Brocade Fabric OS v5.3.0a
Release Notes v1.0

September 7, 2007

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v5.3.0a Release Notes v1.0	First release	September 7, 2007

Contents

Quick Look

If you are already using the most recent version of the Fabric OS v5.3.0 Release Notes, here is the change in this version of the Release Notes.

- The list of the defects for Fabric OS v5.3.0 is replaced at the end of these release notes by a list of the closed defects in Fabric OS v5.3.0a.

- Reference the Web Tools Documentation Addendum to the Documentation Updates section of this document

- A bulleted list of the new SNMP features that were part of the FOS v5.3.0 release have were added to New Fabric OS Features section of this documents.

- An iSCSI support table was added to Documentation Updates section of this document

- Additions were made to the known issues table in the Others section of this document. See FC4-48 and FC10-6

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

- - o Support for CHAP binding
    - o Support for LUN delete from a virtual target
- Access Gateway mode support on the Brocade 200E
- Access Gateway enhancements:
  - o Web Tools support
  - o Fabric Manager support
  - o 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
  - o Support for security Admin role
  - o Support for account lock-out for admin role.
  - o Support for strong password policies preventing repeat or sequence characters
  - o P-EAP/MS-CHAPv2 support for RADIUS
- FC-IP
  - o Fast Write and Tape Pipelining are supported over secure tunnels
  - o Differentiated Services Code Point (DSCP) markings.
- New FC Fast Write feature
- New SNMP Features
  - o SNMP AD/RBAC support
  - o 3DES and AES privacy protocol support
  - o FCIP MIB
  - o IPv6 trap destination
  - o IPv6 SNMP ACL entries.

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.

   ```
   *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, 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.
   - o 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
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]

Fabric OS Interoperability with Brocade Switches and Firmware	
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
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

Fibre Channel Routing Scalability	
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.
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 • All zones involving the shared ports (domain, port or WWN) of an FC4-48 blade would be treated as session based in "interopmode 2" fabric configuration.

Areas	Description
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. • In rare instances POST/Systemverification failures have been observed on the FC10-6.
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.
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.

Areas	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
	
	• 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.
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.

Areas	Description
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 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.
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.

Areas	Description
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.
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.

RFEs Implemented in Fabric OS v5.3.0

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 Fabric OS v5.3.0

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
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.

Web Tools Documentation Addendum
(Publication Number 53-1000791-01)

This document describes how to set up Fibre Channel over Internet Protocol (FCIP) Tunneling Service through Web Tools. It provides information for:

·   Understanding the FCIP tunneling service
·   Configuring an FCIP interswitch/interfabric link
·   Managing the FCIP tunneling service

iSCSI Administrator's Guide
(Publication Number 53-1000440-01)

The table shown below is missing from the iSCSI Administrator's Guide. It lists the iSCSI support within FOS v5.3.0

Item	Description
iSCSI Initiator Driver Versions	• Windows • MS iSCSI initiator 2.02 and 2.03 • Linux • RH EL 4 Default Initiator • 2.6.10 – 4.0.2 ISCSI initiator (SourceForge,net Initiator) • 2.4.20 – 3.6.2 ISCSI initiator (SourceForge,net Initiator) • SUSE 9 and 10 • Solaris • iSCSI is built-in to 5.11 with the latest Solaris Express release 08/06 • AIX • iSCSI is built-in to the 5..3 ML4 • HP-UX • 11iv1 – B.11.23.03e • 11iv2 – B.11.23.03e
NIC/TOE Cards	• iSCSI HBAs • Alacritech SES2002XT • Qlogic 4050c

Closed Defects in Fabric OS v5.3.0a

This section lists defects that have been closed since the GA release of Fabric OS v5.3.0.

Defect ID	Technical Severity	Description of Closed Defects in Fabric OS v5.3.0a
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. Solution: Made single sequence frame processing logic robust so that the Fibre channel IU (information unit) is not freed prematurely before it is fully processed. Workaround: Upgrade SAS application firmware. Probability: Low Reported in Release: v5.2.0 Service Request#: RQST00000059419
DEFECT000085775	High	Summary: A Diag failure and a FA4-18 fault were observed after continuously running a CP failover test overnight Symptom: Diag failure caused FA4-18 to report a fault. Solution: Removed EBM reinitialization for framer path test. Updated error handling in Anzio driver when link goes down in link up state. Workaround: Use slotpoweroff and slotpoweron commands to cycle power on the blade Probability: Low Reported in Release: v5.3.0

Defect ID	Technical Severity	Description of Closed Defects in Fabric OS v5.3.0a
DEFECT000085977	High	Summary: Panic occurs on Brocade 24000 when running MS commands GPT/GPPN/GPS/GAPNL continuously
		Symptom: Switch will panic occasionally with the following message.
		2007/04/05-21:22:16, [KSWD-1003], 20, FFDC, WARNING, SilkWorm24000, kSWD: Detected unexpected termination of: "[3]msd:0'RfP=657,RgP=657,DfP=0,died=1,rt=12770144,dt=41800, to=50000,aJc=12718644,aJp=12702043,abiJc=1616326908,abiJp=1 616310308,aSeq=767,kSeq=0,kJc=0,kJp=0
		Solution: Fixed the race condition that existed between two threads within management server that would cause IU (Information Unit) corruption while processing GPT/GPPN/GPS/GAPNL commands.
		Probability: Low
		Reported in Release: v5.2.0
		Service Request#: RQST00000059963
DEFECT000202083	High	Summary: Brocade 4900 constantly rebooting in third-party lab.
		Symptom: Name Server crashes. Supportsave shows: "File :/core_files/panic/core.pd1184614039 SECTION:CONSOLE_LOG.
		Solution: The logic that handles device login and logout in the Name Server is made robust to gracefully handle such rare conditions.
		Probability: Medium
		Reported in Release: v5.3.0
		Service Request #: RQST00000063537
DEFECT000202198	High	Summary: Brocade 5000 running FOS v5.3x rejects GID_FT command from an HBA with an "FC4-type not registered"
		Symptom: The HBA driver will see its GID_FT query being rejected even if it has previously registered with NS using RFT_ID
		Solution: Modified NS module to properly handle the NS requests that can come in any order
		Probability: Low
		Reported in Release: v5.3.0
		Service Request#: RQST00000063843

Defect ID	Technical Severity	Description of Closed Defects in Fabric OS v5.3.0a
DEFECT000203000	High	Summary: FCIP configuration functionality should be restored in FOS 5.3.x WT. Symptom: Unable to configure FCIP tunnels using Web Tools Solution: Added FCIP wizard and stand-alone tab support for near end tunnel configuration. Probability: High Reported in Release: v5.3.0
DEFECT000203383	High	Summary: GA_NXT returns VI PID and PWWN in FR mode Symptom: In frame redirect mode, the GA_NXT query from initiator returns the VI PID and PWWN instead of host PWWN Solution: Fixed GA_NXT processing logic in Frame redirect mode Probability: Low Reported in Release: v5.3.0
DEFECT000203438	High	Summary: GPN_NN returns VI PID and PWWN in FR mode Symptom: If frame redirect mdoe is enabled the response for GPN_NN query returns VI PWWN and PID instead of initiator PWWN and PID. Solution: Added translation from PWWN to PID for remote devices in the GPN_NN query logic in Frame Re-direction mode. Probability: Medium Reported in Release: v5.3.0
DEFECT000204440	High	Summary: Memory leak in scpd during NS queries Symptom: CP reboots after running for 3 days. Solution: Fixed the memory leak issue in NS API/library that was causing scpd to crash eventually. Probability: Medium Reported in Release: v5.3.0

Defect ID	Technical Severity	Description of Closed Defects in Fabric OS v5.3.0a
DEFECT000087182	Medium	Summary: Open Mode: Zone enforcement does not succeed on 48K with WWN Zoning Symptom: In Open mode, when F-Ports are connected to ports 16-47 on the FC4-48 blade with WWN zoning, the Zone enforcement shows as SESSION BASED and the "portcamshow" command displays mis-leading information. Solution: Fixed zone enforcement logic for shared ports in open mode. Probability: Medium Reported in Release: v5.3.0