BROCADE

Brocade Fabric OS v5.2.2a

Release Notes v1.0

August 21, 2007

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v5.2.2a Release Notes v1.0	First Release	August 21, 2007

Contents

Quick Look for Fabric OS v5.2.2a

Fabric OS v5.2.2a includes the content of all previous v5.2.x releases. If you are already using the most recent version of the Fabric OS v5.2.2 Release Notes, here are the changes in this version.

- The list of the closed defects for Fabric OS v5.2.2a is added at the beginning of the defect tables at the end of this release note.
- An issue regarding Brocade 7500 and FR4-18i devices dropping frames under high-stress bi-directional FCR traffic conditions is described and a new internal AP route policy is added to dedicate some links for ingress traffic and some links for egress traffic. This is documented in the beginning of the Fabric OS v5.2.2a Documentation section of this release note.

Fabric OS v5.2.1 Overview

Hardware

Fabric OS v5.2.1 supports the merge of the Fabric OS 5.0.x software features with those of the Fabric OS v5.2.x software features. This means that in addition to the switches already supported by the Fabric OS v5.2.x software, the following embedded switches are supported in Fabric OS v5.2.1:

- Brocade 3014
- Brocade 3016
- Brocade 4012
- Brocade 4016
- Brocade 4018
- Brocade 4020
- Brocade 4024

In addition, Fabric OS v5.2.1 supports the new Brocade 5000 switch.

The Brocade 5000 Switch

The Brocade 5000 switch is a 32-port autosensing 4/2/1 Gbit/sec Fibre Channel switch that includes advanced interoperability capability for McDATA fabrics, enhanced operating efficiency and optimized system design. The Brocade 5000 is targeted for use as a standalone switch in small SANs, or as an edge switch in larger SAN environments.

Software

Fabric OS v5.2.1 supports a new feature, Access Gateway only on the following embedded switches:

- Brocade 4012
- Brocade 4016
- Brocade 4020
- Brocade 4024

NPIV functionality has been available on the Fabric OS v5.1.x and 5.2.x platforms and is also supported in Fabric OS v5.2.1 on embedded blade server SAN switches including the Brocade 3014, 3016, 4012, 4016, 4018, 4020, and 4024. No NPIV license is required.

Web Tools in Fabric OS v5.2.1 supports the enabling and disabling of Access Gateway, as well as firmware download and various monitoring functions. There is also SNMP support for Access Gateway. Fabric Manager 5.2.0 does not support the Access Gateway feature. Both Web Tools and Fabric Manager 5.2.0 support the new Brocade 5000 switch.

Fabric OS v5.2.1 supports Dynamic Ports on Demand (DPOD) on the following embedded switches:

- Brocade 4016
- Brocade 4018
- Brocade 4020
- Brocade 4024

In addition, Fabric OS v5.2.1 includes fixes for various FOS defects and various Requests for Enhancement (RFEs).

New Features in Fabric OS v5.2.1

Access Gateway

Access Gateway allows a switch to operate in a special 'agmode' that allows simplified connectivity between large numbers of servers and the SAN. Access Gateway leverages NPIV (N_Port ID virtualization) to hide the complexity of the servers (both physical and virtual) attached to it while allowing easy SAN connectivity. The edge fabric switch provides all the fabric services while Access Gateway connects to the edge switch by what appears as an HBA connection. This architecture allows the deployment of many additional servers without requiring a domain and the associated fabric rebuild traffic that is prevalent in dynamic blade server environments. On Fabric OS v5.2.1 Access Gateway is available on the Brocade 4012, 4016, 4020, and 4024.

Dynamic Ports on Demand

Dynamic Ports on Demand (DPOD) is an optional feature on selected embedded switches. DPOD takes the expansion capability of fixed Ports on Demand (POD) and adds the flexibility of connecting to any available port as long as a valid license is available. Previously, POD allowed only specific fixed ports to be utilized. With DPOD, any physically available port can be made active as long as a valid license is available. This allows customers the flexibility of automatically changing port assignments where previously the port assignments were fixed and inflexible. DPOD is tailored for dynamic environments such as blade server deployments and is available on the Brocade 4016, 4018, 4020, and 4024.

New Features in Fabric OS v5.2.0

Brocade Fabric OS v5.2.0 supports two new hardware blades for the Brocade 48000 director: Brocade FC4-48 Fibre Channel port blade and Brocade FC4-16IP iSCSI blade.

- The **FC4-48** port blade offers 48 1, 2, and 4 Gbit/sec Fibre Channel ports for the Brocade 48000 director. Brocade continues to provide its customers with state-of-the-art scalability and a SAN enterprise solution with the industry's lowest power consumption.
- The **FC4-16IP** iSCSI blade enables the Brocade 48000 director to provide iSCSI initiators to FC target connectivity. It features eight auto-sensing 1, 2, and 4 Gbit/sec Fibre Channel and eight 1 Gbit/sec Ethernet (1000Base-T) RJ-45 ports.

Fabric OS v5.2.1 supercedes Fabric OS v5.2.0. All users are strongly encouraged to upgrade to v5.2.1 as soon as they have access to it.

NOTE: Install Fabric OS v5.2.1 software *before you install the new blade types (FC4-16IP or FC4-48).*

New features in the Fabric OS v5.2.0 release are summarized in the following sections.

RAS (Reliability, Availability, Serviceability)

- **Audit logging** provides logs per user-generated events, such as security violation, zoning, firmware download, and configuration changes.
- **Configuration management enhancements** improve switch availability by allowing Fabric Watch and SNMP parameter changes to be non-disruptive.
- **Firmware upgrade enhancements** provide clearer error messages and remove the need to enter "release.plist" in the command line.
- **Daemon restart/monitoring** restarts management daemons automatically when they fail without switch reboot:
    - Snmpd - simple network management protocol daemon
    - Webd - web server daemon
    - Cald - common access layer daemon
    - Rpcd - remote procedure call daemon
    - Arrd - asynchronous response router daemon (send management data to hosts when the switch is accessed via FA API or SMI-S).
    - Trackd - track changes daemon
- **Port Mirroring** captures traffic between two devices for non-disruptive traffic analysis (available on the Brocade 4100, 4900, 48000, and 7500).

Management

- **Role-Based Access Control (RBAC)** adds support for the new RBAC roles: Operator, Zone Manager, Fabric Administrator, and Basic Switch Administrator.
- **Virtual fabrics through administrative domains** (Admin Domains or AD) provides data, management, and fault isolation through administrative domains.
- **DHCP support** for standalone switches.

Security

- **Device Connection Control (DCC), Switch Connection Control (SCC), and the ability to manually distribute passwords** among participating switches in the base Fabric OS.
- **Internet Protocol Security (IPSec)** ensures private, secure communications over Internet Protocol (IP) networks to prevent network-based attacks, which could potentially result in denial of service, data corruption, data theft, user credential theft, and so on. IPSec will be available as a standard license for the Brocade 7500 and FR4-18i blade in the Brocade 48000 director.

Other

- **FCR enhancements** for the Brocade 7500 and FR4-18i blade in the Brocade 48000 director:
    - **Front domain consolidation** providing one front domain per chassis projected to edge fabrics regardless of the number of EX_Ports connected from the Brocade 48000 or FR4-18i blade in the Brocade 48000 to that edge fabric.
    - **McDATA interoperability** in both McDATA Fabric and Open Fabric modes
    - **EX_Port trunking** providing high bandwidth across the router

    - **Router port cost** providing users flexibility to determine the preferred route between two destinations across a metaSAN

- **FCIP enhancements** for the Brocade 7500 and FR4-18i blade in the Brocade 48000 director:
    - **Internet Protocol Security (IPSec)** ensures private, secure communications over Internet Protocol (IP) networks to prevent network-based attacks, which could potentially result in denial of service, data corruption, data theft, user credential theft, and so on.
    - **Fastwrite** reduces the number of round-trips required to complete a SCSI Write IO, which both reduces IO completion latency and increases FCIP ISL bandwidth utilization.
    - **Tape Pipelining** accelerates SCSI Write IOs between geographically remote initiators and tape devices on Fibre Channel SANs linked via FCIP ISLs.
    - **WAN tool**, the **ipperf** option has been added to the **portCmd** command to characterize end-to-end IP path performance factors, such as bandwidth, loss rate, roundtrip time, and path MTU (Maximum Transmission Unit) between a pair of Brocade FCIP ports.
- The **tstimezone** command provides an interactive interface to select Daylight Savings Time based on the country and region.
- The **number of user accounts** is increased from 15 to 256.
- **Zoning database size** increased from 256 KB to 1 MB.
- Long distance mode simplification:
    - **LD is a dynamic distance mode** that automatically discovers lengths and assigns the correct amount of buffer credits with an Extended Fabrics license.
    - **LS is a static distance mode** that allows you to specify the number of buffer credits required with an Extended Fabrics license.
    - **LE** supports up to 10 kilometers at any speed and does not require an Extended Fabrics license.

Optionally Licensed Software

This Fabric OS release includes all basic switch and fabric support software, as well as the following optionally licensed software, which 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
- FC-IP—Fibre Channel over IP extension includes FC-IP trunking, multi-tunnel support, and compression

Licensed Software as Standard

The following licensed software is available 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 v5.2.0 adds support for the FC4-48 and FC4-16IP blades for the Brocade 48000 director. It also supports the Brocade 200E, 3250, 3850, 3900, 4100, 4900, and the Brocade 7500, 24000, and 48000, and the Brocade 5000, new with Fabric OS v5.2.1.

IMPORTANT: The Brocade 12000 is not supported in this release; defect fixes for this platform will be delivered on the Fabric OS v5.0.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. 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.

   *FT00X0054E9
   FT00X0054E9

   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, 3200, 3250, and 3850—Bottom of the chassis
   - Brocade 3800 and 3900—Non-port side of the chassis
   - Brocade 5000, Brocade 4100, 4900, and 7500—On the switch ID pull-out tab located inside the chassis on the port side on the left
   - Brocade 12000, 24000, and 48000—Inside the chassis next to the power supply bays
   - Brocade Multiprotocol Router Model AP7420—Bottom of the chassis and on the back of the chassis.

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

   - Brocade 5000, Brocade 200E, 3014, 3016, 3250, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, and 7500 switches and Brocade 12000, 24000, and 48000 directors—Provide the license ID. Use the **licenseIDShow** command to display the license ID.
   - Brocade Multiprotocol Router Model AP7420—Provide the switch WWN. Use the **switchShow** command to display the switch WWN.
   - All other Brocade switches—Provide the switch WWN. Use the **wwn** command to display the switch's WWN.

Important Notes

This section lists information 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: Brocade 2000 Series and 6400	Fabric OS v2.6.2 [1]
Switches: Brocade 3000, 3200, 3600, and 3800	Fabric OS v3.2.X
Embedded Switch: Brocade 4012	Fabric OS v5.0.0
Switches: Brocade 200E, 325x, 385x, 3900, and 4100 **Embedded Switches**: Brocade 3014, 3016, an 4012 **Directors**: Brocade 12000, 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**: Brocade 12000, 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**: Brocade 12000, 24000, and 48000 (without FR4-18i blade)	Fabric OS v5.0.4
Switches: Brocade 200E, 325x, 385x, 3900, and 4100 **Embedded Switches**: Brocade 3014, 3016, 4012, 4016, 4018, 4020, and 4024 **Directors**: Brocade 12000, 24000, and 48000 (without FR4-18i blade)	Fabric OS v5.0.5
Switches: Brocade 200E, 325x, 385x, 3900, 4100, 4900, and 7500 **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, 4900, 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]
Switches: Brocade 200E, 3014, 3016, 325x, 385x, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, Brocade 5000 and Brocade7500 **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 v5.2.1

Fabric OS Interoperability with Brocade Switches and Firmware	
Router: Brocade AP7420	XPath 7.4.x OS [2]
Fabric OS Interoperability with McDATA Switches and Firmware [2]	
Intrepid 6140 and 6064	EOS v7.x, v8.x [2]
Sphereon 3232, 4300, 4500 and 3216	EOS v7.x, v8.x [2]

(1) Fabric OS v2.6.2 can interoperate with Fabric OS v5.2.0 through the FC routing capability of the Brocade AP7420, Brocade 7500, or FR4-18i blade in the Brocade 48000 director. Customers who wish to have Fabric OS v2.6.2 and v5.2.0 mixed in the same fabric should consult their equipment provider for a detailed list of limitations. New fabric-wide features introduced in Fabric OS v5.2.0, such as Virtual Fabrics, Access Control security policy, new hardware, etc., will not be compatible with Fabric OS v2.6.2.

(2) Fabric OS and McDATA E/OS v4.x, v5.x, 6.x can interoperate through the FC routing capability of the Brocade AP7420 only. Fabric OS and McDATA E/OS v7.x, 8.x can interoperate through the FC routing capability of the Brocade AP7420, Brocade 7500, or FR4-18i blade in the Brocade 48000.

Firmware Upgrades and Downgrades

Fabric OS v5.1.1 supports a maximum MTU value of 2284. However, Fabric OS v5.2.1 and above support an MTU value of up to 2348. Prior to downgrading Fabric OS to v5.1.1, the user must change the MTU size to 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 a firmware downgrade.

Brocade does not support upgrading from more than two previous releases. For example, upgrading from Fabric OS v5.0.x to v5.2.x is supported, but upgrading from Fabric OS v4.4.0 or a previous release directly to v5.2.x is not.

Upgrading a switch from Fabric OS v4.4.0 or a previous release to v5.2.0 requires a two-step process: first upgrade to v5.0.x or v5.1.x and then upgrade to v5.2.0.

In addition, the following conditions must be met before upgrading to v5.2.0:

- 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.

Install the new blade types (FC4-16IP or FC4-48) only after you have installed the Fabric OS v5.2.0 software.

Brocade supports downgrading up to two previous releases, for example, if you upgrade to Fabric OS v5.2.0 from v5.0.x, you can revert back to v5.0.x. However, you cannot downgrade from Fabric OS v5.2.0 to v4.4.0 or to a previous release.

NOTE: If the Brocade 48000 has FC4-48 or FC4-16IP blades installed or any new software features in 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.

For any other new software features or increased scalability limits supported by Fabric OS v5.2.0, downgrade will be disruptive and requires cold reboot.

A v5.2.0 configuration file cannot be used on the same switch after the switch has been downgraded to firmware version v5.0.x or v5.1.x.

When you downgrade to Fabric OS v5.0.x, you will also need to remove additional v5.1.x features (and any installed FR4-18i blades). The firmwareDownload command will guide you to remove any features and blades that need to be removed.

Fabric Scalability

Fabric OS v5.2.0 supports the same fabric scalability as Fabric OS v5.0.x and v5.1.x, that is, 2,560 ports with 50 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 backbone fabric	5
Max # translate domains per backbone fabric	33
Max # total domains per backbone fabric	69
Max # FCR switches per metaSAN	10
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	2500 (with a v5.2.0 only FCR backbone)
Max # entries per LSAN zone	64
Max # hops between edge switches	12
Max # EX_Ports to an edge fabric from FCR	8(4G)
EX_Ports per FCR	32

FICON Support

With this release, the Switch Connection Control high integrity requirement for cascading FICON is available in the standard base Fabric OS. End users can now deploy new cascade FICON directors without purchasing a separate Secure Fabric OS license.

To add a new FICON director into existing cascaded configurations that are already running Secured Fabric OS, it is recommended that users continue to deploy Secure Fabric OS on the new FICON director instead of migrating to FOS ACL configuration.

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 to the System z environment, use an FC4-16 or FC4-32 Fibre Channel port blade**.**

Brocade PKI Certificates

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

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

RADIUS Setup

If Brocade Server blade switch models 3016, 4020 and 4024 are present in a fabric that utilizes the Remote Authentication Dial-In User Service (RADIUS) as the primary source of authentication verify that local authentication has been enabled on the Brocade 3016 and 4020. This allows each switch to take over authentication if the RADIUS servers fail to respond due to a power outage, network problems or if there is a RADIUS configuration error. Failure to have the local switch database as the secondary authentication service could result in a switch module that cannot be accessed via telnet or a web browser.

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.

Area	Description
Diagnostic Command on the Brocade 4016, 4018, and 4024	When run as a separate command from the CLI, diagclearerror might hang or cause the system to panic. This affects only the Brocade 4016, Brocade 4018, and Brocade 4024 platforms. To run diagclearerror from the CLI, first switch directories as shown here: cd /fabos/sbin diagclearerror
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	• Customers upgrading Brocade 24000 switches from Fabric OS v5.0.5 to v5.2.0 while in chassisconfig option 3 or 4 will not get sufficient notification in the session error message or firmwaredownloadstatus command about how to correct the problem. • Before moving the slider UP on a Control Processor blade that is being activated, observe that the 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.

Area	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 an FC4-32 blade with an 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 into the slot and port swap the ports back to the ports' 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 an FC4-48 port. • 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 • In a zoning configuration with members D and P, where "P" is greater than or equal to 256, remove these configurations before downgrading to a lower firmware version (5.1.x or 5.0.x). Otherwise, the downgrade will not be HA compatible with earlier versions. • Do not insert the blade until the system is running Fabric OS 5.2.0.
FC4-16IP iSCSI blade for the Brocade 48000	• iSCSI virtual target creation involves adding LUNs to the virtual targets. The user discovers the LUNs by executing the fclunquery command. Testing has revealed that some devices do not respond properly to the LUN query. The user will need to use tools from the array vendor to determine LUN information required for iSCSI target creation. • Any upper case letters used for the CHAP user name will be transformed to lower case. • Users may install up to four FC4-16IP iSCSI blades per Brocade 48000 chassis, or any combination of up to four FC4-16IP and FR4-18i blades, not to exceed two FR4-18i blades per chassis. Some valid combinations are: o three FC4-16IP blades + one FR4-18i blade o two FC4-16IP blades + two FR4-18i blades o one FC4-16IP blades + two FR4-18i blades o two FC4-16IP blades + one FR4-18i blades • Do not insert the blade until the system is running Fabric OS 5.2.0.

Area	Description
Firmware upgrade/downgrade	• When upgrading from Fabric OS v5.1.0x to v5.2.0x, if there are 2 or more inter-fabric links (IFLs) connected to an edge fabric, one IFL will stay online and the other IFLs will go offline and online. 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 new front domain consolidation feature in Fabric OS v5.2.0 where the IFLs connected to the same edge share the same front domain. • When downgrading from Fabric OS v5.2.0 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 a disabled state. If you wish to retain GE_Ports in a disabled state across afirmware download, you must configure them as persistently disabled. • In a large fabric with a large zoning database (e.g., 2560 ports with a 1MB zoning database), a non-disruptive firmwaredownload on a Brocade 3850 or 3900 can result in an E_Port offline transition. The E_Port offline transition causes a fabric reconfiguration and can cause momentary frame loss. 4 gb/s switches do not experience this issue. • FCIP traffic is disrupted in an upgrade from Fabric OS v5.2.0a to Fabric OS v5.2.0b.
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. • The QuickLoop feature and related commands (listed below) are no longer supported on Fabric OS versions v5.1.0 and higher. o qloopAdd o qloopCreate o qloopDelete o qloopRemove o qloopShow
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.

Area	Description
FC Routing	• If a Brocade AP7420 is present in the backbone fabric, the command fcrDisable may take up to 8 minutes to complete. If the AP7420 is replaced by an FR4-18i or a Brocade 7500, the command completes immediately. • EX_Port trunking is not enabled by default. • Fabric OS v5.2.0 introduces the EX_Port trunking feature. This feature should only be enabled if the entire configuration is running Fabric OS v5.2.0 or later. Enabling the EX_Port trunking feature on a switch running Fabric OS v5.2.0 or later in a configuration containing a Fabric OS v5.1.0 switch will cause the Fabric OS v5.1.0 switch to panic. • When an unstable edge fabric that has multiple EX_Port connections is in a transitional state, on rare occasions one of the EX_Ports may detect an FID conflict and be disabled. If this occurs, manually re-enable the port.
Security	Remove any password enforced expiration of admin or root accounts before downgrading firmware to Fabric OS v5.0.1 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 because they have higher link costs, 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.

Area	Description

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
	• FastWrite and Tape Pipelining will not be supported in conjunction with secure tunnels.
	• 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.
	• User is not informed with the IPSec mismatch RAS event when configuring a tunnel with IPSec mismatch on either end.

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 has 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.
FRU insertion	The FW_FRU_INSERTED message is displayed twice when a power supply FRU is inserted and powered on. There is no functional impact.

Area	Description
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 or higher.
FCIP	• Frame drops observed on FCIP slow links: o The frame drops occur when the FCIP tunnel bandwidth is set to 10 Base-T (10Mbps), E1 (1.048Mbps), or T1 (1.544Mbps). o With E1 or T1, frames are dropped even without an impaired link. o With 10 Base-T, frame drops may be observed when a low impairment is put to the link. • portperfshow indicated incorrect (smaller) bidirectional throughput on the FCIP tunnel when Fastwrite/Tape Pipelining is enabled. • Fast Write/Tape Pipelining did not inform the user when it failed due to multiple equal paths configured on 2 GbE ports. • Backup jobs initiated from the Symantec BackupExec application slowed noticeably after adding significant IO traffic from regular hosts and targets to the FCIP tunnel. A port-based routing policy must be used for Tape devices.
Access Gateway vs. Standard Switch Mode	• When using the Brocade blade server SAN switch in Access Gateway mode, most switch features are no longer applicable. These features include Admin Domains, Advanced Performance Monitoring, direct connection to SAN target devices, Fibre Channel Arbitrated Loop support, Fabric Manager, FICON, IP over FC, ISL Trunking, Extended Fabrics, Management Services, Name Services (SNS), port mirroring, Secure FOS, SMI-S, and Zoning. These switch features are available in the default switch mode of operation.
Access Gateway Mode Port State	• When a disabled port on a switch in Access Gateway mode is connected to a configured loop HBA, the port state alternates between Nosync and Insync. The switchShow command displays the state of the remote HBA port that is continuously attempting to reconnect to the disabled port. • Brocade Access Gateway only supports FCP initiator connections on the F_Ports. Note that cascading Access Gateway devices or connecting FCP targets, loop devices, or FICON channel/control units on the F_Ports is not supported.
LSAN across FCR	• If a mixed fabric is configured for LSAN across FCR, zone changes must originate from the switch running the highest Fabric OS release. For example, if a mixed fabric contains switches running Fabric OS v4.x, v5.1.x and v5.2.x, the zone changes must originate from the switch running Fabric OS v5.2.x. This is true whether or not AD is enabled.

RFEs Implemented in Fabric OS v5.2.2

None

RFEs Implemented in Fabric OS v5.2.1

RFE Number	Description
3868	Disable console magic key break sequence to avoid unintentional switch reboot/hung/panic due to user input or serial line settings.
3863	Add syslog IP addresses to Configuration upload file to allow upload/download.
3814	Log a syslog message when syslogd destination address is removed by syslogdipremove command
3797	When port speed is auto negotiated, Web Tool's ports overview shows port speed as (AN-2), (AN-4), etc. rather than just 1,2,4.
3615	Change HELP to be case insensitive.

RFEs Implemented in Fabric OS v5.2.0

RFE Number	Description
3791	Set backspace key (^H) as erase key for firmwareDownload, configUpload and configDownload commands.
2953	Provide consistency in IP administration and configuration across different features and platforms.
3142	RLIRs are sent only to listeners within the same Brocade zone.
2487	Add domain ID for each ISL in the output for clarity (islShow and trunkShow.) Previously, the port numbers were shown. Adding the domain ID helps identify the destination switch.
2537	Allow administrator to clear port counters when necessary.
3082	Add information to supportShow help file that supportShow is a diagnostic tool.
3099	Add bsn (Brocade Serial Number) in supportShow to identify switch while trouble-shooting.
3114	Add date field to logging field in the portLogDump/Show.
3152	Add "top" (CPU util output) to supportShow.
3273	Successful login message in event log should show IP address of station logging in.
3532	supportShow now includes sfpShow –all.

Fabric OS v5.2.2a Documentation

This section provides information on last-minute additions and corrections to the documentation. The most recent Fabric OS v5.2.0/v5.2.1/v5.2.2 documentation manuals are available on the Brocade Partner Network: *http://partner.brocade.com/*

AP Route Policy

On Brocade 7500 and FR4-18i, there are 8 internal physical links used by EX and VEX port functionality. The links are shared by both ingress and egress traffic on EX/VEX ports. With the introduction of FOS v5.2.2a patch, a new internal AP route policy is added to dedicate some links for ingress traffic and some links for egress traffic.

Environment

The new AP Dedicated Link Policy is to relieve internal congestion in an environment where:

- There is a large amount of traffic going through both directions at the same time
- Reducing the impact of slow devices on the overall switch performance

Brocade advises the default AP Shared Link Policy for most customer environments. It is always better to design a SAN that will localize Host to Target traffic by reducing the amount of traffic through the router.

Configure AP Policy

The following command activates the new dedicated policy:

aptpolicy –ap <AP_POLICY>

aptpolicy -ap 0 --> AP Shared Link Policy (Default)
aptpolicy -ap 1 --> AP Dedicated Link Policy

For example:
To configure AP policy, perform switchdisable, then:

switch:admin> aptpolicy -ap 1
Policy updated successfully.

The policy change is effective right away for all EX/VEX-ports after switchenable.

Notes

- A switch running AP Dedicated Link Policy, upgrade or downgrade it to a firmware level that does not support AP Dedicated Link Policy, the router would continue to operate under AP Dedicated Link Policy for all existing EX/VEX ports. Once the ports go offline/online, AP policy is switched back to AP Shared Link Policy and any new links come online would be AP Shared Link Policy.
- A switch running AP Dedicated Link Policy, upgrade or downgrade it to a firmware level with AP Dedicated Link Policy support, the running AP Dedicated Link Policy stays the same after upgrade/downgrade.

AP policy and routing policy are independent. So to have a port based policy with dedicated link policy, the “aptpolicy” command must be issued twice, as in the following example:

```
switch:admin > switchdisable
switch:admin > aptpolicy 1                  // for setting port based policy
switch:admin > aptpolicy -ap 1              // for dedicated link policy
switch:admin > switchenable
```

"aptpolicy" command shows the current policy (both the routing policy and the link shared/dedicated policy) and the default policy and the policies supported

The output format is as follows:

```
switch:admin > aptpolicy

Current Policy: 1 1(ap)

3 0(ap): Default Policy
 1: Port Based Routing Policy
 3: Exchange Based Routing Policy
    0: AP Shared Link Policy
    1: AP Dedicated Link Policy
```

Fabric OS v5.2.1 Documentation

This section provides information on the documentation for Fabric OS v5.2.1.

New Hardware Documentation

The following new manuals support the Brocade 5000:

Brocade 5000 Hardware Reference Manual
(Publication number: 53-1000424-01)
The Hardware Reference Manual is written for network administrators to provide a complete set of Brocade 5000 switch installation procedures and an overview of the switch hardware. This document is specific to the Brocade 5000 switch running Fabric OS v5.2.1.

Brocade 5000 QuickStart Guide
(Publication number: 53-1000425-01)
The QuickStart guide is intended as an overview to help experienced installers unpack, install, and configure a Brocade 5000 switch quickly. For detailed installation and configuration instructions, refer to the *Brocade 5000 Hardware Reference Manual*.

Brocade 5000 Power Supply/Fan Assembly Replacement Procedure
(Publication number: 53-1000426-01)
This document provides instructions to replace a power supply/fan assembly unit in the Brocade 5000 switch.

Brocade 5000 Rack Mounting Ears Installation Procedure
(Publication number: 53-1000451-01)
This document provides instructions to install mounting ears to the switch and install the switch in a rack with the mounting ears.

Updated Software Documentation

The Brocade Fabric OS V5.2.x manual contains important last minute updates to the Fabric OS v5.2.0 Family Documentation set as well as instructions on using the DPOD feature. Use the Software Addendum and the Fabric OS v5.2.0 documentation set for instructions on administering a Fabric OS SAN.

The most recent Fabric OS v5.2.0 documentation manuals are available on the Brocade Partner Network: http://partner.brocade.com/.

Brocade Fabric OS V5.2.X Software Addendum
(Publication number: 53-1000429-01)
The Software Addendum is written for SAN administrators to provide a complete description of the DPOD feature and important last minute changes to the Fabric OS v5.2.0 documentation manuals. This document is specific to switches running Fabric OS v5.2.1.

New Software Documentation

The following manual supports Brocade Access Gateway only. For detailed Fabric OS administration instructions, refer to the *Fabric OS V5.2.X Software Addendum* and the Fabric OS V5.2.0 Family Documentation set.

Brocade Fabric OS V5.2.1 Access Gateway Administrator's Guide
(Publication number: 53-1000430-01)
The Access Gateway Administrator's Guide is written for SAN administrators to provide a complete description of operating and managing a switch in Access Gateway mode.

Documentation Updates

This section provides information on last-minute additions and corrections to the documentation. The most recent Fabric OS v5.2.0/v5.2.1 documentation manuals are available on the Brocade Partner Network: *http://partner.brocade.com/*

Brocade 5000 Hardware Reference Manual

(Publication Number 53-1000424-01)

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 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 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”

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 4, 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.”

Closed Defects in Fabric OS v5.2.2a

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

Defects Resolved In Fabric OS v5.2.2a		
Defect ID	**Severity**	**Description**
DEFECT000076856	High	**Summary:** Brocade 7500 and FR4-18i may drop frames under high-stress bi-directional FCR traffic conditions **Symptom:** When there is a large amount of traffic going through an EX port in both directions at the same time and when there are slow devices in the fabric, traffic going through the EX port from one fabric to another fabric pauses. After some time, traffic resumes. **Solution:** Introduce a new internal AP route policy to allow ingress and egress path traffic to use dedicated physical links to avoid internal congestion. The command to invoke the new policy is: aptpolicy –ap 1 **Probability:** Low **Risk of Fix:** Medium **Reported in Release:** V5.1.0 **Service RQST#:** RQST00000052396

Closed Defects in Fabric OS v5.2.2

This section lists defects that have been closed since the last Fabric OS GA release, v5.2.1

Defects Resolved In Fabric OS v5.2.2		
Defect ID	**Severity**	**Description**
DEFECT000076709	High	**Summary:** In a dual backbone fabric with EX_Port trunking links to edge fabrics, disabling the slave port of the EX_Port trunk results in the loss of the process login. **Symptom:** Host may not be able to see targets after a port disable/enable of one the EX trunk ports. **Solution:** Switch driver was updating the EX_Port domain upon every port disable event, even if the EX_Port was a slave port. The fix avoids updating the routing information for EX slave port events. **Probability:** Medium **Risk of Fix:** Low **Reported in Release:** V5.2.0

Defects Resolved In Fabric OS v5.2.2		
Defect ID	**Severity**	**Description**
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 a lab by switching an E_Port's transmitter off and on at an interval of 35 ms. **Solution:** The fix updates the port fault counter when the link stays in an AC (active) state and there is a loss of signal. This allows a port fault to be triggered during the resource allocation time period. **Probability:** Low **Risk of Fix:** Medium **Service Request#** RQST00000053684 **Reported in Release:** V5.0.5
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 **Risk of Fix:** Low **Service Request#** RQST00000056062 **Reported in Release:** V5.0.1

Defects Resolved In Fabric OS v5.2.2		
Defect ID	**Severity**	**Description**
DEFECT000081883	High	**Summary:** In extremely rare occurrences, due to Performance Server Daemon (PSD) panic assertions, the standby CP 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 fix is to not apply the partial HA update until the entire dump is received from the active CP. **Probability:** Low **Risk of Fix:** Low **Service Request#** RQST00000056917 **Reported in Release:** V5.0.4
DEFECT000082731	High	**Summary:** Port Mirroring feature is not supported on the Brocade 5000 **Symptom:** Customer will not be able to use the port mirroring feature on the Brocade 5000 switch **Solution:** Add port-mirroring function for the Brocade 5000. **Probability:** High **Risk of Fix:** Low **Reported in Release:** V5.2.1_Ni
DEFECT000082820	High	**Summary:** Performance Server Daemon (PSD) core dumped after firmwaredownload or switchdisable in interop mode. **Symptom:** The switch panics with a (kill software daemon) kSWD of the psd. **Solution:** When interop mode was enabled, the PSD did not properly release the domain database lock. This causes the switch to panic if the remote switch is not a Fabric OS switch and does not understand the performance monitor capability. Fixed code to properly release the lock in this condition. **Probability:** High **Risk of Fix:** Low **Reported in Release:** V5.2.1_Ni

Defects Resolved In Fabric OS v5.2.2		
Defect ID	**Severity**	**Description**
DEFECT000082974	High	**Summary:** After approximately 100 days of continuous running, a memory leak during a sensor poll is seen on a Brocade 4020 (only on this platform). **Symptom:** After approximately 100 days of continuous running, the switch may run too low on memory and panic. This leak only exists on the Brocade 4020 platform. All other platforms will not observe this symptom. **Solution:** Fix memory leak during EM sensor poll on Brocade 4020. **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 **Risk of Fix:** Low **Reported in Release:** V5.3.0
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 system verification 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 **Risk of Fix:** Low **Service Request#** RQST00000058174 **Reported in Release:** V5.2.1

Defects Resolved In Fabric OS v5.2.2		
Defect ID	**Severity**	**Description**
DEFECT000084112	High	**Summary:** Brocade 7500 was placed into a faulty state during firmware upgrade and downgrade testing. This also applies to FR4-18i, which can result in blade fault. **Symptom:** When downgrading firmware from the latest unreleased version of FOS back to FOS 5.2.x, the operation is timed out and either the Brocade 7500 or the FR4-18i blade is placed into a faulty state. RASLOG: [EM-1034], 22/6,, ERROR, BB2_7500_147c, Switch set to faulty, rc=2004c, OID:0x43000000, em_board_lib.c, line: 1347, comp:emd, ltime:2007/03/16-15:20:03 **Solution:** Increase Blade Module initialization timeout from 60 to 120 seconds to allow enough time for blade to initialize before declaring time-out. **Probability:** Low **Risk of Fix:** Low **Reported in Release:** V5.2.0
DEFECT000084841	High	**Summary:** All FC4-16IP blades did not downgrade to FOS v5.2.1a during an internal future release downgrade test. **Symptom:** After a downgrade from an internal future build to FOSv5.2.1a, all FC4-16IP blades still show the internal future builds and did not get downgraded. This issue has not been seen in the field, and has only been observed on systems running with four FC4-16IP blades in the same chassis. **Solution:** Increase the rshd protocol spawning rate limit. **Risk of Fix:** Low **Reported in Release:** V5.2.1

Defects Resolved In Fabric OS v5.2.2		
Defect ID	**Severity**	**Description**
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 **Risk of Fix:** Low **Service Request#** RQST00000059349 **Reported in Release:** V5.2.1
DEFECT000085266	High	**Summary:** Configdownload for Fabric Watch parameters shows successful message from Fabric Manager, but actually download fails for non-disruptive configuration parameters such as Fabric Watch, SNMP, Syslog and Time service. **Symptom:** Download configuration parameter from Fabric Manager reports as successful, but new parameters for Fabric Watch, SNMP, etc. are not accepted and the switch continues to operate with the old configuration parameters. **Solution:** Sections of download data were deemed not applicable due to an invalid flag value. Fix the code to assign a proper default flag value. **Workaround:** Use CLI. **Probability:** Medium **Risk of Fix:** Low **Reported in Release:** V5.3.0

Defects Resolved In Fabric OS v5.2.2		
Defect ID	**Severity**	**Description**
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 **Risk of Fix:** Low **Service Request#** RQST00000059448 **Reported in Release:** V5.2.0
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

Defects Resolved In Fabric OS v5.2.2		
Defect ID	**Severity**	**Description**
DEFECT000086687	High	**Summary**: FICON CUP daemon crashes after switch comes up when it starts processing the RNID command from FICON channels. **Symptom**: Multiple threads work 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
DEFECT000087241	High	**Summary:** Hot code load time on Brocade 5000 internal stress testing comes close to the upper threshold. **Symptom:** When the time for a hot code load is over the known threshold, the result might be a disruptive upgrade. **Solution:** The fix enhances the code to reduce the HCL time, placing it a few seconds within the threshold. **Probability:** Medium **Risk of Fix:** 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. **Risk of Fix:** Low **Service Request#** RQST00000050503 **Reported in Release:** V5.0.5

Defects Resolved In Fabric OS v5.2.2		
Defect ID	**Severity**	**Description**
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. **Probability:** Medium **Risk of Fix:** Low **Service Request#** RQST00000051666 **Reported in Release:** V5.0.5
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 (portdisable/portenable) the EX_Port. **Probability:** Low **Risk of Fix:** Low **Reported in Release:** V5.2.0
DEFECT000076999	Medium	**Summary:** Proxy devices disappear from FCR after disabling the master EX_Port in a dual heterogeneous backbone fabric. **Symptom:** Proxy devices will be removed from FCR after disabling the master EX_Port. **Solution:** Clean up domain reachable information to make sure the LSAN will be updated to the remote front domain if this domain is toggled on/off quickly. **Workaround:** Do not enable EX_Port trunking or disable the master EX_Port. **Probability:** Medium **Risk of Fix:** Low **Reported in Release:** V5.2.0

Defects Resolved In Fabric OS v5.2.2		
Defect ID	**Severity**	**Description**
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 DP 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 DP zone, enable the zone config, and then re-add the D,P zone, and enable the zone config. Or Only use DP 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 **Risk of Fix:** Medium **Service Request#** RQST00000056725 **Reported in Release:** V5.2.0
DEFECT000085078	Medium	**Summary:** FCIP MIB support is needed on the Brocade 7500 and FR4-18i. **Symptom:** There is no FCIP MIB. **Solution:** MIB support has been added for the Gbit Ethernet ports. **Probability:** Low **Risk of Fix:** Low **Reported in Release:** V5.2.0
DEFECT000084839	Low	**Summary:** During high temperature testing the ports on the Brocade 4020 failed to come up. **Symptom:** There is no field impact as the parts that fail this testing are not shipped to the field. **Solution:** The fix involved changing the configuration of an on board device. **Probability:** Low **Risk of Fix:** Low **Reported in Release:** V5.2.1 **Note:** This failure will not be encountered in the field.

Closed Defects in Fabric OS v5.2.1b

This table lists the defects that have been newly closed in Fabric OS v5.2.1b.

Defects Newly Closed in Fabric OS v5.2.1b		
Defect ID	**Severity**	**Description**
DEFECT000078575	High	**Summary:** A PLOGI ACC frame is not routed to the destination virtual port when the host and target are on the same NPIV port. **Symptom:** The traffic path between the host and the target will not be established. This does not impact hosts and devices that are on different NPIV ports or fabrics not using the NPIV feature. **Solution:** Changes code to properly set up the content addressable memory (CAM) entry when the host and target are on the same NPIV port. **Probability:** Medium **Risk of Fix:** Low **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 **Risk of Fix:** Low **Service Request#** RQST00000054793 **Reported in Release:** V5.2.0

Defects Newly Closed in Fabric OS v5.2.1b		
Defect ID	**Severity**	**Description**
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 **Risk of Fix:** Low **Service Request#** RQST00000055906 **Reported in Release:** V5.2.0
DEFECT000082228	High	**Summary:** Host loses target for 15 seconds after a non-disruptive failover on an Access Gateway-enabled switch. This impacts the Brocade 4012, 4016, 4020 and 4024. **Symptom:** Any event that triggers a hareboot, such as a firmware download or a switch panic, might cause the host to temporarily lose visibility of the target on the Access Gateway port. This will interrupt the traffic. **Solution:** Relies on the FLOGI timeframe to send the port-on-line update and to properly set up the internal data structure. **Workaround:** Wait 15 seconds for traffic to resume. **Reported in Release:** Fabric OS version currently under development.
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 OSv5.2.0 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. **Service Request#** RQST00000057678 **Reported in Release:** V5.2.1

Defects Newly Closed in Fabric OS v5.2.1b		
Defect ID	**Severity**	**Description**
DEFECT000084020	High	**Summary:** Upgrading a Brocade 7500 to Fabric OS v5.2.1 on a fabric designated with Fabric ID 128 causes the host to lose the path to the target. **Symptom:** After upgrading a Brocade 7500 to Fabric OS v5.2.1, devices lose paths in the fabric. **Solution:** Fixes the routing code to correctly handle Fabric ID 128. **Workaround:** Change to a Fabric ID other than 128 and reboot the Brocade 7500 **Risk of Fix:** Low **Service Request#** RQST00000057970 **Reported in Release:** V5.2.1
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, 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 **Risk of Fix:** Medium **Service Request#** RQST00000059132 **Reported in Release:** V5.2.1

Closed Defects in Fabric OS v5.2.1a

This table lists the defects that have been newly closed in Fabric OS v5.2.1a.

Defects Newly Closed in Fabric OS v5.2.1a		
Defect ID	**Severity**	**Description**
DEFECT000081361	High	**Summary:** During iSCSI testing, luns continuously disappear from an iSCSI initiator host. **Symptom:** When a header digest error is detected by an iSCSI port, the customer may lose contact with the iSCSI sessions and the iSCSI devices. **Solution:** The code that handles the header digest error incorrectly de-allocates the TCP response buffer twice. The solution is to remove the extra de-allocation of the response buffer. **Customer Impact:** Should not occur under normal maintenance operation; represents an unlikely user scenario. **Probability:** High **Risk of Fix:** Low **Reported in Release:** V5.2.1
DEFECT000081659	High	**Summary:** During iSCSI testing, corrupt TCP payload data is used to test the data digest, and the FC4-16IP GE port crashes unexpectedly. **Symptom:** Customer may see "[ISCS-1000], 37662,, ERROR, l82c7207, Slot X Port GE crashed unexpectedly." from the console when the host detects the iSCSI digest error. **Solution:** Validates the TCP connection handle in the PDU sent by the API. Frees up buffers without sending the PDU if the TCP connection is not valid. Also changes the command timeout from 60 to 45 seconds. **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 **Risk of Fix:** Low **Service Request#** RQST00000056823 **Reported in Release:** V5.2.1

Defects Newly Closed in Fabric OS v5.2.1a		
Defect ID	**Severity**	**Description**
DEFECT000082945	High	**Summary:** During iSCSI stress testing, the host fails to see the target. **Symptom:** Under testing conditions creating heavy IO traffic, the customer may lose iSCSI connections to the targets. **Solution:** When a write command has a packet size of less than or equal to 500 bytes, the buffer reference count should be, but is not reset to 0 when the buffer is freed. The fix zeroes the reference count when the buffer is freed. **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 **Risk of Fix:** Low **Reported in Release:** V5.2.1
DEFECT000081855	Medium	**Summary:** Run from the CLI, diagclearerror causes the console to hang or the system to crash. This affects only the Brocade 4016, Brocade 4018, and Brocade 4024 platforms. **Symptom:** When run as a separate command from the CLI, diagclearerror might hang or cause the system to crash. **Solution:** Adds the proper path reference for the diagclearerror command. **Workaround:** To run diagclearerror from the CLI, first switch directories as shown here: cd /fabos/sbin diagclearerror **Customer Impact:** Should not occur under normal maintenance operation; represents an unlikely user scenario. **Probability:** High **Risk of Fix:** Low **Reported in Release:** V5.2.1