLs in Secure Fabric OS (SFOS))
- Support for FCS with base Fabric OS (formerly in SFOS)
- Support for multiple NTP servers
- Security Enhancements
  - Support for security Admin role
  - Support for account lock-out for admin role.

    - Support for strong password policies preventing repeat or sequence characters
    - P-EAP/MS-CHAPv2 support for RADIUS
- FC-IP
    - Fast Write and Tape Pipelining are supported over secure tunnels
    - Differentiated Services Code Point (DSCP) markings.
- New FC Fast Write feature

RAS (Reliability, Availability, Serviceability)

- The RASLog has been modified to support IPv6. RAS will also obsolete **traceftp** and **savecore** CLI and add its functionality to **supportsave** and **supportftp**.

Management

- Fabric OS 5.3.0 adds a new user role, the secAdmin or Security Administrator. This role has responsibility for logging, auditing, security administration and user management. The addition of the secAdmin role allows users to isolate security management from complete Administrator management.

Security

- All remaining essential elements of SFOS have now been integrated into the base Fabric OS 5.3.0. (Fabric OS v5.3.0 will be the last major release that is compatible with SFOS)
- FICON Cascading no longer requires SFOS.
- MAC policies have now been replaced by IP filters, allowing configuration of acceptable IP addresses and ranges that may gain management access to the switch.
- Protected-Extensible Authentication Protocol (P-EAP with MSCHAP-v2) support for RADIUS.
- DH-CHAP now supported for authentication of HBAs and end-devices in addition to switches.
- Additional password strengthening options.
- Lockout of Admin users that fail authorization.
- Flexible E_Port authentication settings, allowing better interoperability options for fabrics with varying levels of support. Certificate authentication is now optional.
- Auditing of authorization attempts.

Other

- New optional FC Fast Write feature for the Brocade 7500 and FR4-18i provides optimization and performance improvements for synchronous SCSI write operations.
- SAS Re-direction provides simplified virtualization configuration.
- Various Request for Enhancements (RFE)

New Web Tools Features

New Web Tools features in the Fabric OS v5.3.0 release are summarized below.

- Usability enhancements
  - Web-started GUI
  - Revamped Switch Explorer
  - Single-signed application
  - Common GUI components with new search and export capabilities
  - "Advanced" vs. "Basic" views in Switch and Port Admin modules
  - Progress bars, other window handling improvements

- New platform and hardware support
  - FA4-18 blade (including separate FWDL and blade IP setting)
  - Brocade 7600 application platform
  - FC10-6 blade
- Access Gateway Enhancements:
  - Full configuration of Access Gateway parameters such as port mapping, Failover and Failback policies, etc.
  - Tabular display of port mapping, port settings, port status, and WWN of attached devices.
- iSCSI setup wizard for improved usability
- IPv6 support
- Support for Security Admin role, P-EAP protocol
- WTEZ Switch Setup enhancements
- Passive FCS support (enforcement but no configuration)
- IP Filtering
- FC Fast Write support

Optionally Licensed Software

This Fabric OS release includes all basic switch and fabric support software, as well as the following optionally licensed software that is enabled via license keys:

- Brocade Extended Fabrics—Up to 500 km of switched fabric connectivity at full bandwidth over long distances
- Brocade ISL Trunking Over Extended Fabrics—Enhanced to enable trunking over long-distance links of up to 250 km
- Brocade Fabric Manager—Administration, configuration, and maintenance of fabric switches and SANs with host-based software
- Brocade Advanced Performance Monitoring—Performance monitoring of networked storage resources
- Brocade Fabric Watch—Monitoring of mission-critical switch operations
- High Performance Extension (formerly "FC-IP")—Fibre Channel over IP extension includes FC-IP trunking, multi-tunnel support, compression, and the new FC Fast Write feature.

Licensed Software Bundle as Standard

The following licensed software is bundled with the hardware and no additional purchase is necessary:

- Brocade Web Tools—Administration, configuration, and maintenance of fabric switches and SANs
- Brocade Advanced Zoning—Division of a fabric into virtual private SANs
- IPSec – IP Security (for the Brocade 7500 and FR4-18i blade in the Brocade 48000)

Supported Switches

Fabric OS v5.3.0 adds support for the FC10-6 blade and the FA4-18 application blade. Both blades are designed to function within Brocade 48000 director. Fabric OS v5.3.0 also supports the Brocade 200E, 3014, 3016, 3250, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, 7500, 7600, 24000, and 48000.

Access Gateway is also supported by Fabric OS v5.3.0, and is supported on the same embedded switches as 5.2.0. Access Gateway is also supported on the 200e beginning with 5.3.0.

IMPORTANT: The SilkWorm 12000 is not supported in Fabric OS v5.3.0. In addition Fabric OS v5.3.0 does not run on the SilkWorm 2000 series, 3200, 3800 or AP7420. However, it will operate properly with them in the same fabric.

Any enhancements and defect fixes for these platforms will be delivered in Fabric OS v5.3.x releases.

Standards Compliance

This software conforms to the 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*

Technical Support

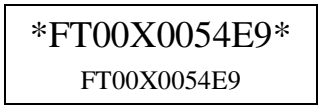
Contact your switch supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information immediately available:

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:

- Brocade 3014—Top of the chassis, under the insertion arm
- Brocade 3016, 4012, and 4024 —Bottom of the switch module
- Brocade 4016 and 4018— Top of the switch module
- Brocade 4020—Side of the switch module
- Brocade 200E, 3250, and 3850—Bottom of the chassis

- Brocade 3900—Non-port side of the chassis
- Brocade 4100, 4900, and 7500—On the switch ID pull-out tab located inside the chassis on the port side on the left
- Brocade 24000 and 48000—Inside the chassis next to the power supply bays

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

- Brocade 200E, 3014, 3016, 3250, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, and 7500 switches and SilkWorm 12000 and Brocade 24000, and 48000 directors provide the license ID. Use the **licenseIDShow** command to display the license ID.
  - All other Brocade switches provide the switch WWN. Use the **wwn** command to display the switch's WWN.

Important Notes

This section lists information that you should consider before you use this firmware release.

Fabric OS Compatibility

The following table lists the earliest versions of Brocade software supported in this release, that is, the *earliest* supported software versions that interoperate. Brocade recommends using the *latest* software versions to get the greatest benefit from the SAN.

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

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

Fabric OS Interoperability with Brocade Switches and Firmware	
Switches: SilkWorm 2000 Series and Brocade 6400	Fabric OS v2.6.2 [1]
Switches: Brocade 3000 and 3600, SilkWorm 3200 and 3800	Fabric OS v3.2.1 and higher
Switches: Brocade 200E, 325x, 385x, 3900, and 4100 **Embedded Switches**: Brocade 3014, 3016, and 4012 **Directors**: SilkWorm 12000, Brocade 24000, and 48000 (without FR4-18i blade)	Fabric OS v5.0.1
Embedded Switch: Brocade 4020	Fabric OS v5.0.2
Switches: Brocade 200E, 325x, 385x, 3900, and 4100 **Embedded Switches**: Brocade 3014, 3016, 4012, and 4020 **Directors**: SilkWorm 12000, Brocade 24000, 48000 (without FR4-18i blade)	Fabric OS v5.0.3
Switches: Brocade 200E, 325x, 385x, 3900, and 4100 **Embedded Switches**: Brocade 3014, 3016, 4012, 4016, and 4020 **Directors**: SilkWorm 12000, Brocade 24000, 48000 (without FR4-18i blade)	Fabric OS v5.0.4

Fabric OS Interoperability with Brocade Switches and Firmware	
Switches: Brocade 200E, 325x, 385x, 3900, and 4100 **Embedded Switches**: Brocade 3014, 3016, 4012, 4016, 4018, 4020, and 4024 **Directors**: SilkWorm 12000, Brocade 24000, 48000 (without FR4-18i blade)	Fabric OS v5.0.5
Switches: Brocade 200E, 325x, 385x, 3900, 4100, and 7500 **Embedded Switches**: Brocade 3014, 3016, and 4012 **Directors**: Brocade 24000 and 48000 (with or without FR4-18i blade) **Router**: Brocade 7500	Fabric OS v5.1.0
Switches: Brocade 200E, 325x, 385x, 3900, 4100, and 7500 **Directors**: Brocade 24000 and Brocade 48000 (any combination of FC4-16, FC4-32, FC4-48, FC4-16IP, and FR4-18i blades) **Router**: Brocade 7500	Fabric OS v5.2.0 [1]
Router: SilkWorm AP7420	XPath 7.4.X [2]
Fabric OS Interoperability with McDATA Switches and Firmware [2]	
Intrepid 6140 and 6064	EOS v7.x, v8.x, v9.x[2]
Sphereon 3216, 3232, 4300, 4500, 4400 and 4700	EOS v7.x, v8.x, v9.x [2]
Intrepid 10000	EOS v9.x[2]

(1) Fabric OS v2.6.2 can interoperate with Fabric OS v5.3.0 through the FC routing capability of the SilkWorm AP7420, Brocade 7500, or FR4-18i blade in the Brocade 48000 director.

(2) Fabric OS and McDATA E/OS v4.x, v5.x, 6.x can interoperate through the FC routing capability of the SilkWorm AP7420 only. Fabric OS and McDATA E/OS v7.x, v8.x and v9.x can interoperate through the FC routing capability of the SilkWorm AP7420, Brocade 7500, or FR4-18i blade in the Brocade 48000.

Firmware Upgrades and Downgrades

- Brocade does not support upgrading from more than two previous releases, for example, upgrading from Fabric OS v5.1.x to v5.3.x is supported but upgrading from Fabric OS v5.0.x or a previous release directly to v5.3.x is not.
- Currently, Brocade does not support downgrading from Fabric OS v5.3.0 to 5.2.1_NI. In order to downgrade from Fabric OS v5.3.0 to v5.2.1_NI you must first downgrade to Fabric OS v5.2.1 or Fabric OS v5.2.2.
- The Brocade 5000 running Fabric OS v5.2.1_NI may not be upgraded to Fabric OS 5.3.0. Fabric OS v5.3.0 does not support Native Interoperability for deployment in M-EOS fabrics.
- Fabric OS v5.1.1 supports a maximum MTU value of 2284. However, Fabric OS v5.2.1 and v5.3.0 support an MTU value of up to 2348. Prior to downgrading the Fabric OS to v5.1.1 the user must change the MTU size less than or equal to 2284. If the configuration of the target unit has an MTU value greater than 2284, the FCIP tunnels will not go online after firmware downgrade.
- Upgrading a switch from Fabric OS v5.0.x or a previous release to v5.3.0 requires a two-step process: first upgrade to v5.1.x or v5.2.x and then upgrade to v5.3.0. In addition, prior to upgrading to v5.3.0 Device-based routing must not be in use, otherwise the upgrade will fail. You can use the **aptPolicy** command to verify the routing policy.

- Chassis configuration options 3 and 4 are no longer supported for the Brocade 48000; see the "Brocade 48000 Chassis Configuration Options" table for details.
- Brocade supports downgrading up to two previous releases, for example, if you upgrade to Fabric OS v5.3.0 from v5.1.x, you can revert back to v5.1.x. However, you cannot downgrade from Fabric OS v5.3.0 to v5.0.0 or to a previous release.
- If the Brocade 48000 contains an FC10-6 or an FA4-18 blade or has enabled any of the new software features in Fabric OS v5.3.0, such as IPv6, you cannot downgrade below Fabric OS v5.3.0. If you wish to do so, you must a) remove these features, b) physically remove the blade(s), and then c) downgrade the firmware.
- If the Brocade 48000 has FC4-48 or FC4-16IP blades installed or any new software features from Fabric OS v5.2.0, such as FCR trunking and administrative domains for virtual fabrics, you cannot downgrade below Fabric OS v5.2.0. If you wish to do so, you must a) remove these features, b) physically remove the blade, and then c) downgrade firmware.
- When you downgrade to Fabric OS v5.1.x, you will also need to remove the v5.2.x features (and any installed FC4-48 or FC4-16IP blade). In all cases, the firmwareDownload command will guide you to remove any features and blades that need to be removed.
- If McDATA i10K in the edge fabric is connected to FCR, before downgrade to Fabric OS v5.2.x or v51.x, disconnect the i10K switch. Failure to do so may result in iswitchd core dump.

Fabric Scalability

Fabric OS v5.3.0 supports the same fabric scalability as Fabric OS v5.0.x and v5.2.x, that is, 2,560 ports with 50 domains.

Fabric OS v5.3.0 using interop mode 1 supports interoperability with McDATA Open Fabric mode for fabrics up to a maximum of 200 ports and 4 domains.

For FC Routing environments, the following scalability numbers apply:

Fibre Channel Routing Scalability	
Max # edge fabrics per metaSAN	32
Max # edge fabrics per chassis	16
Max # local switches per edge fabric	26
Max # front domains per edge fabric	10
Max # translate domains per edge fabric	33
Max # total domains per edge fabric	69
Max # local switches per edge fabric (M-EOS fabric)	16[1]
Max # WWNs per edge fabric (M-EOS fabric)	800[1]
Max # imported devices per fabric (M-EOS fabric)	300[1]
Max # local switches per backbone fabric	10
Max # translate domains per backbone fabric	33
Max # total domains per backbone fabric	69

Fibre Channel Routing Scalability	
Max # FCR switches per metaSAN	6
Max # FCR switches per backbone fabric	6
Max # local WWNs per edge fabric	1200
Max # local WWNs per backbone fabric	512
Max # imported devices per fabric	1000
Max # local & remote WWNs per fabric	1300
Max # device database entries per metaSAN	10000
Max # LSAN zones per metaSAN	3000[2]
Max # entries per LSAN zone	64
Max # hops between edge switches	12
Max # EX_Port s to an edge fabric from FCR	4 8(4G)
EX_Port s per FCR	32

Table Notes:

1) M-EOS fabrics must be running M-EOS 9.x firmware or later.

2) All BB FCRs with Fabric OS v5.3.0 and above

Other Notes:

1) IPFC over FCR is only supported for edge to edge.

2) FC Fast Write is only supported for edge to edge.

FICON Support

For Fabric OS v5.2.0 and later, the Switch Connection Control high integrity requirement for cascading FICON is available in the standard base Fabric OS. End users can now cascade FICON without purchasing a separate Secure Fabric OS license.

NOTE: The FC4-48 Fibre Channel port blade is not supported to connect to System z environments via FICON channels or via FCP zLinux on System z. To attach the Brocade 48000 director o the System z environment, use an FC4-16 or FC4-32 Fibre Channel port blade**.**

PKI Certification

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 on how to obtain certificates from the Brocade Certificate Authority.

Fabric OS

Diagnostics backport test

The backport test passes only in a) a pure Brocade 24000 director or b) a Brocade 24000 system with no FC4-16 blades and under Option 5.

Do not run backport tests in any configuration other than the two listed above; use the minicycle test instead.

Diagnostics spinsilk Test

The following configurations *will pass the spinsilk test*:

- Pure Brocade 24000 director (only CP2 and FC-16 blades)
- Pure Brocade 48000 director, option 5
- Pure Brocade 48000 director, option 5 (with FC4-16 blades)

The following configurations *will fail the spinsilk test;* use the minicycle test instead*:*

- Mixed Brocade 24000 director (with either CP4 or FC4-16 blades)
- Pure Brocade 48000, option 1

"Pure Brocade 48000" refers to a director with CP4 and FC4-16 blades only.

Others

The following are known issues in this release of Fabric OS.

Areas	Description
Brocade 7500	• Brocade 7500 fans operate at the correct speed, that is, at maximum on bootup. However, this initial speed may trigger an error message that indicates that the speed is too high ("above threshold"). You can disregard this message; the fan speed is adjusted to a nominal speed shortly after bootup. This message is benevolent. The fan speed will be adjusted to a nominal speed shortly after bootup.
Brocade 48000	• Before moving the slider UP on a Control Processor blade that is being activated, observe that amber LED is not ON for the active CP for at least 5 seconds and all LEDs are off on new inserted CP. • In a core-edge design, when a fully populated 384-port Brocade 48000 (populated with 8 FC4-48 blades) is an edge switch in a large SAN, it can experience high CPU utilization and may panic if it becomes a principal switch. SAN design best practice recommends deploying a high port-count switch as both core and principal switch to reduce fabric stress and provide ease of management.

Areas	Description
FC4-48 port blade for the Brocade 48000	• Configure command only gives a maximum login per port setting. The command allows over 127, where ports for the FC4-48 blade will honor that value as long as its share areas values are 127 or less. • Before replacing FC4-32 blade with FC4-48 blade, restore ports 16 – 31 of the FC4-32 blade if these ports are used for port swapping. Failure to do so will fault the FC4-48 blade. The only way to restore back to original settings is to add the FC4-32 blade back in to the slot and port swap the ports back to port's default setting. • FC4-48 ports should not belong to the zone or in an administrative domain in which FICON devices are present. • FC4-48 blade does not support loop. Private L_Ports will be shown on these ports in switchShow, but will not participate in the fabric • The porttest and spinfab commands on any platform will not work on E_Ports connected to a FC4-48 port. • In a core-edge design, making an edge 384-port Brocade 48000 the principal switch causes high CPU utilization and may cause panics. SAN design best practice recommends moving the reduction of fabric stress and ease of management. • The FC4-48 Fibre Channel port blade is not supported to connect to the System z environments via FICON channels or via FCP zLinux on System z. To use the Brocade 48000 director to attach to the System z environment, please use the FC4-16 or FC4-32 Fibre Channel port blades
FC10-6 Blade	• Clear the long distance configurations from the FC10-6 ports prior to replacing the FC10-6 with a 4 Gbps blade. If the configurations are not cleared and you install a 4 Gbps blade, some ports may not come online due to a buffer allocation issue. To resolve it, re-install the FC10-6 blade and use **portcfgdefault** to clear the long distance configuration on each of the 10 Gbps long distance ports.
Firmware upgrade/downgrade	• When upgrading from Fabric OS v5.1.0x to v5.2.0x or v5.3.0, if there are two or more inter-fabric links (IFL) connected to an edge fabric, one IFL will stay online and the other IFLs will go online and offline. This will cause a temporary traffic disruption going from multiple IFLs to 1 IFL and then back to multiple IFLs. This is due to the front domain consolidation new feature in v5.2.0 where the IFLs connected to the same edge share the same front domain • When downgrading from Fabric OS v5.3.0 or v5.2.x to v5.1.0x, FC traffic will be disruptive if there is front domain consolidation prior to the downgrade even in the case of a single IFL. • Upon firmware download the FC4-16IP blade does not preserve disabled GE ports in disabled state. If you wish to retain GE ports in a disabled state across firmware download, you must configure them as persistently disabled.

Areas	Description
Fabric OS – CLI commands	• This release does not support underscore (_) as part of the name for dd and ddset in the **iscsicfg** command. • The **slotOff** and **slowOn** commands are now obsolete; use **slotPowerOff** and **slotPowerOn** instead. The **portLogPortShow** command is also now obsolete. • When performing a configdownload, you may receive a message stating "configDownload not permitted." An invalid parameter was passed to the switch. The invalid parameter could be from a switch security policy, such as the password policy, or the NTP server address. This causes a partial configuration to be downloaded onto the switch. For example, when an NTP server address is invalid, configdownload fails and all data processed prior to the NTP server address data had already been saved in the switch and cannot be backed out. To fix the problem, correct the invalid parameter and re-issue the configdownload command.

IPSec for FR4-18i blade	• IPSec implementation details:
	  o Pre-shared key
	  o Main mode (IKE negotiation protocol)
	  o Tunnel mode in ESP (Encapsulating Security Payload)
	• IPSec specific statistics not provided
	• No NAT or IPv6 support
	• Jumbo frames will not be supported on secure tunnels.
	• ICMP redirect is not supported for IPSec-enabled tunnels.
	• Only a single secure tunnel will be allowed on a port. Non-secure tunnels will not be allowed on the same port as secure tunnels.
	• Modify operations are not allowed on secure tunnels. To change the configuration of a secure tunnel, you must first delete the tunnel and then recreate it with the desired options.
	• Only a single route is supported on an interface with a secure tunnel.
	• An IPSec tunnel cannot be created using the same local IP address if ipperf is active and using the same local IP address (source IP address).
	• Unidirectional supported throughput is ~104Mbytes/sec and bidirectional supported throughput is ~90Mbytes/sec.
	• An IPSec tunnel takes longer to come online than a non-IPSec tunnel.

Distance mode	• Distance setting is not persistent. After a configuration uploads and downloads, distance settings will be lost and the desired distance will be shown as 0.

Areas	Description
FC Routing	• If a SilkWorm AP7420 is present in the backbone fabric, the command "fosconfig - disable fcr" may take up to 8 minutes to complete. If the AP7420 is replaced by a FR4-18i or Brocade 7500, the command completes immediately. • EX_Port trunking is not enabled by default. • FCR switch does not support an edge fabric with one McDATA switch set to 'never principal'. The EX_Port connected to that edge fabric will not come up. • FCR switch does not support edge fabrics that consist of McDATA switches with 'domain ID offset'. The EX_Port connected to that edge fabric may fail the RDI process and will not come up. EX_Port s come up disabled (failed to init in time) if attached to a Native mode switch running EOS 9.x that has non-default DID offset configured.
Security	• Remove any password enforced expiration of admin or root accounts before downgrading firmware to 5.0.1 or lower versions.
Diagnostics	• All offline diagnostics commands should be used only when the switch is disabled. • POST can fail if new SFPs are added during POST. SFPs should only be added while the switch is "online" or if the switch is powered off. • When you use the diagnostic commands **systemVerification** and **diagSetBurnin**, the switch or blade will fault when the burn-in error log is full. Clear the burn-in log before running **systemVerification** or **diagSetBurnin.** • If there are ISLs present on the switch that are not used for routing (due to them having higher linkcosts), disable the links before running **spinfab**.
HA	• If there is an already segmented port and backbone devices are exported to an edge fabric, a build fabric / fabric reconfiguration can occur after running **haFailover.** Ensure that there are no segmented ports before upgrading firmware.
Fabric Merge	• Do not try to merge fabrics with conflicting domain IDs over a VE_Port. Before merging two fabrics over FC-IP with VE_Ports at each end, it is recommended that all domain ID and zoning conflicts are resolved.
Scalability	• Support for Default Zoning policies have been added to Fabric OS v5.1.0. Typically, when you issue the **cfgDisable** command in a large fabric with thousands of devices, the name server indicates to all hosts that they can communicate with each other. To ensure that all devices in a fabric do not see each other during a **cfgDisable** operation, you can activate a *Default Zone* with policy set to "no access". If Default zoning policies are enabled, all **cfgEnable/Disable** commands and zoning changes must be run from a switch in the fabric running Fabric OS v5.1.0/v5.2.0. • In large fabrics with more than 1,000 ports, it is recommended that the MS Platform Database is disabled, it is also required that the Platform DB be disabled before downgrading to previous versions of Fabric OS. This can be done using the **msPLMgmtDeactivate** command.

Areas	Description
FRU insertion	• FW_FRU_INSERTED message is displayed twice when a power supply FRU is inserted and powered on. There is no functional impact.
System boot	• Not all Fabric OS services are available when the prompt becomes available during boot up. Wait for all the services to come up before using the switch or performing zoning actions.
Performance Monitoring	• If the user tries to save more than 512 monitors using the **perfCfgSave** command, some of the monitors may be lost.
Management – Proxy switches	• If you are using a Fabric OS v4.x switch as an API or SMI-S proxy to manage a v5.1.0 switch, you must be running Fabric OS v4.4.0d, as a minimum requirement.
FC Fast Write	• Only WWN zone (including normal zone and FC Fast Write zone) is supported on FC Fast Write enabled port. • Only single device loop port is supported. • NPIV (example Access gateway) port is not supported. • FCR backbone devices are not supported. That is FC Fast Write should not be enabled on backbone devices. • FCR edge to edge support is limited by all the target devices on given edge fabric that host talks to should be connected to a Brocade 7500 or FR4-18i in FC Fast Write mode. FC Fast Write should not be enabled on ports when testing the remote mirror application. • When a very high volume of traffic is being sent by host, FC Fast Write IOs may time out and frame may be dropped. • Within the context of FC Fast Write, L_Port is not supported in Fabric OS v5.3.0
iSCSI	• Enterprise storage array targets may not show up consistently in the disk management window of an iSCSI initiator when the same LUNs are mapped to two different virtual targets (VTs). When the initiator logs in to the VTs, the targets keep disappearing from the disk management window. If the session to one of the VTs is disconnected, the remaining VT appears and stabilizes in the disk management window. • Under certain conditions, hosts on an IP network may not be able to issue a ping command to iSCSI gateway ports in another subnet. You can work around this problem by issuing a ping command from the iSCSI gateway port. The hosts will then be able to successfully issue ping commands to the iSCSI gateway port. • An IP network disconnection lasting five seconds or more may cause COPA failure on the disconnected PC, which in turn may cause a loss of connection to an enterprise storage array • If traffic is run from hosts to certain targets with severe impairment conditions in the IP network for hours at time, throughput to the targets will drop, and may take up to 10 minutes to recover after the impairment condition is removed. Note that this problem is highly intermittent, and is unlikely to be seen in a customer environment. We believe that this issue is the result of host/target interaction, and is not the result of action on the iSCSI gateway. • A Microsoft windows PC host was unable to discover enterprise storage array LUNs. The Microsoft iSCSI initiator is able to discover targets if the software is uninstalled and reinstalled without the MPIO option.

Areas	Description
Broadcast Zones	• In Fabric OS v5.3.0, a zone with the name "broadcast" (case-sensitive) is a special zone for setting up recipients of broadcast packets. In Fabric OS versions earlier than v5.3.0, a zone named "broadcast" does not have special significance. Therefore, you must make sure that if a broadcast zone is configured, then the active and standby CPs should be running the same Fabric OS version. Otherwise an HA failover might change the zone configuration. Refer to the *Fabric OS Administrator's Guide* for additional information about broadcast zones.

Fabric OS RFEs Implemented in This Release

RFE Number	Description
2536	Currently the process of renaming an alias or zone is a very time consuming process, especially if you are making several changes. It would be of great benefit if we enhance the Fabric OS to include commands such as alirename
3191	When there's a corrupted zone config [under /etc/fabos/zone*], switch should detect is gracefully instead of rebooting as well as send update the error log through RASLog.
3199	Request for a new command to be added that will provide both the WWN and SN of the switch
3402	Enhancement request, faulty port in fabric watch.
3424	I cannot upgrade a Brocade switch that is on a NAT address because that requires passive FTP.
3740	Include the capability for the customer to specify a quality password policy that includes the ability to prohibit the selection of passwords with consecutive, identical characters.
3770	Provide the ability to set up tsclockserver to use multiple NTP servers in a failover situation? IE - one site NTP fails (DR scenario) there is a backup to be reached by the switches.
3991	Have RASLog message logged when a 2.x switch joins the fabric (Request from Brian Steffler)
3776	Add the functionality of HA failover functionality for Brocade 48K of notifying the customer when there is Ethernet chip (Oscillator chip) issue occurred.

Web Tools RFEs Implemented in This Release

RFE Number	Description
3969	Please provide individual Error counters for FC Ports from Port admin
3970	please provide SFP TX /RX power information in DB level from port admin from Web Tools
3971	Please make Clear Counter feature to reset all the counters that are being displayed

RFE Number	Description
3993	Unable to clear Brocade 7500 or FR4-18i GE port Error counters with 'portStatsClear' CLI command

Documentation Updates

This section provides information on last-minute additions and corrections to the documentation. The most recent Fabric OS V5.3.0 documentation manuals are available on the Brocade Partner Network: *http://partner.brocade.com/*

Brocade Fabric OS Administrator's Guide (Publication Number 53-1000448-01)

On page 12 before the instructions To set static addresses for the Ethernet network interface, insert the following text:

> On an AP blade, configure the two external Ethernet interfaces to two different subnets, or if two subnets are not present, configure one of the interfaces and leave the other unconfigured. Otherwise the following message will show up and also blade status may go into a faulty state after a reboot.
>
> Neighbor table overflow.
> print: 54 messages suppressed

On page 136, under the heading "Restoring a Configuration," a note should be placed before the next section stating the following:

> If a **configupload** command is issued on a non-FCR platform, such as the configuration file from a Brocade 7500 to a Brocade 7600, FCR-like parameters may be viewed in the uploaded data. This is harmless to the switch and can be ignored.

On page 182, under the section Downloading SAS and SA Applications to the FA4-18 blade, the following note should appear after the second paragraph:

> An SAS and SA firmwaredownload is unsupported while the switch is running POST.

On page 201, under the section 'Blade Troubleshooting Tips' add the following bulleted item:

> The director is unable to downgrade after removing FR4-18i blade.
>
> The persistent configuration changes are required to be done prior to the blade removal:
>
> - Either delete EX_Port configuration before removing the FR4-18i blade
> - Or insert a non-Brocade FR4-18i blade in the slot.
>
> Otherwise the system is prone to accidental configuration changes, for example in situations where the user may have done a slotpoweroff for debugging and not intended the EX_Port configuration to be cleared. Pre-install is designed to catch and prevent such accidental changes and requires explicit actions on the part of the user in such situations.

On page 239 in step 8 and page 236 the output for fcrfabricshow should display as follows:

switch:admin> fcrfabricshow

```
FCR WWN: 10:00:00:05:1e:13:59:00, Dom ID: 2, Info: 10.32.156.52 1080::8:800:200C:1234/64,

"fcr_7500"
EX_Port FID Neighbor Switch Info (WWN, enet IP, name)
-----------------------------------------------------------------
7    10 10:00:00:05:1e:34:11:e5 10.32.156.33 "7500" 1080::8:8FF:FE0C:417A/64
4    116 10:00:00:05:1e:37:00:44 10.32.156.34 "7500"


FCR WWN: 10:00:00:05:1e:12:e0:00, Dom ID: 100, Info:10.32.156.50 1080::8:60F:FE0C:456A/64

"fcr_7500"
EX_Port FID Neighbor Switch Info (WWN, enet IP, name)
-----------------------------------------------------------------------
4    95 10:00:00:05:1e:37:00:45 10.32.156.31 "7500"

FCR WWN: 10:00:00:05:1e:12:e0:00, Dom ID: 100, Info: 10.32.156.50, "fcr_Brocade 7500"
EX_Port FID Neighbor Switch Info   (WWN, enet IP, name)
-----------------------------------------------------------------------
4    95  10:00:00:05:1e:37:00:45 10.32.156.31 "Brocade 7500"
5    95  10:00:00:05:1e:37:00:45 10.32.156.31 "Brocade 7500"
6    95  10:00:00:05:1e:37:00:45 10.32.156.31 "Brocade 7500"
```

On page 253, under the IPFC over FCR section, put the following text after the last paragraph:

> If you have an FID with a pre-existing IPFC data session that you want to disable then the IPFC traffic across the FCR may not stop even after disabling the broadcasting to some edge fabrics. When you disable the IPFC traffic broadcast configuration it will take effect on the next ARP command. If there is an active IPFC data session through the FCR, disabling the FID on the FCR, using the fcrbcastconfig command, would be effective after clearing the ARP cache on the host of the IP devices forcing the IP devices to re-send ARP or after the IP devices send the periodic ARP command. Clearing the ARP cache forces the IP devices to re-send ARP or after the IP devices send the periodic ARP command.

Brocade 5000 Hardware Reference Manual (Publication Number 53-1000424-01)

On page 11, under the heading “Items included with the Brocade 5000,” replace the following bullet:

“• Power plug current/voltage rating: 15A/125V”

With:

“• Power plug current/voltage rating: 1.4A/125V”

On page 12, under the heading “Installation and Safety Considerations,” replace the following bullet:

“To install and operate the switch successfully, ensure that the following requirements are met:

• The primary AC input is 90-264 VAC (switch autosenses input voltage), 47-63 Hz.”

With:

“To install and operate the switch successfully, ensure that the following requirements are met:

• The primary AC input is 100-240 VAC (switch autosenses input voltage), 47-63 Hz.”

On page 22, Figure 2 LEDs on Prot Side of Brocade 5000, the captions for callouts 3 and 4 are reversed and should read as follows:

3 System Power LED

4 Power Supply Status LED

On page 30, under the heading "Facility Requirements," replace the following bullet:

"Electrical:

- Primary AC input 90-264 VAC (switch autosenses input voltage), 47-63 Hz."

With:

"Electrical:

- Primary AC input 100-240 VAC (switch autosenses input voltage), 47-63 Hz."

On page 31, in Table 2 "Power Supply Specifications," replace the "Input voltage value" with the following:

"100 - 244 VAC, Universal"

On page 33, under the heading Fibre Channel Port Specifications, the last paragraph should read as follows:

The ports are capable of operating at 1, 2, or 4 Gbit/sec and are able to autonegotiate to the higher of 1 or 2 OR 4 Gbit/sec.

Brocade 5000 QuickStart Guide (Publication Number 53-1000425-01)

On page 5, under the heading "Items included with the Brocade 5000," replace the following bullet:

"• Power plug current/voltage rating: 15A/125V"

With:

"• Power plug current/voltage rating: 1.4A/125V"

On page , under the heading "Site Planning and Safety Guides," replace the following bullet:

"The primary AC input is 90-264 VAC (switch auto-senses input voltage), 47-440 Hz."

With:

"The primary AC input is 100-240 VAC (switch auto-senses input voltage), 47-440 Hz."

Brocade 24000 Hardware Reference Manual (Publication Number 53-0000396-01)

On page 13, under the heading "Disconnect from Network and Fabric," add the following note:

> Note: the **switchShutdown** command is only used for dual domain directors and is used to stop traffic on a single domain.

Web Tools Administrator's Guide (Publication Number 53-1000435-01)

On page 2, in Table 1 and Table 2, change the Java Plug-In version from 1.5.0_06 to 1.6.0.

On page 3, under the heading "Installing Java on the workstation," replace the following sentence:

> Java Plug-in version 1.5.0_06 must be installed on the workstation for the correct operation of Web Tools.

With:

> Java Plug-in version 1.6.0 must be installed on the workstation for the correct operation of Web Tools.

On page 3, in the procedure "To install the JRE on your Solaris or Linux client workstation," replace step 1 and step 2:

> **1.** Locate the JRE on the Internet, at the following URL:
>
> *http://java.sun.com/products/archive/j2se/5.0_06/index.html*
>
> **NOTE**
>
> This URL points to a non-Brocade Web site and is subject to change without notice.
>
> **2.** Select **JRE 5.0 Update 6**.

With:

> **1.** Locate the JRE on the Internet, at the following URL:
>
> *http://java.sun.com/products/archive/j2se/6/index.html*
>
> **NOTE**
>
> This URL points to a non-Brocade Web site and is subject to change without notice.
>
> **2.** Click **Download JRE**.

On page 4, in the procedure "To install the Java plug-in on Windows," replace the last two bullet items in step 3:

- If no Java Plug-in is installed, point the browser to a switch running Fabric OS 5.2.0 or later to install JRE 1.5.0_06. Web Tools will guide you through the steps to download the proper Java Plug-in.
- If an outdated version is currently installed, uninstall it, reboot your personal computer, relaunch the browser, and enter the address of a switch running Fabric OS 5.2.0 or later to install JRE 1.5.0_06. Web Tools will guide you through the steps to download the proper Java Plug-in.

With:

- If no Java Plug-in is installed, point the browser to a switch running Fabric OS 5.2.0 or later to install JRE 1.6.0. Web Tools will guide you through the steps to download the proper Java Plug-in.

- If an outdated version is currently installed, uninstall it, reboot your personal computer, relaunch the browser, and enter the address of a switch running Fabric OS 5.2.0 or later to install JRE 1.6.0. Web Tools will guide you through the steps to download the proper Java Plug-in.

Open Defects in Fabric OS v5.3.0

As of June 7, 2007, the following defects are formally open. However, they are unlikely to impede you in your deployment of Fabric OS v5.3.0. When a workaround to an issue is available, it is provided. Otherwise, no recommended workaround is available at this time.

Deferred Defects

The following table lists defects that being retargeted to a future Fabric OS release.

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000072085	High	Summary: Switch panicked when the switch was being configured to interop mode and domain id was changed at the same time. Symptom: While setting up the fabric to interop mode, when domain id was also changed, one of the switches in the fabric panicked. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.0.5
DEFECT000077966	High	Summary: On an already fully utilized trunking group, a newly added slave port may not be ready to pass the first few frames right away. Symptom: Testing tools that do not retry may detect a few frames lost on the path through the new slave port. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.1

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000078694	High	Summary: After repetitive slotpoweroff/on, a panic happened on a Brocade 48000 with AP blade Symptom: Error message: "kSWD: Detected unexpected termination of: "[6]fabricd . . . " Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Low Reported in Release: V5.2.1
DEFECT000080864	High	Summary: FICON: When multiple instances of a FICON Test program are run on a single CUP port on 7500, CUP port may hang with channel timeout. Symptom: CUP Port hangs with channel timeouts Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.3.0
DEFECT000082405	High	Summary: Under stressful testing scenarios, under rare conditions, about 40 minutes after an overnight hafailover test started, the traffic running from a sw4100, through FC10-6 and FA4-16 to a sw AP7600 was terminated. Symptom: Traffic stopped during an overnight test Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Low Reported in Release: V5.3.0
DEFECT000082551	High	Summary: FICON: When multiple instances of a FICON test program send commands to a CUP port on 7500, CUP port may hang in busy state. Symptom: CUP Port hangs in busy state Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000082629	High	Summary: With interop mode set, a 3250 with v5.3 fails to display the switch name and IP address of the i10K in Open mode in the joined fabric. Symptom: With interop mode set, when a 3250 with v5.3 forms a fabric with an i10K in Open mode, switchshow and fabricshow do not show the switchname and IP address of i10K in fabric. Customer Impact: Usability issue, with no impact to functionality. Probability: High Reported in Release: V5.3.0
DEFECT000082815	High	Summary: FCR: Under some rare misconfiguration scenarios, sometimes the host does not see the target, when redundant links from edge to Back-bone fabric are segmented Symptom: When an edge fabric with redundant links to the BB is segmented, sometimes a target is lost. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.3.0
DEFECT000084815	High	Summary: When LSAN zone entries exceed maximum limit, one of the FCRs in dual BB configuration does not import devices Symptom: Customer may not able to use one FCR in dual BB fabric. Workaround: Remove excess LSAN zones so that the number of LSAN zones created is within the range of the local database limitations. To do that, perform the following steps: 1. Run portDdisable to disable all the EX_Port s that got this error message. 2. Run portDdisable to disable all the other EX_Port s on that FCR connected to the same edge fabrics that the EX_Port disabled in step 1 are connected to. 3. Use Zoning commands on the edge fabrics, to reduce the lsan zone entries on the edge fabrics. 4. Run portEnable on each EX_Port, one at a time, and verify that this error is not reported again. Customer Impact: None if recommended service procedures are followed carefully. Probability: Low Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000085220	High	Summary: Under extremely rare scenario, device entries may be removed from Name Server Data base if one AG NPIV port goes offline and devices try to come online through another NPIV port. Symptom: SMI device discovery is not working as expected. Workaround: Disable and enable the port on which the AG device is connected. Customer Impact: Minimal, since there is a workaround. Probability: Low Reported in Release: V5.3.0
DEFECT000085292	High	Summary: iswitchd panic when doing data migration using DMM Symptom: Issue only happens when DMM issues an invalid frame to the FOS switch. Defect within DMM has been fixed; therefore the panic of the FOS switch is not expected to happen. Workaround: Upgrade SAS application firmware. Customer Impact: Minimal, since there is a workaround. Probability: Low Service Request# RQST00000059419 Reported in Release: V5.2.0
DEFECT000085460	High	Summary: FCR: SANtester traffic does not flow from EOS8 native edge with redundant links to FOS edge with 4 devices per edge Symptom: Traffic can only flow in one direction between FOS and EOS8 native edge fabrics. Workaround: If the traffic does not flow, do portdisable/portenable on the ports connected to the McDATA edge fabrics. Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000085600	High	Summary: Performing continuous switchdisable/enable and bladedisable/bladeenable operations on a large number of switches in a large fabric may cause core principal switch to panic Symptom: Observed panic when running a script that performs switchenable and bladeenable. Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Low Reported in Release: V5.3.0
DEFECT000085775	High	Summary: Running continuous CP failover test overnight, observed Diag failure and FA4-18 became faulty. Symptom: FA4-18 became faulty due to Diag failure. Workaround: Slotpoweroff and on Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Low Reported in Release: V5.3.0:
DEFECT000085842	High	Summary: In a large fabric with several devices, and under rare conditions, while performing firmware upgrade in FCR backbone, when one switch goes through the reboot action, other switches in the FCR backbone may encounter evmd panic. Symptom: Evmd crashes and the following error message is seen: 2007/04/20-10:52:03, [KSWD-1003], 81722, FFDC, WARNING, BB1_7500_152c, kSWD: Detected unexpected termination of: "[14]evmd:0'RfP=965,RgP=965,DfP=0,died=1,rt=4294108048,dt=45236,to=50000,aJc=-910748,aJp=- Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000085923	High	Summary: iSCSI: CP panicked during stress testing of slot power off FC4-16IP blades Symptom: During slotpoweroff/on stress testing, CP panicked after 31 iterations of the test Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Low Reported in Release: V5.3.0
DEFECT000086754	High	Summary: During stressful slotpoweroff/on, bladedisable/enable commands testing on Brocade 48000 (large fabric), iswitchd hit an ASSERT and CP rebooted Symptom: During slot commands test on Brocade 48000 (large fabric), iswitchd ASSERT and CP fail over happen. Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Low Reported in Release: V5.3.0
DEFECT000086899	High	Summary: During continued stress test running switchdisable/switchenable on Back-bone fabric, with SNMP trap and FM running, iswitchd runs into queue full, then asserts and is terminated. Symptom: queue g_isw_q: queue full (miss=1), then iswitchd terminated. Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Low Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000087021	High	Summary: FICON: Whenever a FICON test program sends the first command to a CUP port on a Brocade 5000 switch, the switch sends a busy response. This is not a serious problem because a real world application/operating system would recover from this error. Symptom: CUP Port hangs when coming online Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.3.0
DEFECT000087118	High	Summary: In a large fabric with several devices, and under some rare conditions, while performing Hot Code Load from Fabric OS v5.2.1b to v5.3.0 on Brocade 48000, few frame drops were noticed both on backbone and edge switches. Symptom: A few frame drops may be noticed both on backbone and edge switches. Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Low Reported in Release: V5.3.0
DEFECT000087148	High	Summary: Web Tools Access Gateway: If weblinker restarts, admin user gets spurious " AD permission conflict" error when creating user accounts. Symptom: Problem occurs only if weblinker restarts (possible but unlikely).. Workaround: The workaround is to close the current Web Tools session and start a new one. Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000087178	High	Summary: Under extremely rare conditions, and under stressful testing, slotpoweron and hafailover, an FR4-18i blade faulted with error code 21. Symptom: Observed an FR4-18i turned faulty 21 and the following RAS log message was seen: . [FCIP-5039], 0, FFDC, ERROR, Sending timeout (soft fault) for reason of chip init timed out, OID: 0x43310082, [BL-1009], 52, CRITICAL, Blade slot 3 timed out initializing the chips. Workaround: Slotpoweroff-on Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.3.0
DEFECT000087300	High	Summary: Under rare conditions, POST failed on FC10-6 with v5.3.0_rel_bld47 and blade faulted with error Faulty (51). Symptom: Blade faulty due to POST failure. Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Low Reported in Release: V5.3.0
DEFECT000087303	High	Summary: Under extremely rare conditions, performing "cfgenable" on edge fabric takes longer than normal to complete. Symptom: cfgenable may take a long time to complete. RAS log RTWR-1003 may be seen. Workaround: Portdisable followed by portenable of the VE_Port that's not online. Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Low Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000059663	Medium	Summary: When disabling external ports, the port diagnostic LEDs blinking are not synchronized. Symptom: The physical LEDs for disabled ports flash independently of each other. Customer Impact: No customer impact on switch operation. The amber flashing may appear disorganized to some observers, however, the switch is functioning as expected. Probability: Medium Reported in Release: V5.0.2
DEFECT000063046	Medium	Summary: External port with faulty SFP is disabled then enabled with good SFP and still shows as faulty. Symptom: Port will seem faulty, even though it is actually healthy. Workaround: After enabling the port with the good SFP, remove and re-insert the good SFP. The port will show as healthy. Customer Impact: Usability issue, with no impact to functionality. Probability: Low Reported in Release: V5.0.4
DEFECT000066583	Medium	Summary: After FMSMODE is disabled the CUP port is still online to Host Symptom: Unable to disable CUP feature at the switch Customer Impact; Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.1.0
DEFECT000068760	Medium	Summary: Usability: AD0 allowed user to disable or enable VE_Ports but prevented user from creating or deleting VE tunnels Symptom: Gigabit Ethernet (GE) ports can be configured only from AD0 or AD255. Configuring AD1-AD254 is not allowed. VE_Ports can be created with a GE port. The created VE_Ports can be controlled from any ADs. Customer Impact: Usability issue, with no impact to functionality. Probability: Low Reported in Release: V5.2.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000068786	Medium	Summary: Error message reported when attempting to enable unsupported Fast Write feature on Fabric OS 5.1.0 switch should state "Fast Write mismatch" not "Turbowrite mismatch" Symptom: Messages: "[IPS-1006], 32,, WARNING, sprint_74, Tunnel Configuration Mismatch for slot (0) port(0) tunnel ID(2) reason (TurboWrite; mismatch.)" Customer Impact: Cosmetic issue, with no impact to functionality. Reported in Release: V5.1.0
DEFECT000069724	Medium	Summary: Brocade 4018: Internal ports can be configured as L_Ports under special circumstances for Brocade 4018 (portcfgdefault). Symptom: With the "portcfgdefault" command, the port information window for internal ports on Web Tools will display the Port type and Allow port type as "U_Port" and if the end user executes "portcfglport" it prevents the F_Port server from logging in and could result in unexpected behavior of the internal ports. Workaround: config upload/download may be used to reset the configuration of a switch Customer Impact: Minimal, since there is a workaround. Probability: High Reported in Release: V5.0.5
DEFECT000069966	Medium	Summary: Usability: firmwaredownload downgrades from v5.2 do not offer automatic feature removal to the customer. Symptom: Firmwaredownload does not offer automatic removal of some software features when they block customer downgrade capability. Customer Impact: Usability issue, with no impact to functionality. Probability: High Reported in Release: V5.2.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000075226	Medium	Summary: Usability: Ctrl-C in legacy configdownload code is not blocked during downloads Symptom: Due to considerably longer configdownload times in v5.2, use of the Ctrl-c key to escape from the utility could result in an ill-defined switch state. Workaround: Most configdownloads are fast and will not be interrupted by a user Ctrl-C sequence. The window is also small in which this can create problems. The workaround is to avoid the use of Ctrl-C to interrupt this command. Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Medium Reported in Release: V5.2.0
DEFECT000076372	Medium	Summary: Web Tools does not show the reason for configdownload failure while CLI shows the reason. Symptom: Customer will not know why a particular configdownload operation failed. He/she will have to use configdownload again in CLI to know the reason. Workaround: Use configdownload in CLI Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.2.0
DEFECT000076528	Medium	Summary: cfgtransabort and ad --transabort commands are shown as run when only one of them is executed by the user; note that cfgtransabort is an invalid operation in AD255 and similarly ad --transabort is invalid in AD0-254 Symptom: Aborting Admin Domain transaction generates redundant message about cfg transaction being aborted. Similarly, aborting cfg transaction generates redundant message about ad transaction being aborted. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Medium Reported in Release: V5.2.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000076596	Medium	Summary: No warning message is given when an LSAN zone with a zone name larger than 58 characters is created in AD1 - AD254. Symptom: LSAN zones in AD1- AD254 with names having more than 58 characters are not propagated and no warning is displayed. Workaround: Use LSAN zone names shorter than 58 characters in ADs 1 to 254. Customer Impact: Minimal, since there is a workaround. Probability: Low Reported in Release: V5.2.0
DEFECT000076864	Medium	Summary: Brocade 4020: The "restart module and run standard diagnostics" operation takes longer than the specified 60 second limit. Symptom: No visible symptoms, such as error messages in the management module logs. Customer Impact: Cosmetic issue, with no impact to functionality. Probability: Low Reported in Release: V5.2.1
DEFECT000077592	Medium	Summary: In Web Tools, if the incorrect username is entered at login, the prompt displays an unhelpful error message. Symptom: Message: "invalid encryption data." Behavior of the return value to display the proper error message is inconsistent. Workaround: A common error message can be returned even when the geps_auth_type() function fails or and incorrect username or password results in a login failure. Customer Impact: None if recommended service procedures are followed carefully. Probability: High Reported in Release: V5.2.1
DEFECT000078109	Medium	Summary: configdownload exits with "segmentation fault" when invalid value passed to parameter "Do you want to continue [y/n]:" Symptom: Invalid parameter passed to configdownload can cause “seg” fault Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.1

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000078139	Medium	Summary: McDATA switch and Brocade 24000 in interop mode does not add McDATA ISL back into fabric. Symptom: In an interop environment, with a McDATA switch module (standard mode), a Brocade 24000 switch (interopmode), a "set port <port number> state offline and online" or "set switch state offline and online" on the McDATA port/switch ISLed to the brocade, does not add the McDATA switch back into the fabric. Customer Impact: : Should not occur under normal maintenance operation; represents an unlikely user scenario. Service Request# RQST00000054429 Reported in Release: V5.2.0
DEFECT000078463	Medium	Summary: Brocade 4020 and 3016: restore factory defaults will not restore the default switchname Symptom: When reset factory defaultsBlazer2 switchname is supposed to default to "brocade4Gb". The RASLOG indicates the switchname is "brocade4Gb". However, the switchname at the prompt is still user defined name. Workaround: After restoring factory default, the user may run the following command to restore the default switchname, as a workaround: switchname "brocade4Gb" Customer Impact: Cosmetic issue, with no impact to functionality. Probability: High Reported in Release: V5.2.1
DEFECT000079455	Medium	Summary: Brocade 4020: The "Restore Factory Default" operation leaves ports disabled if the Access Gateway (AG) mode is enabled. Symptom: For a switch that leaves the factory configured as a non-AG mode system, if subsequently AG mode is enabled, the "Restore Factory Defaults" operation does not completely restore the configuration. In particular the ports will be disabled. For a switch that leaves the factory with Access Gateway enabled, the "Restore Factory Defaults" operation will leave all ports disabled and the command "ag --show" will show no mapping. Workaround: If the factory default configuration is with the Access Gateway mode enabled, after performing the Restore Factory Defaults operation, run the "ag --modedisable" command. After the reboot, run "ag --modenable". If the factory default configuration is with the Access Gateway mode not enabled, do the opposite, i.e., "ag --modeenable" followed by "ag --modedisable". Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Medium Reported in Release: V5.2.1

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000079995	Medium	Summary: When adding a new user account, the switch instance number gets appended to the new user account name and sshd fails to find the new user name. Customer Symptom: When using Pageant within PUTTY for authentication, the switches don't ask for the password on login and close the session immediately. The same happens in Linux when a key is loaded via ssh-agent. Workaround: replicate the new user id entry in /etc/passwd file without the switch id 0/1: Newuser0:x:0:600:admin account for newsuer:/fabos/users/admin:/bin/rbash newuser:x:0:600:admin account for newsuer:/fabos/users/admin:/bin/rbash Customer Impact: Minimal, since there is a workaround. Probability: Low Service Request# RQST00000055755 Reported in Release: V4.4.0
DEFECT000080033	Medium	Summary: Disabling F_Ports due to N_Ports not being available keeps changing the port state from "No_Sync" to "In_Sync". Symptom: Status of F_Port keeps changing from No_Sync to In_Sync or In_Sync to No_Sync in output of "switchshow" CLI when N_Port to which F_Port is mapped is Offline. Workaround: Ensure that the N_Port to which the F_Port is mapped is Online. Customer Impact: Cosmetic issue, with no impact to functionality. Probability: Medium Reported in Release: V5.2.1
DEFECT000081210	Medium	Summary: WAN tool ipperf does not refresh the delay during runtime Symptom: Ipperf WAN tool will not refresh the delay Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000082233	Medium	Summary: IPFC: ping to broadcast address FAILS Symptom: ping to broadcast address FAILS Solution: run "ech 0 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts " Workaround: run "ech 0 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts " Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.3.0
DEFECT000083766	Medium	Summary: Open Mode: If zoning is not properly setup such that it causes a zone conflict between Brocade 200E and 4500 switches, switches are segmented partially. Symptom: incomplete segmentation between Brocade 200E and 4500. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario.. Probability: Medium Reported in Release: V5.3.0
DEFECT000083846	Medium	Summary: There could be a misleading RASlog message when FC10-6 blade is inserted into a Brocade 48000 chassis, which should be suppressed. Symptom: RASLog message such as this may be seen: "[FW-1002], 6576,, WARNING, SW_111, Env Temperature 10, is below low boundary(High=60, Low=0). Current value is -31 C" must be suppressed. Temp like -31 C or 64 C at insertion of a blade is clearly a wrong temperature. Workaround: temp sensor values get restored with in a second. Customer Impact: Cosmetic issue, with no impact to functionality. Probability: Medium Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000084037	Medium	Summary: On an FR4-18i or Brocade 7500, if MTU size configured on a GE port between 1261 and 1499 inclusive, firmware downgrade to Fabric OS v5.2.0b patch release is not allowed. This is not correct because Fabric OS v5.2.0b release supports those MTU sizes Symptom: Customer would not be able to downgrade from Fabric OS v 5.3.0 to Fabric OS v 5.2.0b when MTU >1260 <1500 enabled IPIF FCIP is configured on Brocade 7500 or FR4-18i Workaround: Change the MTU to a value lower than 1261 and then downgrade to 5.2.0b. After downgrade change the MTU value to the desired size. Customer Impact: Minimal, since there is a workaround. Probability: Low Reported in Release: V5.3.0
DEFECT000084045	Medium	Summary: In interop mode, cfgsize gives incorrect zone data base size values in the output Symptom: Incorrect zone data base size values are displayed in the output Customer Impact: Usability issue, with no impact to functionality. Probability: Medium Reported in Release: V5.3.0
DEFECT000084472	Medium	Summary: SecurityAdmin role is not allowed to set Switch time Symptom: Request by SecurityAdmin role to set switch time is allowed by the GUI, but the operation triggers exceptions and fails when invoked. Workaround is to call CLI "date" function, which is allowed for this role. Customer Impact: Usability issue, with no impact to functionality. Probability: Medium Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000084646	Medium	Summary: SNMP management applications are not able to use SNMPv3 to view or configure SNMPv1 community strings and SNMPv1 trap recipients. Symptom: swAgtCmtyEntry is not accessible to any of the snmpv3 users existing on FOS Workaround: The workaround is to use SNMPv1 instead of SNMPV3. Customer Impact: Minimal, since there is a workaround. Probability: Low Reported in Release: V5.3.0
DEFECT000084736	Medium	Summary: FTP server recommendation for use on particular 3rd party service processors. Symptom: Unable to use FTP server for config upload/download. Customer Impact: Usability issue, with no impact to functionality. Probability: Medium Service Request# RQST00000059024 Reported in Release: V5.2.1_Ni
DEFECT000084745	Medium	Summary: Setting IP address manually immediately after DHCP set, causes error Symptom: Customer will see "Bad file descriptor". Workaround: When making changes from DHCP to manual wait a minute or so before changing again. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.1_Ni
DEFECT000084761	Medium	Summary: Native Interop: RTWR max retries message logged to console after E_Port disable/enable Symptom: Customer may notice RTWR-1002 messages appear on console output and errdump after fabric perturbation. This does not have any affect on switch operation. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.1_Ni

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000084850	Medium	Summary: When a switch's IDID mode is currently OFF and we disable the switch, the rest of the switches in the fabric get a premature duplicate message Symptom: Switching IDID ON, on one of the switches in the fabric does not give the expected message on the rest of the switches in the fabric Customer Impact: Cosmetic issue, with no impact to functionality. Probability: Low Reported in Release: V5.3.0
DEFECT000085014	Medium	Summary: Config upload button is disabled in zone admin role in Web Tools. Symptom: Customer will not be able to do config upload from Web Tools when logged in as zone admin, although it is allowed from CLI. Customer Impact: Usability issue, with no impact to functionality. Probability: Medium Reported in Release: V5.3.0
DEFECT000085098	Medium	Summary: When SMIA uses a backup FCS switch as a proxy to the fabric with FCS policy configured, zoning transaction through SMIA should be blocked to be consistent with FCS policy enforcement. Symptom: FCS policy not enforced for zoning transactions through SMIA proxy switch in backup FCS list. Workaround: SMIA should use the primary FCS switch as the proxy. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Medium Reported in Release: V5.3.0
DEFECT000085141	Medium	Summary: iSCSI: Under extremely stressful scenario, and under very rare condition, and with a specific type (Vendor's) iSCSI HBA, when Error Recovery Level is set to 1, some I/O failure was observed. Symptom: Some I/O failure observed. Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Low Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000085157	Medium	Summary: Port Media State Wrong: switchShow showing No_Module after changing 75km to 100km with 3rd Party XFP Symptom: sfpshow still shows the XFP data so it is not a No_Module. Workaround: Change the cable to the spec length and try it again. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Medium Reported in Release: V5.3.0
DEFECT000085170	Medium	Summary: When AP blades are present in a Brocade 48000 chassis, operational sequence involving Configremoveall, configdefault followed by reboot does not reset Fabric Watch default parameters. Symptom: FabricWatch switch status policy parameters remain non-default value. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Medium Reported in Release: V5.3.0
DEFECT000085192	Medium	Summary: Web Tools: Not able to retrieve Device Accessibility Matrix for certain Zoning Configurations containing virtual initiators and FC targets. Symptom: Customer would not able to see the device accessibility between the vitual initiators and physical targets as per their choice. Customer Impact: Usability issue, with no impact to functionality. Probability: Low Reported in Release: V5.3.0
DEFECT000085218	Medium	Summary: FICON: Async error reporting events are lost if detected immediately after switch reboot. Symptom: Async error reporting missing events Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000085389	Medium	Summary: Web Tools-Zone Admin window, user is able to select McDATA default Zone and McDATA Safe Zone options. Symptom: From the Zone Admin Window, customer will be able to select McDATA default Zone and McDATA Safe Zone options. This should not be possible from a Brocade 5000. Customer Impact: Usability issue, with no impact to functionality. Probability: Low Reported in Release: V5.2.1_Ni
DEFECT000085412	Medium	Summary: EZSwitch refresh button does not work for "Display Connection" window Symptom: User will not get an updated view of the device connection on doing an explicit refresh operation. This affects EZManager only, and not the EZSwitchSetup wizard. Workaround is to wait 15 seconds for automatic refresh. Workaround: Close EZManager and relaunch it. Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.3.0
DEFECT000085712	Medium	Summary: Web Tools sorts alias names alphabetically and CLI does not sort alias names, which creates inconsistency from the users point of view. Symptom: This may have impact to customer who uses both CLI and Web Tools to perform zone changes and expect the alias names to be kept in the order created rather than sorted Workaround: Consistently use Web Tools for sorted alias names, or consistently use CLI to main user input orders. Customer Impact: Minimal, since there is a workaround Service Request# RQST00000059321 Reported in Release: V5.2.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000085803	Medium	Summary: Web Tools displays E-Port support on internal port, which is not consistent with CLI. Symptom: "Port Administration Services" window still shows E_Port is supported. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.2
DEFECT000085831	Medium	Summary: When trying to create end-to-end monitors between 2 devices that are part of AD2 (switch is not a member of AD2), actual monitors are created on an AD where switch is a member. Symptom: EE monitors are created in the wrong AD. Workaround: Add switch as member of AD2 and then create monitors. Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.3.0
DEFECT000085981	Medium	Summary: Running supportsave in a loop on two Brocade 200E switches, various "sh: /tmp files not found" messages were seen during supportsave execution. Symptom: When supportsave is run continously on a switch, certain types of files are not detected and provide "SupportSave completed sh: /tmp/supportSave_files/CONSOLE0: No such file or directory" messages periodically. The file name varies. Customer Impact: Cosmetic issue, with no impact to functionality. Probability: Medium Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000086015	Medium	Summary: Fabric tree is not displayed properly in Web Tools at times. It moves down and hides itself in the window. Symptom: When the problem occurs, user may not be able to see the switches present in the fabric tree. Workaround: Re-start Web Tools, or refresh AD context by switching to another AD and then returning to the original AD. Customer Impact: Minimal, since there is a workaround. Probability: Low Reported in Release: V5.3.0
DEFECT000086021	Medium	Summary: First Failure Data Capture (FFDC) - -RAS in Brocade 4900 after changing its domain ID to the Principle ID. Symptom: May see FFDC. Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Low Reported in Release: V5.2.2
DEFECT000086046	Medium	Summary: enable AG mode with connecting EX_Port does not log errors in errlog on Brocade 7500 or AG switch Symptom: enable AG mode with connecting EX_Port does not display any error on Brocade 7500 or AG switch Customer Impact: Usability issue, with no impact to functionality. Probability: Low Reported in Release: V5.2.2
DEFECT000086066	Medium	Summary: Proper error message is not displayed when we pass invalid values to -q operand (portcmd --ping) for WAN tool ping. Symptom: This occurs with FCIP. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.2

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000086178	Medium	Summary: With faulted CP and 5 AP blades (unsupported as max supported is 4) in a single chassis, some AP blades may turn faulty. Symptom: Multi-blades faulty at boot up. Workaround: Remove the 5th AP blade, and reboot. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Medium Reported in Release: V5.3.0
DEFECT000086404	Medium	Summary: IOF: Under very rare conditions, Brocade 7500 switch hangs after running several iterations (>20) of fastboot. Symptom: Brocade 7500 switches become completely inaccessible after fastboot and sometimes after firmwaredownload.. Workaround: Power cycle the Brocade 7500. Since the switch has already been fastbooted, there is no traffic disruption. Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Low Reported in Release: V5.3.0
DEFECT000086471	Medium	Summary: Mgmt Apps: When an Initiator has multiple connections made to the same target, the Agent does not show more than one iSCSI connection end point. Symptom: User will not see multiple connections that are part of the same session; only the primary connection will be shown. Customer Impact: Usability issue, with no impact to functionality. Probability: High Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000086531	Medium	Summary: OPEN – FFDC (First Failure Data Capture)- triggered when a switch with insistentDID enabled and a duplicate DID joins a fabric with McDATA and Brocade switches in it. Symptom: When a Brocade switch with insistent DID is enabled and a duplicate DID joins a fabric with both McDATAand Brocade devices (I10K and Brocade 4500), FFDC files are generated. Customer Impact: Usability issue, with no impact to functionality. Probability: Medium Reported in Release: V5.3.0
DEFECT000086664	Medium	Summary: Web Tools Performance Monitor: port throughput graph was not matched between mirror port and host port. Symptom: Running traffic.CLI portperfshow looked OK. After overnight test, port throughput matched for port mirror and host port., but performance monitor graph (did not match. Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Low Reported in Release: V5.2.2
DEFECT000086682	Medium	Summary: WebMgmt_iSCSI_Usability: Cannot update DiscoveryDomain name. Symptom: User will not be able to update the DD name. Workaround is to do the update from CLI. Workaround: When a DD is added; do not update its name. Customer Impact: Usability issue, with no impact to functionality. Probability: Low Reported in Release: V5.3.0
DEFECT000086711	Medium	Summary: SMI: In Brocade_NetworkPipeStatistics, TxByte is having RxByte value and RxByte is having TxByte value when compared with telnet values. Symptom: TxByte and RxByte values in SMI client display are interchanged. Customer Impact: Usability issue, with no impact to functionality. Probability: Medium Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000086749	Medium	Summary: Open Mode: ISL does not come up between McDATA 4500 and Brocade 24000 after the Port/Blade/Switch is disabled/enabled. Symptom: The ISLlink does not come up. The port comes up as gx port on the McDATA switch and Loopback on the Brocade switch. Workaround: Doing a port block and unblock on McDATA switch brings the E_Port link back up. Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.3.0
DEFECT000086799	Medium	Summary: During bladedisable/enable on Brocade 48000 (large fabric), glibc errors were shown on the console and raslogd dumped core. Symptom: Message: "*** glibc detected *** free(): invalid next size (normal): 0x10013078 ***" . Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.3.0
DEFECT000086823	Medium	Summary: iSCSI_Web Tools: Cannot create or abort transaction in Web Tools under certain extreme conditions. Symptom: When there is a system hang or a power surge; and if there is an iSCSI transaction created; and if the Web Tools session gets killed automatically. On the subsequent launch, no iSCSI transaction can be committed if any is created from Web Tools because the Apply and Abort button are deactivated. Workaround: The workaround for a transaction that cannot be aborted from Web Tools is to identify and abort the transaction from the CLI: Usage: iscsicfg --abort transaction -x <transaction id> Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000086929	Medium	Summary: Web Tools: Trunking table is showing trunking data for a slot even though that slot does not have any trunks configured. Symptom: No user impact in Web Tools or FM. This is a back end issue only. Customer Impact: Cosmetic issue, with no impact to functionality. Probability: Medium Reported in Release: V5.3.0
DEFECT000086931	Medium	Summary: A warning message is needed when user attempts to map an F_Port to a disabled port. Symptom: Deleting and re-setting the mapping of a failed-over port to a disabled port does not cause the failover to re-occur as expected, but no warning message is displayed. Customer Impact: Usability issue, with no impact to functionality. Probability: Low Service Request# RQST00000061338 Reported in Release: V5.2.1
DEFECT000087007	Medium	Summary: iSCSI: Discovery Domain does not show all the DD's that are members of DDSET when configured from usability wizard. Symptom: The correct details are not shown. Details are shown correctly in CLI. Solution: Corrected while adding member to DDSET. Probability: Medium Reported in Release: V5.3.0
DEFECT000087020	Medium	Summary: Incorrect port configuration information after blade swaps Symptoms: if you set ports 0-5 on the FC6-10 blade to have an FSPF cost of 100 and then swap the FC6-10 for a 16 port 4 G blade, ports 0-5 will still have a cost of 100 if they come up as E_Ports. Customer Impact: Usability issue, with no impact to functionality. Probability: High Service Request# RQST00000058950 Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000087024	Medium	Summary: iSCSI_Web Tools: In the "Configure DD" screen, when adding a new DD and adding VT and VI, it also adds VT and VI from the existing DD. Symptom: The copying of VT and VI from the existing DD to the new DD will create confusion, but these "ghost" entries are transient. When user advances to the next wizard step they will be gone. Customer Impact: Cosmetic issue, with no impact to functionality. Probability: Medium Reported in Release: V5.3.0
DEFECT000087061	Medium	Summary: Web Tools: In "Zoneadmin" role, when ADs are configured, "set default mode" option (under zoning actions tab) should be disabled. Symptom: Some scenarios have been discovered that result in the Default Zoning menu in Web Tools Zone Admin being enabled when user-defined ADs exist - either for low-permission users or when user-defined ADs have been defined but not applied. If a user invokes this menu item in one of these scenarios to set default zoning to "All Access" mode (an operation which is not allowed), the resulting transaction will fail but remain open, and subsequent attempts to abort this transaction from Web Tools to enable further zoning operations will also fail. Workaround : Display the transaction id from the CLI with "cfgtransshow", and then abort the transaction from the CLI with "cfgtransabort <txn id>". Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Medium Reported in Release: V5.3.0
DEFECT000087075	Medium	Summary: After fastbooting all the switches in a large fabric with 54 domains, fully populated 384 port core switch and 1mb database, cfgshow reported fabric busy for almost 30 minutes and a few E_Ports were segmented because of a zone conflict. Workaround: portdisable then portenable will bring the segmented E_Ports back online. Wait for 30 minutes and cfgshow –show will report the cfgshow output. Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Medium Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000087084	Medium	Summary: MgmtApps: If an active IPv4 policy has "80 accepted; 80 denied; and 443 accepted," both http and https are disabled on the switch. Symptom: User interface allows invalid combinations that may result in loss of connectivity to the switch from Web Tools. For example, if user happens to configure an active policy with http allowed for "any," as well as http denied for "any" and https allowed for "any", both http and https would be disabled on the switch, and user will not be able to invoke Web Tools. Workaround: Modify the active policy or switch to another known good policy from CLI. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.3.0
DEFECT000087129	Medium	Summary: Web Tools: On Brocade 48000 director, Web Tools displays DHCP is on, and hence user can not change IP address from Web Tools since Web Tools blocks the static IP address from changing when DHCP is enabled. Symptom: No customer impact unless DHCP is enabled on a bladed switch, and there is no user-accessible scenario that supports this. But even if the switch does get into this state (which should not happen in a production environment), user should still be able to set static IP from Web Tools. Workaround: Set the ip address from the CLI. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.3.0
DEFECT000087161	Medium	Summary: Firmware upgrade on Brocade 7500 switch from Fabric OS v5.1.1b to v5.3.0_rel_bld46 sees segmentation fault message, which is actually meaningless and harmless. Symptom: Message occurs at the end of the firmwaredownload. Customer Impact: Cosmetic issue, with no impact to functionality. Probability: Medium Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000087209	Medium	Summary: During the firmware download process, creating an IP interface while Blade Processor (BP) code is still loading may rarely result in a kernel panic. Symptom: Unexpected switch behavior. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.3.0
DEFECT000087218	Medium	Summary: FCR keeps showing proxy devices from the edge fabric even though devices are no longer part of those Ads. Symptom: Customer may see incorrect proxy devices. Workaround: Make the similar changes in the remote fabric. (Whenever AD is supported in the remote fabric), otherwise move the LSAN zones manually to other ADs (zone --copy can be used for that). Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.3.0
DEFECT000087238	Medium	Summary: If a device tries to login to an NPIV port using a port worldwide name (PWWN) that is already used by another device that has already logged in, the switch simply drops the new login (FDISC) request instead of rejecting it. Symptom: Switch does not respond to FDISC with duplicate PWWN from different switch port. Solution: Switch should reject the FDISC with duplicate PWWN from different port. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Medium Reported in Release: V5.3.0

Defects Deferred in Fabric OS v5.3.0		
Defect ID	**Severity**	**Description**
DEFECT000087292	Medium	Summary: MIBS: Walk and Table View shows different outputs for the same table Symptom: swTrunkTable returns wrong data when queried with "getbulk". Workaround: Only use the Walk view. Use getmany to get the data from swTrunkTable. Customer Impact: Minimal, since there is a workaround. Probability: Low Reported in Release: V5.3.0

Closed Defects in Fabric OS v5.3.0

This section lists defects that have been closed since the last Fabric OS GA release v5.2.2. The closed defect reports were run on June 7, 2007,

Defects Closed Without Code Change

This table lists defects that have been closed since the last Fabric OS GA release v5.2.2.

The defects in the table include the defect Summary (there are no Workarounds for the defects listed in this table). Also included is an Explanation of Closure field as described below.

Already Fixed

Brocade already had a fix for these defects: see the Already Fixed In Release field to see the release in which each defect was fixed.

Will Not Fix

Brocade has determined one of the following:

a) The defect does not require a fix (e.g., a corner case occurring only in extreme test case conditions, extremely unlikely to occur under normal operating conditions).

It may not be possible to provide a solution. Other Resolved without Code Change

The remainder of defects resolved without code change fall into this category, including:

a) Defects determined to be invalid.
b) Issues for which there is not enough information to make an assessment.

Defects resolved with code change are not included in this report, but are disclosed in the respective release notes of the releases in which they are fixed.

Defects Closed Without Code Change								
Defect ID	**Service Request**	**Summary**	**Found in Release**	**Severity**	**Explanation of Closure**	**Reason Code**	**Already Fixed In release**	**Workaround**
DEFECT000070936		Firmware fallback from Fabric OS v5.1.0c to internal release, while running FICON traffic, resulted in channels detecting out-of-order frames.	V5.1.0	High	Will Not Fix	Will Not Fix		
DEFECT000075341		Incorrect WARNING messages displayed when SFPs are removed from ports on Brocade 48000 (FC4-48 port blade), moved to other ports and hafailover is issued.	V5.2.0	Medium	Will Not Fix	Will Not Fix		
DEFECT000077972		Cannot enable Access Gateway mode without a Zoning License.	V5.2.1	Medium	Will Not Fix	Will Not Fix		Make sure zoning license is installed before doing ag --modeenable
DEFECT000057804		EZM: Display device does not show legends when Restore Fixed Zone is done.	V5.0.1	Medium	Other Resolved without Code Change	Duplicate		Close and reopen the EZManager window after restoring fixed zoning.
DEFECT000066007		Common Access Layer daemon (cald) out of memory panic.	V5.0.3	High	Other Resolved without Code Change	Not Reproducible		
DEFECT000066553		After 12 days of uptime, Brocade 24000 edge switch connected to Brocade 48000 backbone fabric received Out of Memory error and rebooted.	V5.1.0	Medium	Other Resolved without Code Change	Not Reproducible		

Defects Closed Without Code Change								
Defect ID	**Service Request**	**Summary**	**Found in Release**	**Severity**	**Explanation of Closure**	**Reason Code**	**Already Fixed In release**	**Workaround**
DEFECT000069136		During FCR 3rd party interop testing, frame drop occurs while enabling EX_Port s on secondary FCR in a dual redundant backbone fabric configuration.	V5.1.0	Medium	Other Resolved without Code Change	Not a Defect		
DEFECT000073736		Usability: auditcfg: Meaningful security-related messages are sent to syslog by design with no fallback to RASLog or other persistent storage.	V5.2.0	Medium	Other Resolved without Code Change	Converted to RFE		
DEFECT000074418		Brocade 7500 GE port was stuck in "No_Sync" state	V5.2.0	Medium	Other Resolved without Code Change	Duplicate		1. Issue portdisable followed by portenable on the GE that is stuck in No_Sync state. 2. Pull out the cable and plug it back in (without pausing during the insertion of the cable).
DEFECT000074892		Usability: High availability of transferred supportsave files is not ensured with current implementation	V5.2.0	Medium	Other Resolved without Code Change	Converted to RFE		Retry supportsave
DEFECT000074981		Some storage device port comes up as L_Port instead of F_Port after reboot and the hosts no longer see that storage device.	V5.2.0	Medium	Other Resolved without Code Change	Not a Defect		If problem happens, lock gport by issuing portcfggport

Defects Closed Without Code Change								
Defect ID	**Service Request**	**Summary**	**Found in Release**	**Severity**	**Explanation of Closure**	**Reason Code**	**Already Fixed In release**	**Workaround**
DEFECT000076244		Unexpected termination of zoned, switch crashes after upgrade	V5.2.0	High	Other Resolved without Code Change	Duplicate		Perform upgrade while fabric is stable.
DEFECT000076587		After changing zone configuration in the edge fabric, one of the FCRs in the backbone fails to display an xlate domain in fabricshow	V5.2.0	Medium	Other Resolved without Code Change	Duplicate		If EX port is disabled and enabled the xlate domain will appear correctly in both FCRs. This should be minimal impact to the user considering the entire zoning configuration was changed and a certain level of interruption was already expected.
DEFECT000076608		FVT/SWAT: In an FCR-enabled switch, the ports connecting to hosts and targets become "Disabled (Switch not ready for F or L ports)".	V5.3.0	Medium	Other Resolved without Code Change	Not Reproducible		"switchdisable" and "switchenable" return the ports to normal.
DEFECT000076677		ISCSI stress testing: targets lost, PDUs for 1 session sent to another session	V5.2.0	High	Other Resolved without Code Change	Duplicate		
DEFECT000076684		After 20 hours of continuous slotpoweroff/on stress testing, out of memory condition observed.	V5.3.0	Medium	Other Resolved without Code Change	Not Reproducible		

Defects Closed Without Code Change								
Defect ID	**Service Request**	**Summary**	**Found in Release**	**Severity**	**Explanation of Closure**	**Reason Code**	**Already Fixed In release**	**Workaround**
DEFECT000077823		Web Tools should display a list of devices connecting to the NPIV port.	V5.2.1	Medium	Other Resolved without Code Change	Duplicate		Customer can use CLI to see the required information.
DEFECT000078355		Virtual port login (FDISC) from NPIV-capable HBA on an F_Port is not handled correctly.	V5.2.1	Medium	Other Resolved without Code Change	Duplicate		Disable NPIV on all F_Ports of Access Gateway switch using "portcfgnpivport <port> 0"
DEFECT000079971		IOF: a few extra xlate domains with a missing ipaddress appear in the fabricshow results for an edge fabric after a disable/enable of all switches in one backbone.	V5.2.1	Medium	Other Resolved without Code Change	Duplicate		
DEFECT000080024		If the failover policy is disabled, failover should not take place during either physical switch reset or reboot.	V5.2.1	Medium	Other Resolved without Code Change	Duplicate		Always make sure that the N_Ports to which F_Ports on Access Gateway are mapped are Online, i.e., by ensuring they have a POD license, NPIV configured on the fabric side, etc.
DEFECT000081656	RQST00000056686	Intermittent First Failure Data Capture (FFDC) events being logged on a Brocade 48000.	V5.1.0	High	Other Resolved without Code Change	Duplicate		

Defects Closed Without Code Change								
Defect ID	**Service Request**	**Summary**	**Found in Release**	**Severity**	**Explanation of Closure**	**Reason Code**	**Already Fixed In release**	**Workaround**
DEFECT000082207		Web Tools: "LSAN Fabrics" should show all the FCRs in the backbone fabric in order to be consistent with the "fcrfabricshow" CLI.	V5.3.0	Medium	Other Resolved without Code Change	Converted to RFE		

Defects Closed With Code Change

The tables below list defects that have been fixed with code changes in Fabric OS v5.3.0.

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000080217	Critical	Summary: Brocade 48000 running FICON with fsmode enabled panics after an upgrade from Fabric OS v5.0.x to v5.1.x or v5.2.0. Symptom: Problem occurred on a Brocade 48000 with FICON fsmode enabled, dynamic load sharing (DLS) on, and with a port based route policy. After the upgrade and a disable/enable on a port to trigger a reroute, the switch panics with the following message displayed on the console: "ASSERT - Failed expression: !old_path, file = rte_path.c, line = 1366;" Solution: Fabric OS v5.1 introduced a new flag during route calculation. After an upgrade from Fabric OS v5.0 to v5.1, a new active CP running Fabric OS v5.1 uses the old way of calculating the route, rather than using the new flag. This causes a route miscalculation and the switch panics. Workaround: Avoid the combination of "Port based routing (external = 1, internal = 2) + DLS ON" in a FICON fsmode enabled setup. DLS off is recommended for a FICON environment. Service Request# RQST00000056030 Reported in Release: V5.1.0
DEFECT000065145	High	Summary: Kernel Oops error when the counter is overrun during stress-to-fail test. Symptom: Switch failed with kernel trace. Solution : Fixed by upgrading to Linux 2.6 Customer Impact: Should not occur under normal operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000069537	High	Summary: During stress testing of an unsupported configuration, chassis containing more than the supported number of FC4-18i and FC4-16IP blades, on one occasion the switch panicked and rebooted. Symptom: Switch reboots. Solution: Emd was leaking virtual memory in the stack area as a result of not doing either a pthread_join or pthread_detach on the short lived thread used to unburden the HSM thread during the approx 1 min while AP blades were moving from UP to ON/enabled. This fix uses the wt_exec thread pool vs creation and destroying a thread each time an AP blade is brought up. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.0
DEFECT000070043	High	Summary: When performing port mirroring, a Brocade 48000 printed an exception error and the kernel rebooted. Symptom: Error message: "Exception in kernel mode: sig=4, WARNING, SilkWoOops: Exception in kernel mode, sig: 4". This is a rare occurrence with a heavily loaded system. Solution: Fixed by upgrading to Linux 2.6 Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000071195	High	Summary: configdownload with new timezone is not being validated nor applied completely; date uses old timezone, tstimezone shows new time zone Symptom: tstimezone command does not show the correct time and date if configdownload interface is used to update timezone. Solution :validating the time zone parameters in the config download's config file, if invalid then abort the config download Workaround: After doing configdownload, run 'tstimezone' CLI to update Time Zone. The CLI validates the timezone as well as applies it. A reboot is required to make timezone completely effective in either case (config download or using CLI). Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.2.0
DEFECT000074395	High	Summary: After executing trunk disable/enable on all edge switches in a large scalability fabric, one core Brocade 24000 E_Port gets stuck in "Loopback" mode. Symptom: Cfgtrunkdisable/Cfgtrunkenable will cause the ports to be permanently in IN_SYNC. Solution : Resolves the mis-merge (from source control system) caused by the other defect fix Workaround: Issue a portdisable/portenable on the problem port to recover it back to E_Port online state. Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Medium Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000074978	High	Summary: AD filter: port mirror allowed the addition of a mirror port in AD3 in which the SID and DID were not port members. Symptom: The AD Enforcement on SID/DID is not performed. The traffic can be monitored between any SID/DID even though the ports are not under your AD Solution: Added SID and DID check for the AD Enforcement. The SID and DID both need to be part of AD apart from the mirror port to form a port mirror connection Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.0
DEFECT000075139	High	Summary: Issue hafailover command and the new active CP got Oops and reboot during initialization. Symptom: New active CP got Oops and reboots with error "kernel BUG at cachemap.c:91! Oops: Exception in kernel mode, sig: 4; >>NIP; c0010bb0 <consistent_alloc+0xa0/0x1c8 [kernel]> " Solution : Fixed by upgrading to Linux 2.6 Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.0
DEFECT000075170	High	Summary: GE0 port on an FR4-18i blade was stuck in No_Sync state, preventing a VE tunnel from coming up. Symptom: After reboot of a CP, the VE tunnel does not come up. Solution: Fixed by changing vendor's HW. Not a SW problem Workaround: Refrain from using copper SFPs. Remove and reinsert the cable on the GE ports Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000075874	High	Summary: In interop mode, no registered state change notification (RSCN) sent to hosts after zoning changes using cfgEnable. Symptom: In interop mode, following cfgEnable, switch does not generate RSCN to host(s). As a result, the host(s) do not PLOGI, nor do they discover target(s). Solution: Updates the nameserver code in interop mode to send out the RSCN after the zone change. Workaround: Perform portdisable/portenable on host port after cfgEnable (only if in interop mode). Customer Impact: Minimal, since there is a workaround. Probability: High Service Request# RQST00000051734 Reported in Release: V5.1.0
DEFECT000076053	High	Summary: When there is more than the supported number of EX_Ports attached to the same edge fabric, the switch might panic. Symptom: Continuous rebooting (due to panics) on FCR switches. Solution: Fixed code to gracefully handle an excessive number of EX_Port s. Workaround: Use only the supported number of EX_Port s. Customer Impact: Minimal, since there is a workaround. Probability: High Reported in Release: V5.1.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076284	High	Summary: With more than the supported number of AP blades (five) enabled, powering on the 4th and 5th AP blades at the same time immediately results in a failover. Symptom: A cold boot of the system with more than the allowable number of AP blades may result in all AP blades enabled. Solution: Changes to EM recovery and HSM code. Workaround: Power off one of the enabled AP blades (power on and subsequent failovers should work). Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Medium Reported in Release: V5.2.0
DEFECT000076350	High	Summary: During Scalability testing, after firmwardownload to Fabric OS v5.2.0 build, FR4-18i blade faulted. Symptom: Due to a rare occurrence an FR4-18i blade might become faulty after firmware download and slotpoweron followed by slotpoweroff. Solution: Increase the timeout values and add additional messaging to the connection time Customer Impact: This problem has been observed only once and several attempts to reproduce it failed. Probability: Low Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076525	High	Summary: Tape Pipelining needs to properly handle target recovery in a congested IO condition Symptom: Tape backup job failures were occasionally observed in congested IO conditions Solution: Since REC from target is terminated at ingress fabric (near the target) and Tape Pipelining does not have the target proxy ID. Tape Pipelining will send REC ACC payload with the final translation IDs. Therefore, the FCR code will fail the conversion from the physical to proxy and proxy to physical for the orig_id and the resp_id and will clear those fields in the payload. The fix is not to clear those fields if the conversion fails. Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Medium Reported in Release: V5.2.0
DEFECT000076541	High	Summary: After changing FID and enabling FCR switch in backbone, all connected ports remain disabled due to a timing window of the LE_Port offline and switch offline, leading to a computed stale link-state. Symptom: After enabling switch, all connected/active ports are disabled. Solution : The defect was caused by a timing window related to LE_Port offline and switch offline. This led to a stale link-state being computed. This affects the consequent update FSPF sent after switch online again. Fix this by skipping the xlate domainoperation if switch is not online yet. Workaround: Perform a switchdisable/switchenable. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076598	High	Summary: Slotpoweron on an FC4-16IP port blade and hafailover after its FC initialization completes causes all its iSCSI ports to be stuck at "No_Sync" while the FC ports come online. Symptom: If the active CP fails over after an FC4-16IP port blade has been slotpowered on, all the iSCSI ports of the FC4-16IP can get stuck at "No_Sync", while the FC ports come online. Solution: Updated the admin state maintenance for FC4-16IP GE ports. Workaround: Issue portdisable and portenable for all affected iSCSI ports. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.0
DEFECT000076640	High	Summary: After an all switches disable on a Brocade 48000 with FC4-48 port blades, the standby CP asserted and rebooted Symptom: Error message: "Failed expression: snode != NULL". Solution: Standby CP automatically rebooted. Workaround: No workaround is needed. After the reboot the standby CP comes up online and HA is synchronized Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Low Reported in Release: V5.2.0
DEFECT000076657	High	Summary: HAfailover during FCIP IO (through an IPSec enabled tunnel) sometimes causes VE_Port to go down/up. Symptom: With IPSec tunnel configured, the VE might go down and then come back up during HAfailover. Solution: The fix increases the TCP timeout for IPSec tunnels Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076686	High	Summary: ISCSI: isnsccfg --set command should not accept an FR4-18i port. Symptom: User will be able to configure the isns client to communicate with an isns server through a port on the FR4-18i blade. This will not work. Solution: Check if GE port specified is a Brocade FR4-18i or FC4-16IP port. Do not allow port manipulation for Brocade FR4-18i ports. Currently we allow any operation if the port is a GE port irrespective of iscsi/fcip port. Workaround: The user should either a) Configure the isns client to communicate with the isns server with a management port, or b) Run slotshow first, confirm the slot number to be that of a FC4-16IP and then use this slot/port combination. Customer Impact: Minimal, since there is a workaround. Probability: High Reported in Release: V5.2.0
DEFECT000076721	High	Summary: FICON traps include an incorrect value. Symptom: FICON traps are being sent with the wrong "Enterprise" value, which results in the trap being processed as a swFault. Solution: Fix SNMP code to send proper trap value. Service Request# RQST00000052448 Reported in Release: V4.4.2
DEFECT000077358	High	Summary: In a Web Tools switch report, the port detail does not display information for the selected port. Symptom: In the "customized" port detail report, the user will not be able to filter the report by port number or port range. Even if the user gives a particular port range, the report will be generated for all the ports. Solution: Filtering of port is missing while generating the port report. Added it back. Customer Impact: Usability issue, with no impact to functionality. Probability: High Service Request# RQST00000053109 Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000077690	High	Summary: On 2 Gbit/sec platforms, a switch panic condition can occur if an unstable or faulty port generates an excessive number of interrupts. Symptom: The switch executes a panic reboot because the link generates more interrupts than the switch could process. This condition was simulated in the lab by switching an E_Ports transmitter off and on at an interval of 35 msec. Solution: The solution is to update the port fault counter when the link stays in an AC (active) state and there is a loss of signal to allow a port fault to be triggered during the resource allocation time period. Probability: Low Service Request# RQST00000053684 Reported in Release: V5.0.5
DEFECT000078391	High	Summary: I/O fails when rebooting active CP Symptom: Rebooting the active CP will cause traffic disruption. The warning text that appears when this command is run from Admin does not appear when this command is run from Root. Solution: Warning text, that rebooting the active CP will disrupt traffic, is now displayed when this command is run from Root. Service Request# RQST00000054754 Reported in Release: V5.2.0
DEFECT000078733	High	Summary: Brocade 7500 router not passing N_Port login (PLOGI) frames. Symptom: The problem occurred in an edge-to-backbone fabric situation in which the host is in the edge fabric and the target is in the backbone fabric. The PLOGI is neither accepted nor aborted. A second attempt twenty seconds later is responded to immediately. This only happens when there are devices in the fabric for which the link is taken online/offline quickly within a short period of time. Solution: Ensures the correct routine for the edge-to-backbone situation is called. Probability: Medium Service Request# RQST00000054793 Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000080062	High	Summary: Brocade 4900 with Fabric OS v5.1.0d: several ISLs failed and became G ports. Symptom: This issue was observed only once, and was never seen again at the customer site. It has not been observed at any other sites, and was not reproducible within a lab environment. Issue observed was a HW / SW interlock that became stuck, requiring a port disable/enable to clear the condition. Solution: Customer Visible RASLog CDR-1004 will be generated, informing the user to reset their port, should this issue ever happen again. Probability: Low Service Request# RQST00000055962 Reported in Release: V5.1.0
DEFECT000080107	High	Summary: Using the API to access default zoning information may cause the switch to panic. Symptom: This happens if an application is using the API to retrieve ZoneCapabilityobj. The switch reboots with the error message: "[KSWD-1003], 2371, FFDC, WARNING, ED_48000B, kSWD: Detected unexpected termination of: "[22]cald:0'RfP=727,RgP=727,DfP=0,died=1,rt=278." Solution: Fixes code to avoid using an invalid pointer. Probability: Medium Service Request# RQST00000055906 Reported in Release: V5.2.0
DEFECT000080787	High	Summary: API library crash as the zone library does a memcpy that does not include the terminating zero to the buffer. Symptom: 3rd party application crashes during an activation of a large zoneset with over 1200 zones. Solution: The solution is to have the zone library append a terminating zero to all active zone database data buffers returned by the API during zone buffer copy. Probability: Medium Service Request# RQST00000056062 Reported in Release: V5.0.1

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000081074	High	Summary: NPIV FDISC failure on SW7500 Brocade switch Symptom: When VC-FC port tried to log into the Brocade switch, it issued a FLOGI to log into the fabric but one of the FDISC failed. Solution: 1. Both the stage interval and login rate are made configurable parameters. They can be modified either by config download operation or by running the configure command. 2. All virtual login requests (FDISC) on NPIV ports will always be accepted without any busy reject. 3. A NPIV device connected to an F_Port will be treated like a regular F_Port. There will be no special consideration to stage a NPIV capable F_Port. Service Request# RQST00000056508 Reported in Release: V5.2.0
DEFECT000081198	High	Summary: Customer set fabric.ops.mode.pidFormat to 0, caused continuous reboots after upgrading to FOS 5.2.0 Symptom: Switches being upgraded to 5.2.0a (4.4.0d -> 5.1.0a ->5.2.0a) went into continuous reboots because the fabric.ops.mode.pidFormat was previously set to zero in the config. This is not a valid setting, and may have been changed to zero during a previous confg download from a 3.X config onto the 4.X switch. Valid values for fabric.ops.mode.pidFormat are 1 and 2. FOS versions prior to 5.2.0 do not reboot if this value is incorrectly set. Solution: When the system boots up, it goes to gets the PID format value from the configDB. The logic is that if it is not of value 2, it will put the value 1 down to the kernel no matter what value is it. But when NS tries to get the PID value from the configDB, it will return a value 0. The fix will make NS also take the value of the PID format from Kernel to avoid the error. Workaround: Use the configure command to change the pidFormat value back to 2 prior to upgrading to FOS 5.2.0. If a value of 1 is required, then set the pidFormat value to 2, save the config, then re-run to change the pidFormat value to 1. Service Request# RQST00000056490 Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000081883	High	Summary: Due to Performance Server Daemon (PSD) panic assertions, the standby CP on all directors can get stuck in a reboot loop. Symptom: Due to a race condition, a partial HA update arrives before a full update arrives from the active CP. As a result, the standby CP goes into a continuous restart cycle while it attempts to apply the partial HA updates. This is an extremely rare event: hitting a timing window while conducting an HA failover event at the same time as an internal end-to-end monitor wraps its counter. Solution: The solution is to not apply the partial HA update until a full update is received from the active CP. Probability: Low Service Request# RQST00000056917 Reported in Release: V5.0.4
DEFECT000082321	High	Summary: Upgrade to Fabric OS v5.2.0a switch panics one day later with "kSWD: Detected unexpected termination of: "[3]msd:" Symptom: An application in use at customer site, issued a MS request with a WWN that did not exist within the fabric. Upon processing of this WWN, the MS Daemon panicked. Solution: Properly handle WWNs that cannot translate to a PID within the fabric. Service Request# RQST00000057135 Reported in Release: V5.2.0
DEFECT000082754	High	Summary: Request Brocade 24000 not to forward broadcast PLOGI frame. Symptom: A 3rd party system is sending PLOGI frames with its DID as a broadcast format: 0x22ffffff. The Brocade 24000 forwards the frame as a broadcast frame, which causes other devices in the fabric to misbehave. Solution: Check for invalid ELS broadcast frames with cmd code PLOGI, PDISC and ADISC and do not forward these frames. Probability: Low Service Request# RQST00000057230 Reported in Release: V5.0.3

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000083116	High	Summary: During a small window, if a device sends its PLOGI very fast and before the name server information has been fully propagated, the PLOGI might be dropped by a switch using domain/port zoning. Symptom: The host does not see the device. This impacts all platforms running Fabric OS v5.2.0 and above with (domain, port) zoning. It does not impact WWN zoning or a host that retries PLOGI. Solution: Ensures the code properly responds to the FCGS command to retrieve the index for the fast PLOGI device used by domain/port zoning. Probability: Low Service Request# RQST00000057678 Reported in Release: V5.2.1
DEFECT000083764	High	Summary: CLI systemverification incorrectly reports a false positive failure on the FC4-16IP blade. Symptom: This is a command that should only be run under the guidance of service personal, and would not be used by a customer in a normal operating environment. If this diagnostic is run as part of a maintenance action, the FC4-18i blade could be incorrectly identified as being faulty. The false positive failure only exists while running on FC4-16IP blades -- all other blades are not affected by this defect. Example of the false positive error reported by the systemverification test: 2007/03/06-21:35:41, [CDR-5668], 0,, ERROR, ED_48000B, S2,P25(27): Port Fault: Hard 0(2) fault1=254 fault2=5. Solution: The CDR-5668 message is benign on the FC4-16IP blade, and is changed from an ERROR to a Warning severity in future releases to prevent the blade from being faulted. Workaround: The CDR-5668 error is benign and can be ignored. Probability: Low Service Request# RQST00000058174 Reported in Release: V5.2.1

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000083798	High	Summary: "(S)tats" menu option does not work while executing minicycle command. Symptom: "sh: diagshow: command not found" message is displayed on console when selecting (S) for "Stats" from the menu shown while running the minicycle command. Solution: Added "diagshow" command in /fabos/cliexec slinked to the cmdhdl command. Service Request# RQST00000058127 Reported in Release: V5.2.1
DEFECT000084134	High	Summary: Firmware upgrade from Fabric OS v5.2.1 to v5.2.1_ni is not seamless Symptom: Customer cannot upgrade from Fabric OS v5.2.1 to v5.2.1_ni seamlessly. All Web Tools and CLI support to perform functions on the switch is lost until a file is created and firmware commit is issued. Solution: Factory_ag.conf has been moved to new location. Copy all the files in /etc/fabos/ag/ directory care of firmwarerestore.Cold recovery is used when changing firmware from a NI to non-NI version. Workaround: Manually create the missisng entry and do firmwarecommit as following: touch /etc/fabos/ag/fos_config.backup; firmwarecommit Probability: High Reported in Release: V5.2.1_Ni
DEFECT000084702	High	Summary: msd panic due to assert during dynamic RLIR call back Symptom: Switch panic in FICON environment. Solution: During domain offline SCN clean up callback queues properly. Probability: Low Service Request# RQST00000058989 Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000084883	High	Summary: When upgrading firmware to Fabric OS v5.2.1 or v5.2.1a, the internal routing table information will be overwritten. Symptom: On a Brocade 7500 or a Brocade 48000 with an FR4-18i blade in it, established EX_Port routes can be lost as the routing table information is overwritten during the upgrade, causing lost paths to be observed. On the following platforms the overwritten routing data will lead to imbalanced routes, potentially resulting in a performance problem: Brocade 200E, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 7500, 48000. Solution: Properly synchronizes the route HA data structure during firmware upgrade and firmware downgrade. However, with this solution, on an Access Gateway configured switch (Brocade 4012, 4016, 4020, and 4024) already operating with Fabric OS v5.2.1 or v5.2.1a, a disruption occurs when upgrading to Fabric OS v5.2.1b or later code. Switches running pre-v5.2.1 version, or Fabric OS v5.2.1/v5.2.1a version that have not been configured as an Access Gateway switch will upgrade to Fabric OS v5.2.1b and later non-disruptively. Probability: High Service Request# RQST00000059132 Reported in Release: V5.2.1
DEFECT000085212	High	Summary: Process login drop due to devices in different edge fabrics with same node WWN. This applies to Brocade 7500 and Brocade 48000 with FCR-18i blade. Symptom: Customer symptom could be that the host can not see the device, with the name server daemon queue full, etc. When there are two devices with the same node WWN connected to 2 edge fabrics, the FCR may not forward the NS request to the proper domain, which results in the Name Server request timing ut and retrying every 2 seconds. Solution: Fix the EX_Port code to forward the name server request to the correct edge fabric to avoid the RSCN delay. Probability: Medium Service Request# RQST00000059349 Reported in Release: V5.2.1

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000085328	High	Summary: Traffic cannot be routed into backbone fabric from an EX_Port on Brocade 7500 with domain ID 7 or 12, and from an EX_Port on Brocade 48000 with FR4-18i blade with various fabric domain IDs. Symptom: Customer may experience connectivity problem between two edge fabrics such as the host not seeing a device, or traffic loss, etc. if there are specified domains on the EX_Port switches in the backbone fabric. Solution: When the EX port comes up, the Brocade 7500 incorrectly filters route-to- backbone domain IDs 7 and 12. The Brocade 48000 with FR4-18i incorrectly filters out the route to 16 backbone domain IDs depending on the slot number. This includes domains 7, 12, 23, 28, 39, 44, 55, 60, 103, 108, 119, 124, 135,140, 151 and 156. The code is fixed to correctly set up the backbone route. Workaround: Assign domain IDs to Brocade 7500 to avoid domain ID 7 and 12 and Brocade 48000 with FR418i blade to avoid the listed 16 domain IDs on the backbone fabric. Probability: Low Service Request# RQST00000059448 Reported in Release: V5.2.0
DEFECT000085437	High	Summary: Test script causes switch panic when rapidly cycling through repeated supportsave commands. Symptom: Test script running repeated, rapid supportsave commands causes out of memory (OOM) condition. Workaround: If this test situation is somehow duplicated in the field, stop performing repeated supportsaves. Service Request# RQST00000057220 Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000085660	High	Summary: E_Port or FL_Port is faulted and host cannot see target. This affects 4G/sec platforms with FL ports connected. Symptom: The host lost the target due to FL/E port being faulted with RASLog : CDR-5351], 217492/0, FFDC, CRITICAL, Brocade4100B, LKSM [OID 0x43028005] (2) (S0,BP5): Port to be faulted due to busy buffer stuck error, OID:0x43028005, proto_lksm.c, line: 1229, comp:swapper, ltime:1970/01/01-06:00:00 [CDR-1002], 217493/2792, FFDC, ERROR, Brocade4100B, Port 2 chip faulted due to internal error., OID:0x43028005, proto_lksm.c, line: 1232, comp:swapper, ltime:1970/01/01-06:00:00. Solution: When the LIP is received while the switch is no longer in the state of listening for LIP (after loop initialization is finished and switch has sent out the CLS), the LIP will cause the buffer to get stuck. This can also impact the receiving E_port due to buffer hold up on the FL port. The end result is that the port is being faulted. The code is fixed to process the LIP properly. Probability: Low Service Request# RQST00000059565 Reported in Release: V5.2.1
DEFECT000086639	High	Summary: 'Disable NodeName Zone Checking' parameter setting is incorrect in interopmode. Symptom: When interop mode was set to 1, 'Disable NodeName Zone Checking' parameter also changes from 0 to 1. But, 'Disable NodeName Zone Checking' was returned to 0 after switch was rebooted. Solution: If secure mode is disabled, "zoning.check.nodeNameDisabled" configuration should not be affected. Make sure the parameter stay at 1 in interop mode. Probability: Low Service Request# RQST00000060870 Reported in Release: V5.2.1

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000086687	High	Summary: FICON CUP daemon crashes after switch comes up when it starts processing the RNID command from FICON channels. Symptom: Multiple threads are working on the same request, which eventually leads to a daemon crash. This problem affects the FICON environment for Fabric OS v5.1 and later .The switch panics due to a ficu panic: kSWD: Detected unexpected termination of: "[4]ficud:0'RfP=712,RgP=712,DfP=0,died=1, Solution: Fixes a race condition in handling the RNID command. Probability: Medium Service Request# RQST00000060939 Reported in Release: V5.2.1
DEFECT000063566	Medium	Summary: With Web Tools, the error message is not clear when the fmsmode setting fails. Symptom: It is unknown what the exact error is that causes setting of fmsmode to fail when using Web Tools. Solution: Using a new error mapping function for FICON related errors. Customer Impact: Usability issue, with no impact to functionality. Probability: Medium Reported in Release: V5.1.0
DEFECT000068888	Medium	Summary: Web Tools is missing "Invalid CRCS" under Fabric Watch end to end class pull down menu. Symptom: Missing "CRC Error" option in Web Tools under End-to-End class. In CLI "Invalid CRCS" is displayed. Solution: Made code changes to avoid printing Invalid CRCS options for non bloom platforms. Customer Impact: Usability issue, with no impact to functionality. Probability: High Reported in Release: V5.0.5

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000070707	Medium	Summary: In AS4 and Sol10, All the Applets like Zone admin and name server windows are not refreshed properly after resizing. Symptom: GUI components size will be a bit squeezed. Solution: new GUI alignment solved the problem Workaround: Resizing the panel, Scrollbar comes. This happens only for the first time. Customer Impact: Cosmetic issue, with no impact to functionality. Probability: Medium Reported in Release: V5.2.0
DEFECT000071471	Medium	Summary: Need errlog messages for DHCP configuration/operations on a switch Symptom: errlog (RASLog) messages will not be available for diagnosing DHCP problems. Solution: Adds the logging of IP address changes that was requested Customer Impact: Usability issue, with no impact to functionality. Probability: Medium Reported in Release: V5.2.0
DEFECT000072169	Medium	Summary: Web Tools allows (switch,port) members to be added as a member of a zone when the switch is in interop mode. Symptom: The user might be led to believe that a zone with a member as (switch,type) is actually created successfully. Solution: When Switch is in interop mode in order to maintain consistency with CLI, made code changes to support WWN zoning and block D, P Zoning. Added check at Switch level also , to block adding D, P members. This scenario will come only on pizza box switch with interop mode enabled. For chassis based switch, switch level members cannot be added and user can check only at slot/port level. Check to handle this scenario is already present. Customer Impact: Usability issue, with no impact to functionality. Probability: High Reported in Release: V5.0.5

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000072269	Medium	Summary: Some switches are segmented with reason alias ID overlap when selected switches in fabric are configured to use Alias Server Symptom: Some switches are segmented with reason alias ID overlap when selected switches in fabric are configured to use Alias Server This defect will only show up when there is any switch in the fabric with active alias ID tokens defined. In this case, the Fabric OS v5.2 switch will segment out of the fabric with reason "domain overlap" in switchshow. But the console log will display a message with "alias id overlap". Although these messages are misleading the situation can be determined by fabricshow as it will display some alias tokens after the domain list. Solution: The fix is to prevent allocation and distribution multicast group IDs and tokens. Workaround: Fabric OS v5.2.0 does not support Alias Server. Refrain from using the Alias Server feature in fabrics that include Fabric OS v5.2.0 switches. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000072479	Medium	Summary: Solaris- Events list in Call Home e-mail is not getting updated with exact reason for alert because the switch is already in marginal state and the marginal event does not impact the current marginal status. Symptom: Customer will not get an event message for call home when switch status has an event that doesn't change the current switch status. For example, a switch in marginal state has another event that is marginal. Solution: Fabric Watch sends message when ever there is change in switch status from Healthy to Marginal/Marginal to Down /Down to Healthy/Down to Marginal. it gives a message describing the contributing factor for the status change. When switch status is changed to a Marginal or down state, the first contributing factor which has made the status change is reported, but if the switch remains in Marginal or down state and if some other factors(Power supply,Fan etc) goes down yet not changing the switch status such instances are not reported. Due to this we do not get the exact picture of all the factors that contributed for the switch status. This problem is resolved and messages are displayed reporting the status change with the contributing factor when there is switch status change also when the switch is in marginal/down state are reported as well. Workaround: user has to check switchstatusshow CLI for contributing factors. Customer Impact: Usability issue, with no impact to functionality. Probability: Low Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000072617	Medium	Summary: FCIP:Error message is not proper while editing\adding the subnet mask of an IP address conflicting from the existing IP Addresses. Symptom: In the Port Administration Services window, "IP Interfaces" tab, if the user edits/adds a subnet mask of an IP address that conflicts the with the existing IP Addresses the following behavior occurs: In the GE Port Configuration Wizard, an error dialog is shown with the message " Failed to edit IP Interface;Reason:com.brocade.dm.Dao Exception...". Solution: corrected error message displayed. Workaround: Input the correct subnet mask to correct the problem. Another workaround is to use the CLI command "portcfg". If the user makes the same mistake, a proper error message is generated. Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.2.0
DEFECT000072778	Medium	Summary: Device Connection Step in EZManager not differentiating ports as Storage and Hosts Symptom: User will not be able to differentiate between Storage and HBA ports if no devices/hosts connections are made. Solution: To show storage and host images for ports in device connection view. Workaround: Use EZSwitchSetup screen shot to see storage and HBA ports classification. Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000072942	Medium	Summary: send class 2 SOFi error frames from SANtester to attack switch with 600+ devices, Brocade 480000 reboots with wdtd on, extremely slow if wdtd is turned off. Symptom: Generation of a very big core file causes the system to remain busy for a long time. This results in a watchdog timer timeout. This is a rare case as nearly all daemons and applications do not generate a very big core file if they crash. Solution : Fixed by upgrading to Linux2.6 Probability: Low Reported in Release: V5.2.0
DEFECT000073596	Medium	Summary: The enc_out is increasing on unused ports on 2G bit/sec platforms after HAreboot. Symptom: The enc_out is increasing after a HAreboot or firmwaredownload operation in the unused ports. Solution: As part of solution, Enc Out counter is no longer incremented if the port is not active. Also changes have been made to reset these counters during HA reboot/firmware download if the port is not active. Service Request# RQST00000050503 Reported in Release: V5.0.5
DEFECT000073600	Medium	Summary: Web Tools should display "logged in" RADIUS account information Symptom: Web Tools is not displaying "logged in" RADIUS account information. Solution: Prevent user to change user account configured in RADIUS server in Web Tools. After WTBE sends User accounts from RADIUS server to WTFE, WTFE need to change GUI to prevent user to make changes to this account. Customer Impact: Cosmetic issue, with no impact to functionality. Probability: Medium Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000073608	Medium	Summary: SFP tab: SFP tab not showing the Units for temperature, and Rx power and TX power. Symptom: In Web Tools under SFP tab, the units for temperature, Rx and Tx power are not shown. Solution: Hardcoded units for temperature, rx power, tx power for an SFP or XFP. Mimicked the implementation CLI so that WTFE can be isolated from any change in the future.. Probability: High Reported in Release: V5.2.0
DEFECT000073903	Medium	Summary: Fabric Topology Window does not reflect the units for Bandwidth Demand and Total Bandwidth on Web Tools. Symptom: Customer will not be able to see the units of Total Bandwidth and Bandwidth Demand from Web Tools. Solution : Added Units for "Total Bandwidth" and "Bandwidth Utilization" attributes and "Total Bandwidth" attribute should always display the value in Gbps. Probability: Low Reported in Release: V5.2.0
DEFECT000074463	Medium	Summary: Web Tools should provide real fail reason when config upload fails due to invalid file path. Symptom: Customer will see an error message of " Directory change failed" instead of " File path provided is not valid" Solution : Enhanced configupload to use configupload API instead of configupload CLI and capture the output of ncftpput to get the exact error code for FTP provided "config upload failed due to invalid path." when failure occured. Probability: High Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000074876	Medium	Summary: F_Port Route cleanup does not happen correctly when NPIV is used Symptom: There is no obvious external symptom. An internal investigation discovered this deficiency. Solution: Implemented NPIV support for AG F_Port. The software now allows multiple logins on each F_Port of AG using NPIV protocol as described in FC-FS. Probability: Low Reported in Release: V5.2.1
DEFECT000074926	Medium	Summary: EZSwitchSetup: Device display is overlapped in Display Connection window. Symptom: If the window size is not maximized, the images of hosts and ports don't overlap. Even if they overlap, the two images do not merge completely and are easily distinguishable. Solution: Fixed the x-coordinate of switch image as zero so that on resizing the image, the x-coordinates of host/storage will not change and the images will not overlap. Reduced the y-coordinate of host/storage image by 20 pixels to avoid overlapping Workaround: Reduce the browser window size. Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.2.0
DEFECT000075058	Medium	Summary: portstatsclear help page description of behavior on 2GB and 4GB platforms is ambiguous Symptoms: help page shows inaccurate data Solution: The help page now clarifies the exact role correctly. Probability: Medium Service Request# RQST00000051350 Reported in Release: V5.0.4

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000075112	Medium	Summary: FR4-18i tracedump files contain many BLADE PROCESSOR (BP) error messages and one empty file. Symptom: Incomplete support files. Solution: In the new supportsave implementation on Blade Fabric OS (BFOS), on board ASIC statistics are not included. Hence updated the configuration file. Also updated the iflpr script file to check for the proc entry before accessing it. (This proc entry will be present only in FC4-16IP blade). Probability: Low Reported in Release: V5.2.0
DEFECT000075261	Medium	Summary: Scal_2560: After a couple of iterations all core switch fastboot, some of the E_Ports on core switch stuck in "Mod_Val" Symptom: When rebooting all core switches in a loop, E_Ports may get stuck in "Mod_Val" mode. Solution: Do a portdisable/portenable on the problem port and it will come online. Probability: Low Reported in Release: V5.2.0
DEFECT000075467	Medium	Summary: Error messages are generated when applying iSCSI easycreate operation from Web Tools on unreachable FC Targets. Symptom: No error messages if LUN information is not retrievable from an FC Target. Errors are only displayed when applying the operation. Solution. : Added a new property called EasyCreateWarning to iscsivirtualtarget class.. Will show list of all warnings along with FC WWNS for which it failed. Probability: Low Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000075565	Medium	Summary: Web Tools event filtering uses a time range of 0-11 as opposed to 1-12. Symptom: In Web Tools Fabric Events and Events window, on invoking filter button and filtering based on from time or to time, on providing a time greater than 12 (e.g. 12:30 PM) will result in an error stating that time should be in range of 0-11 Solution: Web Tools can go with 24hrs notation for event filtering instead of 12hrs.or Web Tools can go with "(1-12)" hour in am/pm instead of existing "(0-11)" hour in am/pm. Probability: Medium Reported in Release: V5.2.0
DEFECT000075615	Medium	Summary: Additional Port Info column in FC Ports tab shows "None (FMS Mode)" instead of "Disabled (FMS Mode)" Symptom: Additional Port Info column in FC Ports tab shows "None (FMS Disabled)", although CLI shows it as "Disabled (FMS Mode)". Solution: An API similar to switch_port_is_active_fms_port() should be provided to web linker. Workaround: The user can refer to the jPortStatus column in FC ports tab to know the port status. Customer Impact: Minimal, since there is a workaround. Probability: Low Reported in Release: V5.2.0
DEFECT000075760	Medium	Summary: During firmware download upgrade process, seeing "Blade rebooted during firmware commit The operation will be restarted." messages for FR4-18i blades after the commit has started on these blades. Symptom: firmwaredownloadstatus output shows that FR4-18i blades both rebooted during a firmware commit process that had already started. The process recovers. Solution: Increased timeout values in the Blade Management (BM) code). Probability: Medium Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000075911	Medium	Summary: EZSwitchSetup: Fixed zone cannot be configured with all ports designated as storage or hosts. Symptom: The correct constraint is being enforced, but the message displayed does not describe how to correct the misconfiguration. Solution: Modified the message to display a meaningful message when user selects all ports as either storage or host. Probability: Medium Reported in Release: V5.2.0
DEFECT000076026	Medium	Summary: Error messages observed during IPsec FCIP IO. Symptom: On initiating IPsec FCIP IO, error message displays on console: "[CDR-5206], 0,, ERROR, sprint_73, UPSM [OID 0x4302880a] (1) (UP10): Invalid event [0x1030035, 0x0, 0x0], OID:0x4302880a, proto_upsm.c, line: 1797, comp:snmpd, ltime:1970/01/01-00:00:00". Solution : Switch driver updates the EX_Port domain when the port is disabled. If the EX_Port is a slave port, the new embed route with the new domain(switch domain) could collide with the existing domain route for the edge fabrics. This can cause the EX trunk's domain route corrupted. So we should avoid update the embed route for EX slave port. Probability: Medium Reported in Release: V5.2.0
DEFECT000076037	Medium	Summary: LinkRNIDDeviceRegistration trap provides wrong nodeRNIDIncidentPortWWN and nodeRNIDConnectedPortWWN Symptom: Wrong information during request node identification data (RNID) registration. Solution: Fill the incident port WWN and connected port WWN fields before calling ms_ficon_notification() Probability: Medium Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076060	Medium	Summary: Port type gets swapped in the SAM Report when the port indices of 2 ports are swapped. Symptom: Customer will see wrong port type after port swap on issuing fwsamshow from CLI. Solution: Function getPortTypeNameFormat expects port number as input and not the index number so invoking getPortFromIndex function for the same. Probability: Medium Reported in Release: V5.2.0
DEFECT000076110	Medium	Summary: Name server daemon (nsd) panic results in CP fault after firmware download. Symptom: Error Message: [KSWD-1003], 8,, WARNING, Brocade24000, kSWD: Detected unexpected termination of: "[0]nsd:0'RfP=689,RgP=689,DfP=0,died=1,rt=53469, dt=49072, to=50000, aJc=1969,aJp=0,abiJc=-250011492, abiJp=0, aSeq=1,kSeq=0,kJc=0,kJp=0,J=4397 ,rs=2' Solution: Gracefully handle invalid zone type during zone enforcement after failover. Service Request# RQST00000051760 Reported in Release: V5.0.5
DEFECT000076112	Medium	Summary: FCIP:In the absence of IPSEC license,"Show IP Security policies" doesn't give the policy details where as secured tunnel gives the IPSEC policies associated with it. Symptom: The customer will be unable to view the policy details in the absence of IPSEC license from "Show IP Security policies". Solution: Removed license check when processing policy show command. Probability: Medium Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076195	Medium	Summary: After changing an expired password and selecting another AD during the same session, the password expiration message and password prompt are displayed again. Symptom: User has to change the password on every ad select in the same session. Solution: Unset the "passwd_aged" environment variable, after an expired password is successfully changed during login. This makes sure no additional prompting appears when "ad --select" is run in the login session.. Probability: Medium Reported in Release: V5.2.0
DEFECT000076255	Medium	Summary: Error messages from ACL configuration through SMI are too generic and do not contain sufficient information to debug the problem. Symptom: CAL returns "Error in PolicyAdd", this is not sufficient for end user to figure out what the problem was. Solution: convert errocodes returned by sec/acl libraries to descriptive string using function provided Probability: High Reported in Release: V5.2.0
DEFECT000076260	Medium	Summary: Portstats: Selecting the "Show delta" radio button and clicking on the clear counter button does not clear the counters; instead it changes the values to negative. Symptom: Clicking on the clear counter button does not clear the counters; instead it sets the values to negative. Solution: On selecting show delta button, stats will be first shown as zero, then after first refresh cycle, it will show delta values. Even on clicking 'Clear Counters' button, it will first show all zero values, then after first refresh cycle, it will show new values. Probability: Medium Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076265	Medium	Summary: FFDC files are generated when IP address is manually set to a switch which is in DHCP network Symptom: Customer may see FFDC warning messages when manually changing switch IP address Solution. : Listen to IPv6 addresses Customer Impact: Cosmetic issue, with no impact to functionality. Probability: Low Reported in Release: V5.2.0
DEFECT000076269	Medium	Summary: No warning message is displayed when using Web Tools to configure/Edit FCIP tunnels with the Fast Write -tape pipelining feature Symptom: When configuring fast write using Web Tools, the customer will be not receive a warning indicating that the Fast Write and tape pipelining features should not be used with multiple equal cost paths. Solution: Fix some FCIP defects related to message, dialog exception throw out. Customer Impact: Cosmetic issue, with no impact to functionality. Probability: Medium Reported in Release: V5.2.0
DEFECT000076272	Medium	Summary: Able to establish API session to AD 255 using "user" login which has AD membership only to AD 0 which is not allowed from CLI. Symptom: End users of SMI and Web Tools will not observe this error because all operations are performed via an Admin role user. Solution: Check if incoming request has logged in with new header information that contains ad and verify that the ad is allowed for the user specified during login. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076308	Medium	Summary: Web Tools should make the feature consistent with CLI and allow user to configure long distance for ports if current AD owns these ports but not switchmembership Symptom: Port long distance settings are read-only for owned ports on non-owned switches in WT Extended Fabric tab, but editable for owned ports in WT port configuration wizard. Solution: Extended Fabric panel had not been modified to support a filtered view of the E_Ports on a switch, because the original requirement had been that port distance settings would be read-only if the switch was not owned. When the panel became read/write, port numbers for filtered ports were not being handled correctly, resulting in index out of bounds errors and updates being sent to the wrong ports. These problems are now fixed, but a remaining issue is that non-owned E_Ports on a non-owned switch are not being presented in read-only mode, as they would be in the main port admin module. A new defect will be opened for this problem, which requires a back-end change. Workaround: Use the Web Tools port configuration wizard Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.2.0
DEFECT000076373	Medium	Summary: When a port is taken out of a faulty state implicitly by removing the cable or removing a module, SNMP traps are repeatedly sent. Symptom: SNMP traps are repeatedly sent from the switch every 2 seconds. Solution: The SNMP trap problem was caused by too many port offline SCNs being sent out during port fault and recover when there is laser fault. The fix will send an offline SCN to the upper API if and only if there is no light or no module. (Cover cable remove & module remove cases only) Probability: Medium Service Request# RQST00000051666 Reported in Release: V5.0.5

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076400	Medium	Summary: Firmware downgrade to Fabric OS v5.1 or prior is blocked even after ports 256-383 are removed from a DCC policy created using [*] option. Symptom: Every time ports are removed, VERIFY is displayed on console. Deleting the DCC policy will resolve the problem. Solution: When using secPolicyRemove DCC_POLICY_xxx sw[p0 pN] to remove ports from the DCC member list, if there is a device WWN member, and the removed ports are at the tail end of the current port list, there will be a trailing comma at the end of port list. For example, if current DCC policy is: SwitchWWN(0, 1, 2, 3, 4, 5, 6);DeviceWWN. If port 5 & 6 is removed, the DCC policy will become SwitchWWN(0, 1, 2, 3, 4,);DeviceWWN. Since some code path is counting the number of commas as the number of ports in the DCC policy, this will lead to logic error. Existing code already takes out trailing comma if port list is at the end of policy. But when port list is followed by Device WWN, the logic doesn't work. Since the removal logic uses # to mark the ports to be deleted, added extra code to detect the condition of comma followed by all # before the closing parenthesis), and take out the trailing comma. Workaround: Delete that DCC policy and continue Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.2.0
DEFECT000076401	Medium	Summary: Admin having permissions to just AD255 is able to create ADs through configdownload. Symptom: Admin user account with permissions to only AD255 will be able to create Admin Domains. Expected behavior is that only Admin user accounts with permissions for all ADs should be able to create/modify ADs. Solution: We can not make a direct call to security library from zoning library, so I made a replica of secAmIPFAdmin in zone library. Customer Impact: Usability issue, with no impact to functionality. Probability: Medium Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076430	Medium	Summary: The confirmation dialogue is not appearing when we close the name server table by clicking the 'X' button. Symptom: User will experience an unexpected close by clicking the 'X' button accidentally. Solution: Conformation dialog is removed from the Close button. Workaround: Customer can click on the Yes / No instead of the "X" button Customer Impact: Usability issue, with no impact to functionality. Probability: Low Reported in Release: V5.2.0
DEFECT000076433	Medium	Summary: Detailed view of any device does not refresh properly when Auto refresh option is selected. Symptom: Customer will see empty values for Name Server entry in the detail view, upon attempting to resize/scroll the window. Solution: Event Filter Hour format has Changed from "0 to 11" to "1 to 12" and Tested with some Filter operation corrected the alignment. Workaround: Close and open the detail view dialog after the refresh cycle. Customer Impact: Minimal, since there is a workaround. Probability: Low Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076462	Medium	Summary: Role name(and sometimes user name also) missing from error message when a user exits from a telnet session Symptom: SEC-3022 misses the role name or user name. Solution: The solution is getting the ENV variables from the pam and then displaying them in the AUDIT message. Role name was not appearing when a user exits out of the telnet session. Explicitly setting the role name in pam_sm_close_session will make the role name appeared in the SEC-3022 Explicitly setting the role name using gset_role for getting appeared in the AUDIT messages Workaround: Look at SEC-3020 audit message (logged when a user logins) for the particular user and find his role. Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.2.0
DEFECT000076490	Medium	Summary: Brocade 3850 with port configured for longDistance and R_DY transmits ARB(vc). Symptom: Brocade 3850 running Fabric OS v5.2 with the following port configuration: - portcfglongdistance <port> LS 1 50 - portcfgislmode <port> 1 produces ARB (vc) fill words instead of idles. This might cause failures with certain long distance devices Solution: The driver was enabling ARB(vc) flow control primitive for long distance links irrespective of flow control mode negotiated or set through CLI portCfgIslMode. Added an additional check for VC_RDY flow control mode before setting ARB (vc) as flow control primitive. Workaround: fabric.ops.mode.longDistance must be set on all switches in fabric. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076498	Medium	Summary: Web Tools is not correctly reflecting the physical switch state of a persistently disabled switch when the switch is fastbooted. Symptom: Web Tools shows port LEDs as dark (not lit) instead of slowly blinking yellow when switch does a fastboot after it is persistently disabled. Solution: update the port speed and led even when switch is persistently disabled or investigate further and see if this is expected behavior. Customer Impact: Cosmetic issue, with no impact to functionality. Probability: Medium Reported in Release: V5.2.0
DEFECT000076509	Medium	Summary: No event is generated when the IP address of a switch is changed. Symptom: Customer cannot determine that the IP address of the switch was changed by issuing the command errdump or errshow because an ip address change event was not registered. Solution: Log a RASLOG message whenever IP address is changed through non-web interfaces. Customer Impact: Usability issue, with no impact to functionality. Probability: Medium Reported in Release: V5.2.0
DEFECT000076514	Medium	Summary: Several issues observed in ZoneAdmin and in AD when the switch is configured in PID format 2 Symptom: Customer will not able to see the ports 16-32 when configuring a switch in PID 2 format Solution: Enhanced the area ID mapping when PID format change to 2. Workaround: Perform zoning operations from the CLI when the switch is configured in PID 2 format. Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076538	Medium	Summary: Fabric is busy after running a group of commands repeatedly and not able to execute any commands. Symptom: Switch may report fabric busy following a long string of operations Solution: incorporate brocade times() in toolchain so that there is no 5 second lag during jiffy roll-over Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Medium Reported in Release: V5.2.0
DEFECT000076545	Medium	Summary: When using interactive mode to execute pathinfo with an invalid source port value, there is no errors message. If execute the pathinfo with an invalid source port value, it will tell user there is no response. Symptom: User may think that the invalid source port value is being taken because there are no error or warning messages. Solution: In interactive mode, if the source port value is given as MAX_PORT, it is assumed as embedded port (documented in man page) but in non-interactive mode, pathinfo gave error message as "No Response". In order to make the behavior same in both interactive and non-interactive mode, the source port value is assumed -1(embedded) if the given value is MAX_PORT in non-interactive mode.. Workaround: Use pathinfo cli command in batch mode. Customer Impact: Usability issue, with no impact to functionality. Probability: Medium Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076550	Medium	Summary: iSCSI: Inconsistent results when a login request is rejected by FC4-16IP Symptom: After receiving a login reject, intermittently under some conditions the subsequent login attempts may fail as well. Solution: Move the session back to init state after rejecting a login. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Medium Reported in Release: V5.2.0
DEFECT000076585	Medium	Summary: iSCSI: Switch runs out of memory when running slotpoweroff/on continually on two separate FCR-16IP blades. Symptom: Switch may run out of memory if continually running slotpoweroff/on on multiple iSCSI gateway blades for a long period (> 9 hours). Solution: The timeout of tftd server is 15 minutes by default. When running slotpoweroff/on stress test, there are about 80 tftpd server instances on CP after 14 hours testing. The change here is to tune the timeout to 3 minutes so that tftpd server is terminated if there is no activity for 3 minutes. This improves the system resource usages. Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Low Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076597	Medium	Summary: In Secure FOS, Web Tools gets null pointer from java console when trying to modify default admin and user accounts Symptom: In SFOS, when the attempt is made to modify default admin account (login as root) and user account (login as root or admin), Web Tools should bring up the modify dialog for user to modify description and/or status. A null pointer exception appears in java console. Solution: Enhanced AD capable check in Secure FOS. Add protection to null object comparison. Workaround: Use CLI to complete modifying the default user account in secured FOS. Customer Impact: Minimal, since there is a workaround. Probability: Low Reported in Release: V5.2.0
DEFECT000076681	Medium	Summary: iSCSI: SendTargets=All sends portal information of disabled GE ports to 3rd-party host during login. Symptom: 3rd-party host takes a long time to log in due to wrong portal information being sent. Solution: If the portal is configured with an IP address, the port is considered for reach ability by the host at any point in time. To interop with 3rd-party OS, user should remove the IP address of the ports that are disabled or not reachable by the 3rd-party port. Workaround: Remove the IP address of the disabled port. portcfg ipif slot/ge# delete <ipaddress> <netmask> Customer Impact: Usability issue, with no impact to functionality. Probability: High Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076687	Medium	Summary: ISCSI: iSNS console log reports incorrect name for management port. Symptom: The console log for iSNS reports the management port as slot/port 0/0. Solution: Add new RASLog message for the case where the user configures isns server to communicate through the management port. Customer Impact: Cosmetic issue, with no impact to functionality. Probability: High Reported in Release: V5.2.0
DEFECT000076693	Medium	Summary: iSCSI: AIX host is not able to see disks after successful login (with and without CHAP) when immediate data is set to enable Symptom: The user may not see the targets after successful iSCSI login using AIX if immediate data is enabled. Solution: Fix text parameter processing code to return the negotiated value instead of configured value. Workaround: Disable immediate data Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.2.0
DEFECT000076710	Medium	Summary: ISCSI: with multiple switches in the fabric and ISNSC enabled, error is logged on only one switch. Symptom: iSNS error message is logged on only one switch in the fabric: it should be logged on all switches. Solution: Modified to log RASGLOG message for detecting multiple iSNSC enabled switches in fabric on all iSCSI enabled switches. Customer Impact: Usability issue, with no impact to functionality. Probability: Medium Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076732	Medium	Summary: After changing Backbone FID, switchshow not displaying some LE Port information. Symptom: Switchshow output is incorrect; LE port information is not displayed for some EX_Ports or VEX_Ports. Solution: In a setup where there are two FCRs in the same BB connecting to the same edge fabric, there is a time window where both FCR are disconnected from the edge, but none of them detects this condition because LRNE are sent every five seconds. If the old owner port comes up quickly, the old proxy device is not cleaned up, and therefore the new xlate domain is not established. Workaround: LE_Ports are functioning correctly, only a display issue. Customer Impact: Minimal, since there is a workaround. Probability: Low Reported in Release: V5.2.0
DEFECT000076736	Medium	Summary: LE ports are not up after trunkdisable/enable. Symptom: EX_Port does not go online Solution: unknown - need to recreate the problem to get the fcrlog right after the error occurs. Workaround: The work around is switchdisable/enable of the FCR switch. Customer Impact: Minimal, since there is a workaround. Probability: Low Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076740	Medium	Summary: During switchdisable/switchenable test, found EX_Port is left Disabled (Setting VC Credits failed). Symptom: EX_Port fails to come online after switch is enabled and switchshow shows the port is disabled due to (Setting VC Credits failed), User has to manually restore the port. In addition, when the Ex port trunk master is unplugged, non-trunk master ports are disabled. Solution: The fix is not to disable the port if the port is already offline. Workaround: Disable and then enable the EX_Port . Probability: Low Reported in Release: V5.2.0
DEFECT000076760	Medium	Summary: execquery(Brocade_SwitchFcPortRateStats) is not returning correct Instances, Symptom: execquery(Brocade_SwitchFcPortRateStats) is not returning correct Instances, When AD's are created in the Switch Side without stopping the SMI-A it always returns Instances with respect to AD0. Solution: When a request comes from user defined AD, bypass the cache. Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.2.0
DEFECT000076786	Medium	Summary: Sometimes when trying to add/modify AD list for multiple user accounts simultaneously, AD list for user accounts changes. Symptom: When this happens, the AD list for the first add/modify user account will be added to the second or following add/modify user accounts AD list. Solution: Enhance the string buffer handling for user AD list Workaround: Apply the change for adding or modifying user account AD list one user at a time. Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000076815	Medium	Summary: Port Detail Report displays the iSCSI Ports. Symptom: Customer sees the iSCSI ports in the Port Detail Report, also shows incorrect values. Solution: FW CLI fwportdetailshow was displaying iSCSI ports. Code changes are made to fix this. Customer Impact: Cosmetic issue, with no impact to functionality. Probability: Medium Reported in Release: V5.2.0
DEFECT000076911	Medium	Summary: swFCPortOpStatus of swFCPortScn is not reported correctly trap.<H556> Symptom: swFCPortOpStatus of swFCPortScn is not reported correctly. Solution: In case of Laser_Flt physical state of Port, properly populate the attribute for swFCPortOpStatus. Probability: Low Service Request# RQST00000052638 Reported in Release: V5.2.0
DEFECT000076913	Medium	Summary: Excessive "logins" cause out-of-memory (OOM) panic. Symptom: Switch panics while switching between user roles and executing "Configshow" command. Solution: Enforce a maximum limit of the use of "login" command similar to the enforcement of maximum telnet sessions and total sessions. Workaround: Although using login again and again appears to be performing a new session, realize that this is not actually happening. When working with the switch after about 5 logins, perform a logout and then login again before continuing. Service Request# RQST00000052689 Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000077105	Medium	Summary: Reported vulnerabilities about open SSL VU#386964 & VU#547300 Symptom: VU#547300:OpenSSL SSL_get_shared_ciphers() vulnerable to buffer overflow < http://www.kb.cert.org/vuls/id/547300> VU#386964:OpenSSL SSLv2 client code fails to properly check for NULL < http://www.kb.cert.org/vuls/id/386964> Solution: FOS v5.3 upgraded to OpenSSL 0.9.8d, which contains fixes for vulnerabilities VU#386964 & VU#547300 Service Request# RQST00000052641 Reported in Release: V5.0.4
DEFECT000077107	Medium	Summary: Denial-of-Service Condition Affecting X.509 Certificates Verification (NISCC#729618) Symptom: CVE-2006-2937 http://cve.mitre.org/cgi-bin/cvename.cgi?name=2006-2937 OpenSSL 0.9.7 before 0.9.7l and 0.9.8 before 0.9.8d allows remote attackers to cause a denial of service (infinite loop and memory consumption) via malformed ASN.1 structures that trigger an improperly handled error condition. CVE-2006-2940 http://cve.mitre.org/cgi-bin/cvename.cgi?name=2006-2940 OpenSSL 0.9.7 before 0.9.7l, 0.9.8 before 0.9.8d, and earlier versions allows attackers to cause a denial of service (CPU consumption) via parasitic public keys with large (1) "public exponent" or (2) "public modulus" values in X.509 certificates that require extra time to process when using RSA signature verification. Solution: FOS v5.3 upgraded to OpenSSL 0.9.8d, which contains fixes for vulnerability NISCC#729618 Workaround: None Service Request# RQST00000052640 Reported in Release: V5.0.3

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000077357	Medium	Summary: Incorrect time in Web Tools Switch Health Report. Symptom: The time of Switch Health Report in Web Tools is not correct after using the tstimezone command with "--old" option. Solution: The "Wed Nov 1 2006 01:03:37 GMT-3" timestamp is in POSIX format. It is equivalent to "Wed Nov 1 2006 01:03:37 GMT+3:00" which is a more commonly accepted format. Made changes to change from former to latter for consistency in WT. Probability: Low Service Request# RQST00000053108 Reported in Release: V5.2.0
DEFECT000077986	Medium	Summary: Incorrect port behavior when the RX side of the cable is disconnected, while the TX side is still inserted. Symptom: Disconnect the RX cable going into the switch; expect Loss of Synchronization for a period of more than R_T_TOV so that HBA can flag the link as down to trigger the software to use another path. But it takes almost 150 seconds for path failover to happen and it is too long for database management applications. Solution: Send out LIP in loss of light situation to notify the remote side. Probability: Low Service Request# RQST00000054158 Reported in Release: V5.2.0
DEFECT000077992	Medium	Summary: Installation of PKI certificate is delayed on specific switches due to timing of the startup function. Symptom: After installed certificate into Brocade 5000, pkishow still indicated "EMPTY" Solution: remove the startup function as this is no longer needed for the thread to process requests. Reported in Release: V5.2.1

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000078105	Medium	Summary: The last character of config uploaded Banner will disappear Symptom: Performing a configupload followed by configdownload removes the last char of any banner text that was set earlier via the "bannerset" CLI command. Solution: Fix code to not assume there is line feed character. Probability: Low Service Request# RQST00000054386 Reported in Release: V5.2.0
DEFECT000078134	Medium	Summary: Name server operation not consistent with Brocade Mi10K Director. Symptom: While running in open mode, the RSCN received from a Brocade Mi10K Director in the fabric was not immediately forwarded. This delay in RSCN processing is only observed while connected to a Brocade Mi10K Director in open mode. Solution: During processing of the Device Online RSCN from i10K, extract the Port Id from the Device Entry of the RSCN payload by masking off the Port State byte. This caused the RSCN to not get processed and forwarded to local devices. At a later point GE_PT was issued and based on the response from i10K it was determined that the remote device was now online and a RSCN was generated to the local device. This is the reason why the RSCN sent out to the local device seemed to be delayed. This problem has not been seen with other McDATA Switches because the Port State field in the device entry of the RSCN is zero. This masked the bug until we hit it on i10K. Service Request# RQST00000054439 Reported in Release: V5.2.0
DEFECT000078313	Medium	Summary: Brocade 4016 displays incorrect RASLog message for a failover situation when the Access Gateway switch is rebooted. Symptom: Port goes offline and comes back online during Hot Code Load or HAreboot Solution: Mark a port as logically online when FLOGI is complete instead of waiting FCP probing. FCP probing is not performed when the Access Gateway mode is enabled on a switch. Customer Impact: Cosmetic issue, with no impact to functionality. Probability: Low Reported in Release: V5.2.1

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000078467	Medium	Summary: The counter Address_err seems to be counting inappropriate data. Symptom: Address_err on FOSv5.2.0a isn't counted even if Switch receives the invalid SOFc1 frames. Solution: Invalid class frames (C1, C4) were dropped but not counted in any of the portShow counters; fixed by counting such errors in the "Delim_err" field of portShow; and added this counter into slotErrShow also. Customer Impact: Usability issue, with no impact to functionality. Probability: High Service Request# RQST00000054781 Reported in Release: V5.2.0
DEFECT000078585	Medium	Summary: When assigning an IP address to a GE port with no cable connection, the FC4-16IP blade reports back to the iSCSI initiator that the port is valid. Symptom: Since the sendtarget reply will have the IP address of the offline port, any request to that port will delay the host operation. The customers will notice a delay in getting the updated information. Solution: If the port is offline, then the IP address assigned to the port is not given in sendtarget response. Service Request# RQST00000055012 Reported in Release: V5.2.0

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000078622	Medium	Summary: "Fan * is not faulty." messages occur after upgrade to Fabric OS v5.2.0x. Symptom: A customer would see the following messages on bootup of the switch. [HIL-1208], 10,, INFO, SilkWorm200E, Fan 1 is not faulty. [HIL-1208], 11,, INFO, SilkWorm200E, Fan 2 is not faulty. [HIL-1208], 12,, INFO, SilkWorm200E, Fan 3 is not faulty. The Fans are NOT faulty, and do not need to be replaced. This is simply an informational message that shall be removed in future releases to avoid any confusion. Solution: EM uses skipFlag which skips all the reading's of the sensor in the boot up sequence since most of the reading are error prone. since we poll the sensors often, hence reading the sensor again gives the right values. Service Request# RQST00000054728 Reported in Release: V5.2.0
DEFECT000078793	Medium	Summary: Disconnecting the Rx end of the cable on an L_Port and leaving the Tx end unchanged results in unexpected behavior. Symptom: The device is HBA comes up as a Loop device, unplug the RX cable on Brocade bloom based switch, no Async Event and no sufficient LIP are genera Solution: Send out LIP in los light situation to notify the other side; Service Request# RQST00000055104 Reported in Release: V5.0.5

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000079304	Medium	Summary: Access Gateway should handle an IPv6 address in a GMAL payload. Symptom: IP Address in "ag --show" truncated to 16 characters (which is the size of IPv4 address) depending on the size of IP address string for edge switch to which N_Port is attached. Fabric OS v5.2.1 supports IPv4, not IPv6. Solution: Added IPv6 support for Access gateway. Following CLIs will display IPv6 address if configured "agshow --name <AG>" on attached fabric. "ag --show" will display IPv6 address of the AG switch itself Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.1
DEFECT000079553	Medium	Summary: switchdisable and switchenable on switch that directly connects to storage will cause the storage to see GLIEN reject error message. Symptom: GLIEN reject error message. Solution: For GLIEN command, removed the remote switch MS service capability check before forwarding which was based on firmware version check. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Medium Reported in Release: V5.2.1

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000079747	Medium	Summary: Brocade 4100: F_Port count is incorrect in agshow --name <AG> Symptom: User will observe that F_Port count is incorrect in agshow --name <AG>. Solution: During registration of AG attributes with a fabric, only register those F_Ports that are online and mapped to N_Port(s) connected to the same fabric Workaround: Make sure N_Ports of Access Gateway are connected to switches in a single FC fabric Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Low Reported in Release: V5.2.1
DEFECT000079968	Medium	Summary: CLI: iscsicfg --show/delete ddset -n xxx complains "Requested object doesn't exist" even though that object does exist. Symptom: User could not use iscsicfg --show ddset -n or iscsicfg --show dd -d or iscsicfg --delete ddset -n, ... on those DD/DDSETs received from Microsoft iSNS server. Solution: iSNS client to convert DD and DDSet name to lowercase. Workaround: Use iscsicfg --clear dd for clear ddset and dd. Customer Impact: Minimal, since there is a workaround. Probability: Medium Reported in Release: V5.2.1
DEFECT000080439	Medium	Summary: iSCSI: During 1024 session testing, one of the ports lost multiple sessions after approximately 4 hours of traffic run Symptom: switchshow -iscsi shows less than 64 sessions on the port, but the iSCSI initiator will not be able to log in to the target (out of resources error). Solution: Add timer to cleanup the resources if not all IO context were cleaned up. Customer Impact: Should not occur under normal maintenance operation; resulted from stress-to-fail testing designed to push the limits of the switch and fabric to point of failure. Probability: Medium Reported in Release: V5.2.1

Defect ID	Severity	Description of Newly Closed Defects with Code Change
DEFECT000082722	Medium	Summary: Incorrect GID_FT response from NameServer. Symptom: The NS assumes that the device's FC4 type is FCP when the GID_FT request is sent to the switch asking for PIDs of type FCP. The PID of the sending device is incorrectly included in the reply list Solution: When a host without a FC4 type comes online and FCP is assumed before UPD_AREA SCN is received, ensure not to include host PID in reply list to all NS queries based on FC4 type (GID_FT, GPN_FT, GNN_FT). Service Request# RQST00000057411 Reported in Release: V5.2.1
DEFECT000083680	Medium	Summary: Unable to merge an upgraded switch with a Brocade 48000 with an FC4-48 blade when using domain/port zoning of the upper 32 ports of the blade. Symptom: When creating a D,P zoning definition that uses the upper 32 ports of an FC4-48 blade, connected to another switch running Fabric OS v 5.1.0, the two switches properly segment due to the zoning conflict. After upgrading the firmware to Fabric OS v5.2.0, the switches remained segmented, though the correct behavior is to remove the segmentation. Solution: The zone HA version was not properly being updated during HAreboot. Fixed code to correctly update the zone HA version, allowing the subsequent zone merge between the upgraded switch and a Brocade 48000 at Fabric OS v5.2 to properly resolve without segmentation. Workaround: Remove the specific D,P zone, enable the zone config, and then re-add the D,P zone, and enable the zone config. Or Only use D,P zoning for the upper ports of a FC4-48 blade after all switches in the fabric have been upgraded to Fabric OS version 5.2.0 or higher. Or use WWN zoning. Probability: Medium Service Request# RQST00000056725 Reported in Release: V5.2.0