Brocade Fabric OS v5.2.0b

Release Notes v1.0

January 19, 2007

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v5.2.0b Release Notes v1.0	First Release	January 19, 2007

Contents

Quick Look

If you are already using the most recent version of the Fabric OS v5.2.0a Release Notes, here is a list of the changes in this Fabric OS v5.2.0b version of the Release Notes.

- References to SANmark compliance removed from the Standards Compliance section on page 6.
- A correction on the "Max # EX_Ports to an edge fabric from FCR" in the Fibre Channel Routing Scalability table on page 10.
- Two new bullets at the end of the Important Note on Firmware Upgrade/Downgrade (page 13).
- Three new entries at the end of the Documentation Updates section, one for the iSCSI Gateway Service Administrator's Guide, another for the Fabric OS Administrator's Guide, and another for the Fabric OS Command Reference. (pages 18-19).
- A list of the Fabric OS v5.2.0b closed defects at the end of this document (page 20).

Overview

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

- The **FC4-48** port blade offers 48 1-, 2-, and 4-Gbit/sec Fibre Channel ports for the SilkWorm 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 SilkWorm 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 v5.2.0 supercedes Fabric OS v5.1.0. All users are strongly encouraged to upgrade to v5.2.0 as soon as they have access to it.

NOTE: Install Fabric OS v5.2.0 software *before you install the new blade types (FC4-16IP or FC4-48).*

New Features

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
  - Evmd - event monitor 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 SilkWorm 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 SilkWorm 7500 and FR4-18i blade in the SilkWorm 48000 director.

Other

- **FCR enhancements** for the SilkWorm 7500 and FR4-18i blade in the SilkWorm 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 SilkWorm 48000 or FR4-18i blade in the SilkWorm 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 SilkWorm 7500 and FR4-18i blade in the SilkWorm 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 SilkWorm 7500 and FR4-18i blade in the SilkWorm 48000)

Supported Switches

Fabric OS v5.2.0 adds support for the FC4-48 and FC4-16IP blades for the SilkWorm 48000 director. It also supports the SilkWorm 200E, 3250, 3850, 3900, 4100, 4900, 7500, 24000, and 48000.

IMPORTANT: The SilkWorm 12000 and embedded switch modules SilkWorm 3014, 3016, 4012, 4016, 4018, 4020, and 4024 are not supported in this release; defect fixes for these platforms will be delivered in Fabric OS v5.0.x releases.

Standards Compliance

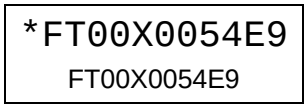
This software conforms to the Fibre Channel Standards in a manner consistent with accepted engineering practices and procedures. In certain cases, Brocade might add proprietary supplemental functions to those specified in the standards. For a list of standards conformance, visit the following Brocade 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.

   The serial number label is located as follows:

   - SilkWorm 3014—Top of the chassis, under the insertion arm
   - SilkWorm 3016, 4012, and 4024 —Bottom of the switch module
   - SilkWorm 4016 and 4018— Top of the switch module
   - SilkWorm 4020—Side of the switch module
   - SilkWorm 200E, 3200, 3250, and 3850—Bottom of the chassis
   - SilkWorm 3800 and 3900—Nonport side of the chassis
   - SilkWorm 4100, 4900, and 7500—On the switch ID pull-out tab located inside the chassis on the port side on the left
   - SilkWorm 12000, 24000, and 48000—Inside the chassis next to the power supply bays
   - SilkWorm Multiprotocol Router Model AP7420—Bottom of the chassis and on the back of the chassis.
3. **World Wide Name (WWN)**
   - SilkWorm 200E, 3014, 3016, 3250, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, and 7500 switches and SilkWorm 12000, 24000, and 48000 directors—Provide the license ID. Use the **licenseIDShow** command to display the license ID.
   - SilkWorm Multiprotocol Router Model AP7420—Provide the switch WWN. Use the **switchShow** command to display the switch WWN.
   - All other SilkWorm switches—Provide the switch WWN. Use the **wwn** command to display the switch WWN.

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: SilkWorm 2000 Series and 6400	Fabric OS v2.6.2 [1]
Switches: SilkWorm 3000, 3200, 3600, and 3800	Fabric OS v3.2.X
Embedded Switch: SilkWorm 4012	Fabric OS v5.0.0
Switches: SilkWorm 200E, 325x, 385x, 3900, and 4100 **Embedded Switches**: SilkWorm 3014, 3016, an 4012 **Directors**: SilkWorm 12000, 24000, and 48000 (without FR4-18i blade)	Fabric OS v5.0.1
Embedded Switch: SilkWorm 4020	Fabric OS v5.0.2
Switches: SilkWorm 200E, 325x, 385x, 3900, and 4100 **Embedded Switches**: SilkWorm 3014, 3016, 4012, and 4020 **Directors**: SilkWorm 12000, 24000, 48000 (without FR4-18i blade)	Fabric OS v5.0.3
Switches: SilkWorm 200E, 325x, 385x, 3900, and 4100 **Embedded Switches**: SilkWorm 3014, 3016, 4012, 4016, and 4020 **Directors**: SilkWorm 12000, 24000, and 48000 (without FR4-18i blade)	Fabric OS v5.0.4
Switches: SilkWorm 200E, 325x, 385x, 3900, and 4100 **Embedded Switches**: SilkWorm 3014, 3016, 4012, 4016, 4018, 4020, and 4024 **Directors**: SilkWorm 12000, 24000, and 48000 (without FR4-18i blade)	Fabric OS v5.0.5
Switches: SilkWorm 200E, 325x, 385x, 3900, 4100, 4900, and 7500 **Directors**: SilkWorm 24000 and 48000 (with or without FR4-18i blade) **Router**: SilkWorm 7500	Fabric OS v5.1.0
Switches: SilkWorm 200E, 325x, 385x, 3900, 4100, 4900, and 7500 **Directors**: SilkWorm 24000 and SilkWorm 48000 (any combination of FC4-16, FC4-32, FC4-48, FC4-16IP, and FR4-18i blades) **Router**: SilkWorm 7500	Fabric OS v5.2.0 [1]
Router: SilkWorm 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 SilkWorm AP7420, SilkWorm 7500, or FR4-18i blade in the SilkWorm 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 SilkWorm AP7420 only. Fabric OS and McDATA E/OS v7.x, 8.x can interoperate through the FC routing capability of the SilkWorm AP7420, SilkWorm 7500, or FR4-18i blade in the SilkWorm 48000.

Firmware Upgrades and Downgrades

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 SilkWorm 48000; see the "SilkWorm 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 SilkWorm 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 SilkWorm 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.

Fabric OS

Diagnostics backport test

The backport test passes only in a) a pure SilkWorm 24000 director or b) a SilkWorm 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 SilkWorm 24000 director (only CP2 and FC-16 blades)
- Pure SilkWorm 48000 director, option 5
- Pure SilkWorm 48000 director, option 5 (with FC4-16 blades)

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

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

"Pure SilkWorm 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
SilkWorm 7500	Silkworm 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.
SilkWorm 48000	• Customers upgrading SilkWorm 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 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 SilkWorm 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 SilkWorm 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 the 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. • 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 SilkWorm 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.

Area	Description
FC4-16IP iSCSI blade for the SilkWorm 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 SilkWorm 48000 chassis, or any combination of up to four blades of FC4-16IP and FR4-18i, 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.
Firmware upgrade/downgrade	• When upgrading from Fabric OS v5.1.0x to v5.2.0x, if there are 2 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 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 disabled state. If you wish to retain GE_Ports in a disabled state across firmware 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 SilkWorm 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.

Area	Description
Fabric OS – CLI commands	• This release does not support underscore (_) as part of the name for dd and ddset in the **iscsicfg** command. • The **slotOff** and **slowOn** commands are now obsolete; use **slotPowerOff** and **slotPowerOn** instead. The **portLogPortShow** command is also now obsolete. • 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.
FC Routing	• If a SilkWorm AP7420 is present in the backbone fabric, the command fcrDisable may take up to 8 minutes to complete. If the AP7420 is replaced by a FR4-18i or a SilkWorm 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 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 occasion 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 5.0.1 or lower versions.
Diagnostics	• All offline diagnostics commands should be used only when the switch is disabled. • POST can fail if new SFPs are added during POST. SFPs should only be added while the switch is "online" or if the switch is powered off. • When you use the diagnostic commands systemVerification and diagSetBurnin, the switch or blade will fault when the burn-in error log is full. Clear the burn-in log before running systemVerification or diagSetBurnin. • If there are ISLs present on the switch that are not used for routing because they have 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.

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 ends.

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.
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.

Area	Description
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.
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. • Fastwrite/Tape Pipelining did not inform 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. Port-based routing policy must be used for Tape devices.

RFEs Implemented in This Release

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 is sent only to listeners within 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.

Documentation Updates

This section provides information on last-minute additions and corrections to the documentation. The most recent Fabric OS V5.2.0 documentation manuals are available on the Brocade Partner Network: *http://partner.brocade.com/*

Fabric OS v5.2.0 Command Reference (Publication number: 53_1000240_01)

The **auditShow** command is deprecated in this release. Remove the command and any references to it. Note that equivalent functionality is available using the **auditcfg –show** command.

The **slTest** command is supported only on SilkWorm 200E, 4012, 4100, and 48000 platforms. Note that the SilkWorm 4900 is not supported.

Silkworm 200E Hardware Reference Manual (Publication number: 53-1000633-02)

On page A-1, in Table A-1, SilkWorm 200E, replace the "n/a" listed for the 2-Gbit/sec and 4-Gbit/sec, 9µ long wavelength with "10 km (6.2 mi)". In the same table for the 4-Gbit/sec replace the cable 62.9 µ with 62.5 µ.

Fabric OS Administrator's Guide (Publication Number 53-1000239-01)

On page 4-6, Table 4-6, Port Information: The port number for TCP NTP should be 123 (not 37).
On the Section II page, delete the last bulleted item, a reference to Chapter 22. This chapter is now in a standalone document, entitled, "iSCSI Gateway Service Administrator's Guide."

iSCSI Gateway Service Administrator's Guide
(Publication number 53-1000412-01)
A new manual has been added in this release, the iSCSI Gateway Service Administrator's Guide (Publication number 53-1000412-01). This document is designed to instruct SAN administrators in how to configure and manage the iSCSI gateway service provided by the FC4-16IP blade in the SilkWorm 48000 director.

On page A-1, replace Table A-1 with the following table:

Table A-1: iSCSI target gateway scalability guidelines

Object	Maximum
# iSCSI sessions per port	64
# iSCSI ports per FC4-16IP blade	8
# iSCSI blades in a switch	4
# iSCSI sessions per FC4-16IP blade	512
# iSCSI connections per switch	1024
# TCP connections per switch	1024
# TCP connections per iSCSI session	2
# iSCSI sessions per fabric	4096
# TCP connections per fabric	4096
# iSCSI targets per fabric	4096
# CHAP entries per fabric	4096
# LUNs per iSCSI target	256
# Members per discovery domain	64
# Discovery domains per discovery domain set	4096
# Discovery domain sets	4

iSCSI Gateway Service Administrator's Guide
(Publication number 53-1000412-01)
On page 3-3, add the following sentence to the note:
The **fcLunQuery** command only gets addresses from targets that support the **ReportLuns** command.

Fabric OS Administrator's Guide
(Publication Number 53-1000239-01)
On page 2-34, remove the row the Evmd row (shown below) from Table 2-3 List of Daemons That are Automatically Restarted. Evmd is not restarted on failure.

Evmd	Event Monitor Daemon (Port and Switch SCNs, firmwareDownload, configDownload)

On page 3-15, replace the second paragraph in Setting the Password History Policy with the following paragraph:
.
You specify the number of past password values that are disallowed when setting a new password. Allowable password history values range between 1 and 24. The default value is 1, which means ***both the current password***

cannot be reused. The value 2 indicates that ***the current and two previous passwords*** cannot be used (and so on, up to 24 passwords).

Fabric OS v5.2.0 Command Reference (Publication number: 53_1000240_01)

On page 2-317, the **isnscCfg** command also displays the operational status. Replace the description of the show option with the following:

--**show** Displays the current iSNS client configuration and operational status of the peering.

Replace the third example with the following:

To display the current configuration and operational status of the iSNS client daemon

```
switch:admin> isnsccfg --show
iSNS client is peering with iSNS server 192.168.131.124 on slot 7, port ge0
Operational Status: Not connected to iSNS server.
```

Closed Defects in Fabric OS v5.2.0b

This table lists the defects that have been newly closed in this version of Fabric OS.

Defects Closed in Fabric OS v5.2.0b		
Defect ID	**Severity**	**Details**
DEFECT000075126	High	Summary: During slotpoweroff/slotpoweron CLI test, an error message is displayed, then an FC4-16IP blade slot is faulted. Symptom: Error message: "boot failure faulting blade.." and an FC4-16IP blade generates a faulty (21). Solution: The change applies to the FC4-16IP blade, to set the boot_status register to BS_LOAD_OS (0xB0) only after successfully loading and validating the kernel image from CF. Probability: Low Risk of Fix: Low Reported in Release: V5.2.0
DEFECT000075449	High	Summary: Switch panic or CP failover when a kernel process is spawned by a non-root user. Symptom: "free_uid()" is on the console log backtrace. This problem applies to all platforms. Solution: Applies a Linux kernel patch to allow correct tracking of the root process. Probability: Low Risk of Fix: Low Service Request# RQST00000051415 Reported in Release: V5.0.3
DEFECT000076560	High	Summary: Error message displayed after upgrading the firmware on a local SilkWorm 48000 and the FR4-18i blade in the SilkWorm 48000 on the remote side of an FCIP tunnel is faulted. Symptom: Error message: "CP-4350 heartbeat dead" and FR4-18i blade generates faulty (21) message. Solution: Increased delay from 2 to 4 seconds between the blade daemon and an IPSEC daemon. Probability: Medium Risk of Fix: Low Reported in Release: V5.2.0

Defects Closed in Fabric OS v5.2.0b		
Defect ID	**Severity**	**Details**
DEFECT000076639	High	Summary: ISCSI: FC4-16IP blade running 1024 sessions stops responding after running for three days Symptom: An FC4-16IP blade stopped responding to commands after running stress-test traffic for three days. Solution: Fixes enforcement API to free memory for each target in the target list returned by DB when DDSET is enabled. Probability: Medium Risk of Fix: Low Reported in Release: V5.2.0
DEFECT000076688	High	Summary: ISCSI: unable to disable iSNS after peering with iSNS server Symptom: The error "An outstanding transaction on switch" is reported when disabling the iSNS client with the command fosconfig --disable isnsc. Solution: When any DD/DDSet operation fails, it may leave an outstanding transaction that was started by the iSNS client. The fix is to abort any outstanding transaction when any DD/DDSet operation fails. Workaround: Step One: display the outstanding transaction: iscsicfg --show transaction Step Two: abort transaction that is displayed in Step 1 above: iscsicfg --abort transaction -x <transaction id> Probability: Medium Risk of Fix: Low Reported in Release: V5.2.0
DEFECT000076747	High	Summary: ISCSI: host loses target with any IO when port is set to Error Recovery Level 2 (ERL2), digests enabled. Symptom: When port configuration is set to ERL2 with digests enabled, the host loses its targets. Solution: Write data was sent to the target before the digest calculation ended, creating buffer pointer mismatch. The fix disables digest when immediate data is enabled. Workaround: From initiators, reconnect to targets. Probability: Low Risk of Fix: Low Reported in Release: V5.2.0

Defects Closed in Fabric OS v5.2.0b		
Defect ID	**Severity**	**Details**
DEFECT000077099	High	Summary: Using the tape pipelining feature, accessing data spanning on a 1Gb tape library causes the backup application to remain stuck in running state. Symptom: Using the tape pipelining feature, backing up a set of data whose size is larger than the available space on a tape may cause the backup application to get stuck in the running state. This was observed with a 1Gb tape library; however, the faster 2Gb tape library successfully spans the data across two tapes. Solution: The fix checks for an early end of medium status and pauses the tape pipelining operation until it encounters the write file marker. Probability: Medium Risk of Fix: Low Reported in Release: V5.2.0
DEFECT000077274	High	Summary: CUP Port fails to come online on a SilkWorm 7500 due to F-Rej to PLOGI to the CUP Port Symptom: CUP Port fails to come online on a SilkWorm 7500 in a FICON environment Solution: Path to embedded destination for CUP Port was missing. This was because the policy on the embedded destination node was being set to (int: dev-based, ext: port-based), forcing the path calculation to use the virtual graph. This was because the original requested policy for the destination node (int: none, ext: port-based) was missing from the supported policy capabilities for the SilkWorm 7500 platform. Adding this combination as one of the supported policies solved the problem. Probability: Medium Risk of Fix: Low Reported in Release: V5.2.0
DEFECT000077317	High	Summary: When using the SMIAgent to connect to a switch in a larger fabric containing more than 383 FDMI devices, the LoginAsUser fails and switch panics. Symptom: The switch will either reboot or HA failover depending on the platform type. Solution: The fix is to prevent a buffer overflow in an FDMI interface function. The buffer overflow corrupts the header of the following malloc'd buffer. This results in a core dump when the second buffer is freed. This problem will happen only when there are more than 383 FDMI HBA entries in the fabric. Probability: Medium Risk of Fix: Low Reported in Release: V5.2.0

Defects Closed in Fabric OS v5.2.0b		
Defect ID	**Severity**	**Details**
DEFECT000077478	High	Summary: Linux 2.6 iSCSI initiator is not able to discover a third-party storage array. Symptom: The initiator was disconnecting the session and reconnecting. Any target which sends out sense data (sense len % 4 == 0) will experience the problem. Solution: Add pad bytes to the response PDU to ensure it is word aligned. Probability: Medium Risk of Fix: Low Reported in Release: V5.2.0
DEFECT000077479	High	Summary: iSCSI: Cannot fail back after performing a Path Failover with certain third-party multi-pathing software. It works with iSCSI GE ports, but not on FC. Symptom: Disruption in LAN: - Host logs in again to the target after every time2wait value (20 seconds). Disruption in SAN: - There is no disruption, as the virtual target is marked offline. Solution: Return "target is not currently operational" after a normal login to a VT that is in an offline state so the initiator can retry the login. Workaround: Log in again to the target when it comes back online. Probability: High Risk of Fix: Low Reported in Release: V5.2.0
DEFECT000078296	High	Summary: Registration to a storage array by a specific third party storage management agent fails with CRC error on the FC side. Symptom: Registration to array fails, preventing the host from discovering its devices in the storage group. Solution: This happens when write data is not 4-byte aligned. The fill bytes are added to the FC header, but total number of bytes to send does not include the fill bytes. This leads to CRC error detected on the FC side. The fix is to include fill bytes in total number of bytes to send to FC target. Probability: Medium Risk of Fix: Low Service Request# RQST00000054696 Reported in Release: V5.2.0

Defects Closed in Fabric OS v5.2.0b		
Defect ID	**Severity**	**Details**
DEFECT000078298	High	Summary: Third-party storage array adapter disengages when running I/O between iSCSI host and certain third-party storage array via FC4-16IP (iSCSI to FC bridge) with iSCSI Header and Data Digest enabled Symptom: Array changes into DD (Dead Director) mode when running IO with header/data digest enabled. Solution: Copy packets from iSCSI initiator to the previous buffer if it has room and send to FC target with minimum of 512 byte in each frame. Workaround: Disable header/data digest. Probability: Medium Risk of Fix: Low Service Request# RQST00000054700 Reported in Release: V5.2.0
DEFECT000078988	High	Summary: iSCSI traffic through an FC4-16IP blade has low throughput between iSCSI initiator and certain third-party storage array. Symptom: iSCSI traffic through an FC4-16IP blade has noticeably low throughput. Solution: When sending write data to FC target, check and only send minimum of 2KB or remain bytes of the Xfer Ready. Workaround: Disable immediate data. Probability: Low Risk of Fix: Low Service Request# RQST00000055325 Reported in Release: V5.2.0

Defects Closed in Fabric OS v5.2.0b		
Defect ID	**Severity**	**Details**
DEFECT000076656	Medium	Summary: If the domain ID of a switch changes, iSCSI initiators may not be able to access targets due to the Name Server database containing stale iSCSI host information. Symptom: iSCSI initiators not able to access targets. Solution: Switch driver F-port LOGO processing assumes the local Domain ID to be defined by the configured Domain ID. The fix is to remove this assumption and derive the pertinent PID from the SID of the LOGO frame. Notify Nameserver of the Virtual Initiator logout with UPDSCN_DEL_AREA rather than UPDSCN_UPD_AREA since the latter is not subject to synchronization problems. Workaround: Avoid domain ID changes. Probability: Low Risk of Fix: Low Reported in Release: V5.2.0
DEFECT000076685	Medium	Summary: ISCSI: a command does not exist to report current iSNS status Symptom: A command is needed to report to the user the current iSNS status. Solution: As a part of isnsccfg --show also display whether current operational status is connected to the iSNS server or not. Probability: Medium Risk of Fix: Low Reported in Release: V5.2.0
DEFECT000076696	Medium	Summary: On a SilkWorm 48000, the rtedebug cli returns error: "REASON: ROUTE_ABSENT" for a device connected to FC4-48 port blade. Symptom: Following lengthy stress tests that included, but were not restricted to, setting the switch speed to 1, 2, 4, switchdisable, switchenable, and disabling and enabling trunking on the switch, users may see ROUTE_ABSENT for a device connected to an FC4-48 port blade when user issues an internal routing debug CLI (rtedebug) to verify the routing paths. Solution: During E_Port master change, the loopback route for the E_Port on an FC4-48 share port is added automatically, which is prohibited behavior for the FC4-48 shared E_Ports. The fix is to not allow this. Probability: Low Risk of Fix: Low Reported in Release: V5.2.0

Defects Closed in Fabric OS v5.2.0b		
Defect ID	**Severity**	**Details**
DEFECT000076727	Medium	Summary: After extended stress testing with repeated slotpoweroff/on on two FC4-16IP blades, ICPD stopped by kSWD and switch CP failed over. Symptom: Performance server may crash if slotpoweron, slotpoweroff is issued continuously for over 11 hours on a switch containing an FC4-16IP blade. Solution: This fix will address the memory leak in PS when PS receives ROUTE_CHANGE SCN. If it fails to get the list of domains reachable, the previously allocated memory is not getting released. This causes approximately a 12K memory leak during slotpoweroff/slotpoweron tests. Probability: Low Risk of Fix: Low Reported in Release: V5.2.0
DEFECT000077512	Medium	Summary: SupportSave fails with illegal Option -s saving CORE_FFDC Symptom: Supportsave prints out error messages and fails to collect core file and FFDC data. Solution: Rescan switchname and remove none digital, alphabetical,- and _ characters before applying the switchname to savecore command. In addition, included fabric data distribution parameters in supportShow/Save. Workaround: Change the switch name to exclude space characters. Customer Impact: Usability issue, with no impact to functionality. Probability: Low Risk of Fix: Low Reported in Release: V5.2.0

Defects Closed in Fabric OS v5.2.0b		
Defect ID	**Severity**	**Details**
DEFECT000077616	Medium	Summary: Ports 32-47 on an FC4-48 port blade come up as G-ports for certain third-party storage arrays. Symptom: An HBA that sends a previously assigned PID in the SID of the FLOGI on ports 32 - 47 on the FC4-48 port blade will come up as a G-port. Solution: The FC driver was masking out the arbitrated loop physical access (ALPA) when an F-port received an FLOGI with SID already assigned. Fix was not to mask out the ALPA and leave the ALPA base bit, which is 0x80 in this case. Workaround: Use ports 0 - 31 on the FC4-48 blade as a workaround if the HBA uses previously assigned PID in the SID of the FLOGI. Probability: Medium Risk of Fix: Low Service Request# RQST00000053630 Reported in Release: V5.2.0
DEFECT000078465	Medium	Summary: Some operations initiated from Fabric Manager, Web Tools, and/or SMI-A will fail if the system switch is running Fabric OS v5.2.0a for more than 30 days.. Symptom: All common access layer (CAL) based asynchronous operations initiated from Fabric Manager. Web Tools and SMI interfaces will fail in this situation. Fabric Manager operations that fail include: SupportSave, TraceRoute, & FICON Setup/Merge wizards. SMI operations that fail includes ACL configuration. Web Tools operations that fail include all configuration related functions for AD, ACL and iSCSI. Solution: The fix prevents the generation of invalid transaction IDs. Workaround: Reboot the switch or run the operation from the CLI rather than the management tool. Risk of Fix: Low Reported in Release: V5.2.0

Closed Defects in Fabric OS v5.2.0a

This table lists the defects that have been newly closed in this version of Fabric OS.

Defects Closed in Fabric OS v5.2.0a		
Defect ID	**Severity**	**Details**
DEFECT000076589	High	Summary: Running a script that is repeatedly adding and removing LSAN zone failed when LSAN zone added to edge fabric zoning configuration does not propagate to both FCRs. Symptom: LSAN zones not equal across multiple FCRs (SilkWorm 7500 or SilkWorm 48000 with an FR4-18i blade) in backbone. Devices not imported as expected. Customer Impact: Should not occur under normal maintenance operation; represents an unlikely user scenario. Probability: Medium Reported in Release: v5.2.0