Brocade Fabric OS v6.3.0c
Release Notes v1.0

December 18, 2009

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v6.3.0c Release Notes v1.0	Initial release	December 18, 2009

Contents

Quick Look

If you are already using the most recent version of the Fabric OS v6.3.0b Release Notes, the following are the significant changes in this version:

- The table at the end of these notes contains a list of the additional defects closed with Fabric OS v6.3.0c since the release of Fabric OS v6.3.0b.

- Added additional information to the *Encryption Behavior* section of the *Important Notes*.

Overview

Brocade Fabric OS v6.3.0 supports the following new hardware platforms:

- **Brocade FX8-24: Next Generation distance extension blade for the DCX and DCX-4S**
    - Supports 12 FC ports operating at 1/2/4/8 Gbps, 10 x 1GbE ports and 2 x 10 GbE ports. (GbE ports require 4 GB Brocade branded SFPs and 10GbE ports require 10GbE Brocade branded SFPs).

- **Brocade 7800: Next Generation distance extension platform for FCIP applications**
    - Supports 16 FC ports at 1/2/4/8 Gbps and 6 x 1GbE optical ports (user can select either copper or optical interface on 2 ports). (GbE ports require 4 GB Brocade branded SFPs and 10GbE ports require 10GbE Brocade branded SFPs).

- **Brocade FCOE10-24: FCoE/CEE blade for the DCX and DCX-4S**
    - Supports 24 10GbE CEE ports

- **Brocade 8000: FCoE/CEE switch**
    - Supports 24 10GbE CEE ports and eight 1/2/4/8 Gbps FC ports
    - Initially supported by FOS v6.1.2_CEE, the Brocade 8000 is now supported as part of the FOS v6.3 release.

In addition to support for the new hardware platforms and blades, there are several new features in Fabric OS v6.3.0, including:

- **FCIP Enhancements**
    - FCIP Enhancements including enhanced compression, FCIP trunking and adaptive rate limiting features for new extension platforms.

        Note: these features are only enabled on the new Brocade 7800 Extension Switch and the FX8-24 DCX Extension Blade platforms. They are not available on the Brocade 7500 Extension Switch or the Brocade FR4-18i Extension Blade.

- **FCR Enhancements**
    - EX_Port Masterless Trunking
    - EX_Port QoS

- **Adaptive Networking Enhancements**
    - Bottleneck Detection for F_Ports (does not require Adaptive Networking license)
    - QoS support for D,I zone definitions in addition to WWN zone definitions

- **Access Gateway Features/Enhancements**
  - Adaptive Networking license supported on switches running in AG mode
  - Extend APC Auto Rebalancing support to port groups (login balancing can optionally be enabled on individual port groups)
  - Added option to disable Auto Rebalancing of logins when new N_Ports are detected
  - Added option to disable Auto Rebalancing of logins when fewer F_Ports are detected
  - Added optional support for persistent ALPA assignment
  - APC now auto-detects connection to M-series switch as N_Port connection

- **Encryption Platform Enhancements**
  - System Card support
  - Quorum card support for multi admin-based authorization of sensitive operations
  - Thales Encryption Manager for Storage key management support
  - HP tape encryption support
  - Brocade Encryption Switch support for Cisco fabric connectivity using NPIV mode
  - Support for multipath through a single EE (encryption engine)
  - Support for Host Clustering Applications and VMware ESX Server
  - Key vault Credentials support for SKM
  - HA clustered key vault support for:
    - NetApp LKM Appliances
    - HP SKM Appliances
    - EMC/RSA RKM Appliances

- **FICON Enhancements**
  - Blade-based port swaps

- **Native Connectivity Enhancements**
  - Support layer2 connectivity to M-EOSn 239 DID Open Fabric Mode fabrics
  - Support layer2 connectivity to M-EOSn/c fabrics using non-default DID base offset in McDATA or Open Fabric Mode

- **L2 Ethernet Feature Enhancements for Brocade 8000/FCOE10-24**
  - 802.1x
  - FIP VLAN Discovery

- **Miscellaneous**
  - Persistent WWN based PID assignment
  - Fabric Watch support for CPU and Memory utilization
  - Support for additional 3-chassis ICL connection topologies
  - Support for new 8-link (half bandwidth) ICL license on DCX
  - Audit logs generated for additional CLI/DCFM security configuration events
  - Last 256 audit entries are retained on switch or CP for viewing or clearing
  - Universal Temporary license keys for select features
  - Port Mirroring support with Virtual Fabrics and embedded switch platforms
  - Support for SNMP Informs

New Feature Descriptions

FCIP Enhancements

- FC traffic can be transported over an IP network when the 1 GbE or 10 GbE ports are configured to support FCIP. FOS v6.3.0 supports up to 20 FCIP tunnels on an FX8-24 blade, and 8 FCIP tunnels on the 7800. The FCIP tunnels on the local and remote GbE ports act as the Virtual E-Ports (VE_Ports) connecting the local and the remote fabrics. Performance is optimized for FCP and FICON traffic using Batching/Debatching operations on all data and command frames/IUs. This prevents fragmentation of multiple 2112 size FC frames (batch) into smaller IP frames compared to single frame exchanges (e.g. FC frame generators).

- **FCIP Trunking** is a new feature available on the FX8-24 and 7800 that virtualizes two or more TCP connections as part of a single FCIP tunnel. These connections, called circuits, will be explicitly configured to be part of an FCIP tunnel. Their primary purpose is to increase the tunnel bandwidth and provide fail-over paths in the event of a network failure. The functionality of the FCIP trunking and the additional TCP connections is transparent to the applications using the FCIP tunnel. FCIP Trunking requires the optional Advanced Extension license.

- New **Advanced Compression** capabilities on the 7800 allow the FC data frames to be compressed on a per tunnel basis before they are sent over the tunnel as FCIP frames. The FC command frames and all the frames that are generated from or destined for the control processor are not compressed even when compression is enabled on a tunnel. The uncompressed and compressed packets and bytes are counted and maintained on a per tunnel basis. The compression ratio can be found for a given polling interval by reading the number of compressed and uncompressed bytes. The compression is performed by the hardware on a frame-by-frame basis and is performed on FC data frames in the ingress direction before they are encapsulated as FCIP frames.

- The **Adaptive Rate Limiting** (ARL) feature on the FX8-24 and 7800 allows them to change the rate dynamically at which the FCIP tunnel transmits data through the TCP connection(s). ARL will use the information from the TCP connection(s) to determine and adjust the rate limit for the FCIP tunnel dynamically. This allows FCIP connections to utilize the maximum available bandwidth. ARL requires the optional Advanced Extension license.

FCR Enhancements

- EX-Port trunking was initially introduced in the FOS v5.2.0 release. However, when a master EX-Port within a trunk group goes offline, a new area (Master port) needs to be selected; this causes all slave EX-Ports of that trunk group to be disabled and brought online to select a new master EX-Port. The **Masterless EX-Port** feature in FOS v6.3.0 uses the dynamic port binding capability first introduced in FOS v6.2 to reassign the trunk area from the old master port to the new master port. On a master port offline condition, one of the slave ports becomes the new master port and all the other slave ports stay online. The new master port uses the old master port's area and the old master port gets a new and unused area. This way, the PID of the trunk does not change on master port offline.

- FOS v6.0 first introduced new Adaptive Networking features, including FC QoS, allowing users to establish flow-based prioritization of traffic traversing a SAN. FOS v6.3 extends **QoS over FC Routing (FCR)** configurations, allowing support of QoS for traffic flows originating in an

edge fabric, passing through the FC Backbone fabric, and then out to a destination edge fabric. Support of this feature requires configuration of both LSAN zones and QoS zones and requires the Adaptive Networking license be installed on switches in both the edge and backbone fabrics.

Adaptive Networking Enhancements

- If an administrator notices one or more applications running on the Datacenter Fabric is, slowing down then he/she can enable the new **Bottleneck Detection** feature on all suspected edge switches to which F-ports are attached in order to determine if there are any slow-draining devices that are causing network congestion. When bottleneck monitoring is enabled and a switch detects a condition where the offered load exceeds the rate at which the destination device can accept frames, a RAS LOG message can be generated and the administrator can view historic statistics logs for the port to investigate the problem. This new capability is considered part of the Adaptive Networking feature set but does not require a license. This feature is available on all 4G and 8G-capable ports.

Enhanced Native Connectivity with McDATA Products

- FOS-based platforms operating in Interopmode 3 may now participate in Mi10k fabrics using 239 DID mode. Previously, connecting to such fabrics could only be done via FCR.
- FOS-based platforms operating in either Interopmode 2 or 3 may now participate in M-EOS fabrics using non-default DID Base Offset settings.

CEE/FCoE Features

- **802.1X** defines a client/server-based authentication protocol for port access control. It forbids unknown/unauthorized clients from connecting to an Ethernet network through publicly accessible ports. The authentication server component of the system authenticates each client device or host connected to an authentication-enabled network port. Until the client is authenticated, 802.1X allows only the authentication protocol traffic (EAPOL) on the connected port. After the authentication is successful, the port is opened for all network traffic.

- **FIP VLAN Discovery protocol** is supported with the following caveat: the FIP VLAN DISCOVERY request must be received with either a priority-only VLAN tag (VLAN ID = 0), or a VLAN tag with the VLAN ID = FCoE VLAN. FIP VLAN DISCOVERY request received with a valid VLAN ID in the tag not equal to the FCoE VLAN will be dropped. The expected behavior is that the CNA will send a priority tagged FIP VLAN DISCOVERY request.

Optionally Licensed Software

Optionally licensed features in Fabric OS v6.3.0 include:

- **Brocade Ports on Demand** — Allows customers to instantly scale the fabric by provisioning additional ports via license key upgrade (applies to select models of switches).

- **Brocade Extended Fabrics** — Provides greater than 10km of switched fabric connectivity at full bandwidth over long distances (depending on platform this can be up to 3000km).

- **Brocade ISL Trunking** — Provides the ability to aggregate multiple physical links into one

logical link for enhanced network performance and fault tolerance. Also includes Access Gateway ISL Trunking on those products that support Access Gateway deployment.

- **Brocade Advanced Performance Monitoring** — Enables performance monitoring of networked storage resources. This license includes the TopTalkers feature.

- **High Performance Extension over FCIP/FC** (formerly known as "FC-IP Services") (For the FR4-18i blade and Brocade 7500) — This license key also includes the FC-FastWrite feature and IPsec capabilities.

- **Brocade Accelerator for FICON** – This license enables unique FICON emulation support for IBM's Global Mirror (formerly XRC) application (including Hitachi Data Systems HXRC and EMC's XRC) as well as Tape Pipelining for all FICON tape and virtual tape systems to significantly improve XRC and tape backup/recovery performance over virtually unlimited distance for 7500, upgraded 7500E and FR4-18i.

- **Brocade Fabric Watch** — Monitors mission-critical switch operations. Fabric Watch also includes Port Fencing capabilities.

- **FICON Management Server** — Also known as "CUP" (Control Unit Port), enables host-control of switches in Mainframe environments.

- **ICL 16-link, or Inter Chassis Links** – This license provides dedicated high-bandwidth links between two Brocade DCX chassis, without consuming valuable front-end 8Gb ports. Each chassis must have the 16-link ICL license installed in order to enable the full 16-link ICL connections. (Available on the DCX only, previously known as simply the "ICL License" for DCX.)

- **ICL 8-Link, or Inter Chassis Links** – This license activates all eight links on ICL ports on a DCX-4S chassis or half of the ICL bandwidth for each ICL port on the DCX platform by enabling only eight links out of the sixteen links available. This allows users to purchase half the bandwidth of DCX ICL ports initially and upgrade with an additional 8-link license to utilize the full ICL bandwidth at a later time. This license is also useful for environments that wish to create ICL connections between a DCX and a DCX-4S, the latter of which cannot support more than 8 links on an ICL port. Available on the DCX-4S and DCX platforms only (This license replaces the original ICL license for the DCX-4S and is new for the DCX).**Enhanced Group Management** — This license, available only on the DCX, DCX-4S and other 8G platforms, enables full management of the device in a datacenter fabric with deeper element management functionality and greater management task aggregation throughout the environment. This license is used in conjunction with Brocade's Data Center Fabric Manager (DCFM) application software.

- **Adaptive Networking** — Adaptive Networking provides a rich framework of capability allowing a user to ensure high priority connections obtain the network resources necessary for optimum performance, even in congested environments. The QoS SID/DID Prioritization and Ingress Rate Limiting features are the first components of this license, and are fully available on all 8G platforms.

- **Integrated Routing** — This license allows ports in a DCX, DCX-4S, 5300, 5100, 7800 or Brocade Encryption Switch to be configured as EX_Ports or VEX_Ports supporting Fibre Channel Routing. This eliminates the need to add an FR4-18i blade or use the 7500 for FCR purposes, and also provides double the bandwidth for each FCR connection (when connected to another 8G-capable port).

- **7500E Upgrade** (For the Brocade 7500E only) — This license allows customers to upgrade a 4-port (2 FC ports and 2 GE ports) 7500E base to a full 18-port (16 FC ports and 2 GE ports) 7500

configuration and feature capability. The upgraded 7500E includes the complete High Performance Extension license feature set.

- **Encryption Performance Upgrade** — This license provides additional encryption processing power. For the Brocade Encryption Switch or a DCX/DCX-4S, the Encryption Performance License can be installed to enable full encryption processing power on the BES or on all FS8-18 blades installed in the DCX/DCX-4S chassis.

- **DataFort Compatibility** — This license is required on the Brocade Encryption Switch/DCX/DCX-4S with FS8-18 blade(s) to read & decrypt NetApp DataFort-encrypted disk and tape LUNs. DataFort Compatibility License is also required on the Brocade Encryption Switch or DCX/DCX-4S Backbone with FS8-18 Encryption Blade(s) installed to write & encrypt the disk and tape LUNs in NetApp DataFort Mode (Metadata & Encryption Algorithm) so that DataFort can read & decrypt these LUNs. DataFort Mode tape encryption and compression is supported beginning with the FOS v6.2.0 release. Availability of the DataFort Compatibility license is limited; contact your vendor for details.

- **Server Application Optimization** — When deployed with Brocade Server Adapters, this license optimizes overall application performance for physical servers and virtual machines by extending virtual channels to the server infrastructure. Application specific traffic flows can be configured, prioritized, and optimized throughout the entire data center infrastructure. This license is not supported on the Brocade 8000.

- **FCoE** — This license enables Fibre Channel over Ethernet (FCoE) functionality on the Brocade 8000. Without the FCoE license, the Brocade 8000 is a pure L2 Ethernet switch and will not allow FCoE bridging or FCF capabilities. This license should always be installed with the 8000 FC Ports on Demand license.

- **8000 FC Ports on Demand** — This new license enables all eight FC ports on the Brocade 8000. (**IMPORTANT NOTE:** Most Brocade 8000 units shipped with FOS v6.1.2_CEE1 did not ship with this license and need to have it installed <u>prior</u> to upgrading to FOS v6.3.0. Failure to do so will result in disabling of FC ports following the upgrade. Please contact Brocade to obtain this license key). This license should always be installed with the FCoE license.

- **7800 Port Upgrade** — This new license allows a Brocade 7800 to enable 16 FC ports (instead of the base four ports) and six GbE ports (instead of the base two ports). This license is also required to enable additional FCIP tunnels and also for advanced capabilities like tape read/write pipelining. The Brocade 7800 must have the Port Upgrade license installed to add FICON Management Sever (CUP) or Advanced Accelerator for FICON.

- **Advanced Extension** – This new license enables two advanced extension features: FCIP Trunking and Adaptive Rate Limiting. The FCIP Trunking feature allows multiple IP source and destination address pairs (defined as FCIP Circuits) via multiple 1GbE or 10GbE interfaces to provide a high bandwidth FCIP tunnel and failover resiliency. In addition, each FCIP circuit supports four QoS classes (Class-F, Hi, Medium and Low Priority), each as a TCP connection. The Adaptive Rate Limiting feature provides a minimum bandwidth guarantee for each tunnel with full utilization of the available network bandwidth without impacting throughput performance under high traffic load. This license is available on the 7800 and the DCX/DCX-4S for the FX8-24 on an individual slot basis.

- **10GbE FCIP** – This new license enables the two 10GbE ports on the FX8-24. With this license, two additional operating modes (in addition to 10 1GbE ports mode) can be selected:
  - o 10 1GbE ports and 1 10GbE port, or

o 2 10GbE ports

This license is available on the DCX/DCX-4S for the FX8-24 on an individual slot basis.

- **Advanced FICON Acceleration** – This new licensed feature uses specialized data management techniques and automated intelligence to accelerate FICON tape read and write and IBM Global Mirror data replication operations over distance, while maintaining the integrity of command and acknowledgement sequences. This license is available on the 7800 and the DCX/DCX-4S for the FX8-24 on an individual slot basis.

Some models offer bundles that include 2 or more optionally licensed features. These bundles are defined for each unique product, and are outside the scope of this release note document.

Temporary License Support
The following licenses are available for 45-day temporary use, with a maximum of two temporary licenses per feature and per switch (90 days maximum):
- Fabric (E_Port) license
- Extended Fabric license
- Trunking license
- High Performance Extension license
- Advanced Performance Monitoring license
- Adaptive Networking license
- Fabric Watch license
- Integrated Routing license
- Server Application Optimization(support as a temporary license is new in FOS v6.3)
- Advanced Extension license (support is new in FOS v6.3)
- Advanced FICON Acceleration license (support is new in FOS v6.3)
- 10GbE FCIP license (support is new in FOS v6.3)

Note: Temporary Licenses for features available on a per slot basis enable the feature for any and all slots in the chassis.

Universal Temporary License Support (New)
The following list of licenses are available as Universal Temporary licenses, meaning the same license key can be installed on any switch running FOS v6.3 or later that supports the specific feature. Universal Temporary license keys can only be installed once on a particular switch, but can be applied to as many switches as desired. Temporary use duration (the length of time the feature will be enabled on a switch) is provided with the license key. All Universal Temporary license keys have an expiration date upon which the license can no longer be installed on any unit.
- Fabric (E_Port) license
- Extended Fabric license
- Trunking license
- High Performance Extension license
- Advanced Performance Monitoring license
- Adaptive Networking license
- Fabric Watch license

- Integrated Routing license
- Server Application Optimization
- Advanced Extension license
- Advanced FICON Acceleration license
- 10GbE license

Previously Licensed Software Now Part of Base FOS

The following capabilities are included as part of the base FOS capability and no additional purchase or licensing is necessary:

- Advanced Zoning and WebTools licenses are no longer necessary beginning with FOS v6.1. These features are automatically enabled on all products running FOS v6.1 or later.

Supported Switches

Fabric OS v6.3.0 supports the Brocade 300, 5410/5480/5424/5450, 4100, 4900, 5000, 5100, 5300, 7500/7500E, 7600, 48000, Brocade Encryption Switch (BES), DCX/DCX-4S, 8000, and the new 7800. All supported products are qualified for Native Connectivity in interopmodes 2 and 3 for deployment in M-EOS fabrics with the exception of the Brocade 4100 and 8000.

Access Gateway mode is also supported by Fabric OS v6.3.0, and is supported on the following switches: the Brocade 300, 5100, 5480, 5450 and M5424.

Note that FOS v6.3 does NOT support the following platforms and cannot be loaded on them, though these switches may participate in the same fabric as other switches using FOS v6.3:
- Brocade 200E
- All 4G embedded switches, including the 4012, 4016, 4018, 4020, 4024, 4424

Please refer to the *Supported Products and FOS Interoperability* table for the versions of FOS code that must be used on these platforms to interoperate with FOS v6.3. The above noted 4G platforms will continue to be supported by FOS v6.2.x.

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 FC standards conformance, visit the following Brocade Web site: *http://www.brocade.com/sanstandards*

The Brocade 8000 and FCOE10-24 blade conform to the following Ethernet standards:
- IEEE 802.1D   Spanning Tree Protocol
- IEEE 802.1s   Multiple Spanning Tree
- IEEE 802.1w   Rapid reconfiguration of Spanning Tree Protocol
- IEEE 802.3ad   Link Aggregation with LACP
- IEEE 802.3ae   10G Ethernet
- IEEE 802.1Q   VLAN Tagging
- IEEE 802.1p   Class of Service Prioritization and Tagging
- IEEE 802.1v   VLAN Classification by Protocol and Port

- IEEE 802.1AB   Link Layer Discovery Protocol (LLDP)
- IEEE 802.3x   Flow Control (Pause Frames)

The following draft versions of the Converged Enhanced Ethernet (CEE) and Fibre Channel over Ethernet (FCoE) Standards are also supported on the Brocade 8000 and FCOE10-24 blade:
- IEEE 802.1Qbb   Priority-based Flow Control
- IEEE 802.1Qaz   Enhanced Transmission Selection
- IEEE 802.1   DCB Capability Exchange Protocol (Proposed under the DCB Task Group of IEEE 802.1 Working Group)
- FC-BB-5   FCoE (Rev 2.0)

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, including the switch or fabric behavior immediately following the problem, and specific questions
   - Description of any troubleshooting steps already performed and the results
   - Serial console and Telnet session logs
   - Syslog message logs

2. **Switch Serial Number**

   The switch serial number is provided on the serial number label, examples of which are shown here:

   The serial number label is located as follows:

   - Brocade 4100, 4900, and 7500/7500E — On the switch ID pull-out tab located inside the chassis on the port side on the left
   - Brocade Encryption Switch, 300, 5000, 5100, and 5300 — On the switch ID pull-out tab located on the bottom of the port side of the switch

- Brocade 7600 — On the bottom of the chassis

- Brocade 7800 — On the pull-out tab on the front left side of the chassis underneath the serial console and Ethernet connection and on the bottom of the switch in a well on the left side underneath (looking from front)

- Brocade 8000 — On the switch ID pullout tab located inside the chassis on the port side on the left and also on the bottom of the chassis.

- Brocade 48000 — Inside the chassis next to the power supply bays

- Brocade DCX — Bottom right of the port side

- Brocade DCX-4S — Back, upper left under the power supply

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

When the Virtual Fabric feature is enabled on a switch, each logical switch has a unique switch WWN. Use the **wwn** command to display the switch WWN.

If you cannot use the **wwn** command because the switch is inoperable, you can get the primary WWN from the same place as the serial number, except for the Brocade DCX/DCX-4S. For the Brocade DCX, access the numbers on the WWN cards by removing the Brocade logo plate at the top of the non-port side. The WWN is printed on the LED side of both cards.

4. **License Identifier (License ID)**

There is only one License Identifier associated with a physical switch or director/backbone chassis. This License Identifier is required as part of the ordering process for new FOS licenses.

Use the **licenseId** command to display the License Identifier.

Important Notes

This section contains information that you should consider before you use this Fabric OS release.

DCFM Compatibility

FOS v6.3.0 is compatible with Brocade's Data Center Fabric Manager (DCFM) v10.3.x management software. DCFM is a comprehensive SAN management application that enables end-to-end management of Brocade Data Center Fabrics. It is the next-generation successor product to existing Brocade management products, including Brocade Fabric Manager (FM) and Brocade Enterprise Fabric Connectivity Manager (EFCM).

DCFM 10.3 is available in three editions:
- *DCFM Professional:* a fabric management application that is ideally suited for small-size businesses that need a lightweight management product to manage their smaller fabrics. It manages one FOS fabric at a time, up to 1,000 switch ports, and provides support for Brocade

FC switches, Brocade HBAs / CNAs, and Fibre Channel over Ethernet (FCoE) / Converged Enhanced Ethernet (CEE) switches

- *DCFM Professional Plus*: a SAN management application designed for medium-size businesses for managing up to 4 physical fabrics (FOS, M-EOS and Mixed fabrics) up to 2,560 switch ports. It supports Brocade director products (DCX-4S, 48Ks, etc.), FC switches, Fibre Channel Over IP (FCIP) switches, Fibre Channel Routing (FCR) switches/ Integrated Routing (IR) capabilities, Fibre Channel over Ethernet (FCoE) / Converged Enhanced Ethernet (CEE) switches, and Brocade HBAs / CNAs. Enterprise-class customers looking to manage departmental SANs can consider deploying this product as well
- *DCFM Enterprise*: a SAN management application designed for enterprise-class customers for managing up to 24 physical fabrics and up to 9,000 switch ports. DCFM Enterprise supports all the hardware platforms and features that DCFM Professional Plus supports, and also adds support for the Brocade DCX Director product, and Fiber Connectivity (FICON) capabilities

Existing EFCM v9.6.x/9.7.x and FM v5.4/5.5 customers are provided an easy migration path to DCFM Enterprise.

Note: DCFM cannot manage FOS switches or fabrics using Administrative Domains (ADs). Environments using ADs must use the CLI or WebTools for management.

EFCM and Fabric Manager Compatibility

With the introduction of DCFM, both EFCM and Fabric Manager (FM) have been put into sustaining mode. Consequently, **neither EFCM nor FM are qualified or supported for management of switches operating with FOS v6.3 firmware**. Very basic evaluation has shown that there are significant compatibility issues between FM and FOS v6.3, including (but not limited to) compromised functionality in the zoning dialog and performance graphs, port enabling/disabling, and the FICON wizard.

WebTools Compatibility
- FOS v6.3 is supported with JRE 1.6.0 Update 13.

- If the JRE v1.6.0 version is not at Update 13, the DCFM server / client and B-model Element Manager (Web Tools) Crashes on launch

- WebTools Tunnel and TCP graphs only support Tooltips for the first enabled TCP connection graph.

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.

When using the Virtual Fabrics feature, it is highly recommended that all switches participating in a fabric with a logical switch use the latest firmware available for those switches. All switches must be operating at minimum firmware levels noted in the FOS Interoperability table below.

When using any of Brocade's encryption platforms (Brocade Encryption Switch or Brocade FS8-18 blade in a DCX or DCX-4S) it is required that switches attached to hosts and targets or those that are part of the encryption flow be operating with minimum specified levels:

- 2Gb/4Gb platforms must operate with FOS v5.3.1b or later

- 4Gb/8Gb platforms must operate with FOS v6.1.0e, v6.1.1 or later (4Gb platforms may use v5.3.1b but are recommended to use the v6.x versions)

- M-EOS platforms must operate with M-EOS v9.8.0 or later for McDATA Fabric Mode (interopmode 2) or M-EOS 9.9.0 or later for Open Fabric Mode environments (interopmode 3)

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

Supported Products and FOS Interoperability	
Brocade 2000-series switches	Not supported, end of support (December 2007)
Brocade 3200, 3800	Not supported.
Brocade 3000	v3.2.1c [1][6][7]
Silkworm 3016, 3250, 3850 and Brocade 3900, 4100, 4900, 24000, 7500, 7500E, 5000, 200E, 48000	v5.3.2 (2G and 4G platforms) and v6.1.0e and later [5] (4G platforms only)
Silkworm 12000	v5.0.x [6][7]
Brocade 4012, 4016, 4018, 4020, 4024, 4424	v5.3.1b, v6.1.0e and later [5]
Brocade 5410, 5480, 5424	v6.2.0
Brocade 8000	v6.1.2_CEE1 or later
Brocade 7800, DCX and DCX-4S with FCOE10-24 or FX8-24 blades	v6.3.0
Brocade DCX, 300, 5100, 5300	v6.1.0e and later [5]
Brocade DCX-4S	v6.2.0
Brocade DCX with FS8-18 blade(s), Brocade Encryption Switch	v6.1.1_enc
Brocade DCX/DCX-4S/48000 with FA4-18 blade(s), Brocade 7600	v5.2.x or later (DCX requires v6.0.x or later, DCX-4S requires 6.2.x or later)
Mi10k, M6140, ED-6064, ES-3232, ES-4300, ES-4400, ES-4500, ES-4700 (McDATA Fabric Mode and Open Fabric Mode) [2][4]	M-EOS v9.9.5 or later [3]
McDATA ED-5000 32-port FC director	Not Supported

Multi-Protocol Router interop	
Brocade 7420	XPath v7.4.1 [8]
Brocade 7500 and FR4-18i blade	v5.1.0 and higher [8]
McDATA SANRouters 1620 and 2640	Not Supported

Table Notes:

[1] All zoning and fabric operations performed in a fabric with products running older versions of FOS should be done via interfaces to products running the latest version of FOS. This is particularly important for Brocade 3XXX series switches that do not support zoning configuration for newer products.

[2] Other M-EOS models may participate in a fabric with FOS v6.3, but may not be directly attached via E_Port to any products running FOS v6.3. The McDATA ED-5000 director may not participate in a mixed M-EOS/FOS fabric.

[3] It is highly recommended that M-EOS products operate with the most recent version of M-EOS released and supported for interoperability. M-EOS 9.9.5 is the only version of code that has been fully qualified for interoperability with FOS v6.3. M-EOS 9.7.2 is the minimum version of firmware that is supported to interoperate with FOS 6.3. For support of frame redirection in McDATA Fabric Mode (interopmode 2), M-series products must use M-EOS v9.8 or later. For support of frame redirection in McDATA Open Fabric Mode (interopmode 3), M-series products must use M-EOS v9.9 or later. Only the ES-4400, ES-4700, M6140, and Mi10k may have devices directly attached that are having data encrypted or unencrypted.

[4] When routing to an M-EOS edge fabric using frame redirection, the M-EOS fabric must have a FOS-based product in order to configure the frame redirection zone information in the edge fabric.

[5] When directly attached to a Host or Target that is part of an encryption flow.

[6] Products operating with FOS versions less than v5.3.1b or v6.1.0e may not participate in a logical fabric that is using XISLs (in the base fabric).

[7] These platforms may not be directly attached to hosts or targets for encryption flows.

[8] McDATA 1620 and 2640 SANRouters should not be used with XPath or FOS-based routing (FCR) for connections to the same edge fabric.

Fabric OS v6.3.0 software is fully qualified and supports the blades for the 48000 platform noted in the following table:

48000 Blade Support Matrix	
Port blade 16, 32 and 48-port 4Gbit blades (FC4-16, FC4-32, FC4-48), 16, 32 and 48-port 8Gbit blade (FC8-16, FC8-32, FC8-48), and the 6-port 10G FC blade (FC10-6)	Supported with any mix and up to 8 of each. No restrictions around intermix. The 48000 must run Fabric OS v6.0 or later to support the FC8-16 port blade and Fabric OS v6.1 or later to support the FC8-32 and FC8-48 port blades.
Intelligent blade	Up to a total of 4 Intelligent blades (includes iSCSI, FCIP/FCR and Application blade), FC4-16IP, FR4-18i, and FA4-18 respectively. See below for intermix limitations, exceptions, and a max of each blade.
iSCSI blade (FC4-16IP)	Up to a maximum of 4 blades of this type
FC-IP/FC Router blade (FR4-18i)	Up to a maximum of 2 blades of this type. This can be extended under special circumstances but must be approved by Brocade's Product Team. Up to 8 FR4-18i blades can be installed if they are used only for FC FastWrite or FCIP without routing.
Virtualization/Application Blade (FA4-18)	Up to a maximum of 2 blades of this type.
Encryption Blade (FS8-18), Extension Blade (FX8-24), FCoE/CEE Blade (FCOE10-24)	Not supported.

Fabric OS v6.3.0 software is fully qualified and supports the blades for the DCX/DCX-4S noted in the following table:

DCX/DCX-4S Blade Support Matrix	
16-, 32- and 48-port 8Gbit port blades (FC8-16, FC8-32, FC8-48) and the 6-port 10G FC blade (FC10-6)	Supported with FOS v6.0 and above with any mix and up to 8/4 of each. No restrictions around intermix.
Intelligent blade	Up to a total of 8/4 intelligent blades. See below for maximum supported limits of each blade.
FC-IP/FC Router blade (FR4-18i)	Up to a maximum of 4 blades of this type. This can be extended under special circumstances, but must be approved by Brocade's Product Team. Up to 8 FR4-18i blades can be installed in a DCX if they are used only for FC FastWrite or FCIP without routing.
Virtualization/Application Blade (FA4-18)	Up to a maximum of 4 blades of this type.

DCX/DCX-4S Blade Support Matrix	
Encryption Blade (FS8-18)	Up to a maximum of 4 blades of this type.
Extension Blade (FX8-24)	Up to a maximum of 2 blades of this type.
FCoE/CEE Blade (FCOE10-24)	Up to a maximum of 2 blades of this type. Cannot be used in a chassis with other intelligent blades (can only be installed concurrently with FC8-XX and/or FC10-6 blades)

Note: the iSCSI FC4-16IP blade is not qualified for the DCX/DCX-4S.

Power Supply Requirements for Blades in 48k and DCX/DCX-4S Chassis					
Blades	**Type of Blade**	**48K** @200-240 VAC (Redundant configurations)	**DCX/DCX-4S** @110 VAC (Redundant configurations)	**DCX/DCX-4S** @200-240 VAC (Redundant configurations)	**Comments**
FC4-16, FC 4-32, FC4-48, FC8-16, FC8-32	Port Blade	2 Power Supplies	2 Power Supplies	2 Power Supplies	• Distribute the Power Supplies evenly to 2 different AC connections for redundancy.
FC10-6, FC 8-48	Port Blade	4 Power Supplies	Not Supported	2 Power Supplies	
FR4-18i, FC4-16IP*, FA4-18	Intelligent Blade	4 Power Supplies	Not Supported	2 Power Supplies	
FS8-18, FX8-24, FCOE10-24	Intelligent Blade	NA	Not Supported	DCX: 2 or 4 Power Supplies DCX-4S: 2 Power Supplies	• For DCX with three or more FS8-18 Blades, (2+2) 220VAC Power Supplies are required for redundancy. • For DCX with one or two FS8-18 Blades, (2) 220VAC Power Supplies are required for redundancy. • For DCX-4S, (2) 220VAC Power Supplies provide redundant configuration with any number of FS8-18 Blades. • For both DCX and DCX-4S with FX8-24

Power Supply Requirements for Blades in 48k and DCX/DCX-4S Chassis					
Blades	Type of Blade	48K @200-240 VAC (Redundant configurations)	DCX/DCX-4S @110 VAC (Redundant configurations)	DCX/DCX-4S @200-240 VAC (Redundant configurations)	Comments
					blades, (1+1) 220VAC Power Supplies are required for redundancy.

*Note: the iSCSI FC4-16IP blade is not qualified for the DCX/DCX-4S.

FOS Feature Compatibility in Native Connectivity Modes

Some FOS features are not fully supported when operating in the native connectivity modes for deployment with M-EOS based products. All Brocade models that are supported by Fabric OS v6.3.0 support both interopmodes 2 and 3 with the exception of the Brocade 4100 and 8000 and DCX/DCX-4S with one or more FCOE10-24 blades.

The following table specifies the support of various FOS features when operating in either interopmode 2 (McDATA Fabric Mode) or interopmode 3 (Open Fabric Mode) with Fabric OS v6.3.

FOS Features (supported in interopmode 0)	FOS v6.3	
IM = Interopmode	IM 2	IM 3
L2 FOS Hot Code Load	Yes	Yes
FOS Hot Code Load with FCR	Yes	Yes
Zone Activation Support	Yes	Yes[11]
Traffic Isolation Zones[1]	Yes	No
Frame Redirection (devices attached to FOS)[1]	Yes	Yes[11]
Frame Redirection (devices attached to M-EOS)[1]	Yes	Yes[11]
Frame Redirection over FCR[10]	Yes	Yes[11]
FCR Fabric Binding (route to M-EOS fabric with Fabric binding)[9]	Yes	Yes
L2 Fabric Binding	Yes	No*
DCC policies	No	No
SCC policies	Yes[4]	No*
E/EX_Port Authentication	Yes	Yes
ISL Trunking (frame-level)	Yes[2]	Yes[2]
Dynamic Path Selection (DPS, exchange based routing)	Yes[3]	Yes[3]
Dynamic Load Sharing (DLS, port based routing)	Yes	Yes
Virtual Channels (VC RDY)	Yes[2]	Yes[2]
FICON Management Server (Cascading)	Yes	No*
FICON MIHPTO	Yes	No*
Full Scalability (to maximum M-EOS fabric limits)	Yes	Yes
Adaptive Networking: QoS	No	No
Adaptive Networking: Ingress Rate Limiting	No*	No*
Advanced Performance Monitoring (APM)	No*	No*

FOS Features (supported in interopmode 0)	FOS v6.3	
IM = Interopmode	IM 2	IM 3
APM: TopTalkers	No*	No*
Admin Domains	No	No
Secure Fabric OS[5]	N/A	N/A
Fabric Watch	Yes	Yes
Ports on Demand (POD)	Yes	Yes
NPIV	Yes	Yes
Timer Server function (NTP)	No	No
Open E_Port[6]	N/A	N/A
Broadcast Zoning	No	No
FDMI	No	No
Remote Switch	No	No
Port Mirroring	Yes	Yes
Extended Fabrics	Yes	Yes[7]
Alias Server	No	No
Platform Service	No	No
FCIP (VE_Ports)	Yes	Yes
IPFC (IP over FC)	Yes[8]	Yes[8]
M-EOS ALPA 0x13 configuration	Yes	Yes
VE to VEX Port	Yes	Yes
Integrated Routing[9]	Yes[9]	Yes
Domain Offset Support	Yes	Yes
239 Domain Support (available on Mi10k only)	N/A	Yes
Masterless F_PORT Trunking (AG connect to FOS switches only)	Yes	Yes
FC10-6-to-FC10-6 ISL	Yes	Yes
RASLOG Events on duplicate WWNs	Yes	Yes
Virtual Fabrics	Yes	Yes
Logical Fabric using LISLs (XISLs in Base Fabric)	No	No
Port Fencing	Yes	Yes
Bottleneck Detection	Yes	Yes

* indicates the feature is available but not officially tested or supported

1. Requires M-EOS 9.7 or later for redirection between devices attached to FOS switches, M-EOS 9.8 for redirection between devices attached to M-EOS switches, M-EOS 9.9 for use in McDATA Open Fabric Mode. Supported M-EOS platforms include M4400, M4700, M6140, and Mi10k.
2. Only allowed between FOS-based switches
3. DPS is supported outbound from FOS-based switches. (M-EOS can provide reciprocal load balancing using OpenTrunking).
4. SCC policies only supported in conjunction with L2 Fabric Binding support
5. Not supported in FOS 6.0 or later
6. Mode 3 only qualified with M-EOS switches
7. Not on FCR
8. Only supported locally within the FOS switch
9. All routers (EX_Ports) must reside in a backbone fabric running in interopmode 0 only. Only edge fabrics with devices imported to the backbone fabric or other edge fabrics may be operating in IM2 or IM3.
10. To support Frame Redirection to an edge M-EOS fabric, there must be at least one FOS switch in the edge fabric to configure Frame Redirection Zones.

11. Only Frame Redirection Zones may be configured on FOS platforms and sent to fabrics operating in McDATA Open Fabric Mode (interopmode 3). M-EOS 9.9 is required to support FR Zones in McDATA Open Fabric Mode.

Note: FICON Cascaded CUP with M-EOS and FOS qualified only on select platforms.

Firmware Upgrades and Downgrades

Upgrading to Fabric OS v6.3.0 is only allowed from Fabric OS v6.2.0 or later. This policy to support only one-level migration, which began with FOS v6.0.0, provides more reliable and robust migrations for customers. By having fewer major changes in internal databases, configurations, and subsystems, the system is able to perform the upgrade more efficiently, taking less time and ensuring a truly seamless and non-disruptive process for the fabric. The one-release migration policy also reduces the large number of upgrade/downgrade permutations that must be tested, allowing Brocade to spend more effort ensuring the supported migration paths are thoroughly and completely verified.

All products supported by Fabric OS v6.2.X or v6.1.2_CEEx can be upgraded to Fabric OS v6.3. The following is a list of products that can be upgraded to Fabric OS v6.3:

- 5424/5410/5480, 4100, 4900, 5000, 300, 5100, 5300, 7500/7500E, 7600, 8000, 48000, BES, DCX-4S and DCX.

Switches using Integrated Routing and operating with FOS v6.2.2x may <u>not</u> be upgraded directly to FOS 6.3.0/v6.3.0a/v6.3.0b. Units operating with IR and FOS v6.2.2x should be upgraded to FOS v6.3.0c or later or first downgraded to a release prior to v6.2.2.

FOS does not support concurrent FC Routing (EX_Ports) and TopTalkers features.

If there are multiple node EGs (encryption groups) in a fabric, please complete firmwaredownload on one node at a time before downloading on another node.

The Brocade 8000 does not support non-disruptive hot code loads (HCL). Upgrading the Brocade 8000 from FOS v6.1.2_cee1 to FOS v6.3 or from FOS 6.3 to a later FOS version will be disruptive to the IO through the switch.

A code load of DCX or DCX-4s with one or more FCOE10-24 blades from FOS 6.3 to another version will disrupt traffic through the blade.

When upgrading a Brocade 8000 from FOS v6.1.2_CEE or v6.1.2_CEE1 to v6.3, verify that the unit has both the FCoE and FC POD licenses installed. Units missing these licenses that are upgraded to FOS v6.3 will lose functionality following a restart or disabling of ports. Note that when the FC POD license is installed on a unit with FOS v6.1.2, the *licenseShow* output will indicate that the license is "not applicable on this platform." This message can be ignored and will not appear once the unit has been upgraded to v6.3.

If a switch with FOS v6.2 in FIPS (Federal Information Processing Standards) mode with only LDAP authentication support is upgraded to v6.3, login will fail. A switch with v6.2 in FIPS mode must have both LDAP and local authentication configured before upgrading to v6.3. Once the switch is fully operational, the user can login to the switch and import the certificate again. If the switch is not in FIPS mode, users can login to the switch with LDAP after upgrading to v6.3 and then import the certificate.

SAS Version Requirements for FA4-18 and Brocade 7600:

SAS v3.4.0 is the supported SAS version for FOS v6.3.0.
  • When upgrading from FOS v6.2 to v6.3.0 and SAS 3.3.0 to SAS 3.4.0, first upgrade FOS v6.2 to v6.3.0 and then upgrade SAS from 3.3.0 to 3.4.0.
  • When downgrading from FOS v6.3.0 to v6.2 and SAS 3.4.0 to SAS 3.3.0, first downgrade SAS from 3.4.0 to 3.3.0 and then downgrade FOS from v6.3.0 to v6.2. If the switch is downgraded to v6.2 prior to the SAS downgrade to v3.3, the switch will fault.

Scalability
All scalability limits are subject to change. Limits may be increased once further testing has been completed, even after the release of Fabric OS. For current scalability limits for Fabric OS, refer to the *Brocade Scalability Guidelines* document, available under the *Technology and Architecture Resources* section at http://www.brocade.com/compatibility

Other Important Notes and Recommendations

FCIP, FCIP Trunking and High Bandwidth (Brocade 7800 and FX8-24)

- The maximum supported MTU size for the Brocade 7800/FX8-24 is 1500 with FOS v6.3.0.

- FCIP connections are supported only between the Brocade 7800/FX8-24 and another 7800/FX8-24. FCIP tunnels are not supported between the 7800/FX8-24 and the previous generation Brocade 7500/FR4-18i platforms.

- When additional circuits (and the network bandwidth provided by those circuits) are added to an already active tunnel, there is a short period of time where some frame loss can occur due to the process to re-fresh the internal FC frame routing tables in the switch. Therefore, additional circuits should only be added during low I/O periods utilizing the FCIP Tunnel being modified. In addition, if the circuit operation (addition/deletion) to the tunnel increases/decreases the total tunnel bandwidth, an FCIP Tunnel (VE port) disable/enable sequence should be performed after the addition/deletion of the circuit. This will allow the switch to adjust the internal routes to utilize the new bandwidth fully.

- Switching modes between 10G and 1G is disruptive for FCIP traffic.

- Keep alive timeout (milliseconds) - Valid range is 500ms to 7,200,000ms (inclusive). Default value is 10000ms (10 seconds). If FICON is configured the recommended value is 1000 ms (1 second), otherwise the recommended value is the default of 10 seconds. For impairment networks with 100ms latency and 0.5% packet loss, keep-alive time out should be configured as 30seconds. If the local and remote circuit configurations' Keep Alive Timeout values do not match, the tunnel will use the lower of the two configured values.

- Software compression (available on the 7800) modes 2 and 3 are not supported in FICON environments; they are supported only in Open Systems environments.

- Software compression (mode 2, 3) generally gives a better compression ratio, but not the throughput/bandwidth across all six GE ports. Software compression is recommended for low throughput links and supports throughput up to 2Gbps across all 6 GE ports.

- In order to perform the following operations it is necessary to delete the FCIP configuration on the affected ports first:
    - o Switching modes between 1G/10G/Dual
    - o Moving VE/GE port between logical switches
- The FX8-24 supports three different operating modes:
    1) Ten 1-GbE ports mode (default)
    2) Ten 1GbE ports and one 10GbE port
    3) Two 10GbE ports

    Modes 2 and 3 require the slot-based 10 GbE FCIP license.
- ARL (Adaptive Rate Limiting) is not supported on 10G tunnels.
- IPv6, IPSec, Diffserv, VLAN tagging, and "Inband Management" are not supported on the Brocade 7800 or FX8-24.
- FOS v6.3 only supports up to four 1 Gig Circuits per VE/FCIP Tunnel for the 1 gig interfaces. A VE/FCIP Tunnel created over the 10 Gig Interfaces will be limited to 10 circuits created using IPIFs on the same 10 GbE port (and no more than 1G per circuit).
- As a recommended best practice, the VE tunnel shouldn't be over-subscribed (e.g. 8G FC traffic over 500Mbps tunnel). General guidelines are 2:1 subscription without compression and 4:1 with compression.
- Non-disruptive firmware activation on FOS v6.3 will disrupt I/O traffic on FCIP links.
- Fibre Channel Routing (VEX) is not supported on the Brocade FX8-24 blade but is supported on the Brocade 7800.
- Differences between the Brocade 7800/FX8-24 platforms and previous generation 7500/FR4-18i platforms include:
    - o On the 7800, the GbE port does not directly correlate to a VE port
    - o On the FX8-24, GbE ports 0-9 or 10GbE port 1 (xge1) correspond to VE ports 12-21, and 10 GbE port 0 (xge0) corresponds to VE ports 22-31
    - o The CLI syntax for the 7800/FX8-24 varies from the 7500/FR4-18i. Please refer to the *Brocade Fabric OS Command Reference* document for FOS v6.3 for details.
- Both ends of a tunnel must be identically configured for Compression, FW and Tape pipeline options. If a mismatch exists, the tunnel will not be established and the TCP virtual connections will be removed.
- Under Traffic Isolation Zone, configurations with fail over enabled, Non-TI zone traffic will use the dedicated path if no other E or VE paths through the fabric exist, or if the non-dedicated paths are not the shortest paths. (A higher bandwidth tunnel with multiple circuits will become shortest path compared to a single tunnel).
- A VE/VEX Tunnel and E/EX FC port cannot connect to the same domain at the same time.
- The Recommended Keep Alive Timeout must be the same on tunnel/circuits on the switches on both sides of a link.

- Brocade 7800 or FX8-24 cannot receive a ping from an external device (for example – Windows PC).
- Latency measurements supported on FCIP Tunnels (Tested limit under FOS v6.3.0):
    - 1GbE - 200ms round trip time and 1% Loss
    - 10GbE – 50ms round trip and 0.1% Loss
- Brocade 7800 supports Optical and Copper Media types on GE0 and GE1 interfaces. Copper Media type is default on GE0/GE1 ports and does not support auto-sense functions.
- When inserting a 4G SFP in GE ports of an FX8-24 blade or 7800 switch, users may occasionally see one of the following:
    - "No_Light" or "Unknown" for GE ports in switchshow output. Removing and re-inserting the optic should correct this indication.
    - "Can't read serial data" in sfpshow output. Issuing the sfpshow command again should resolve this.

FCoE/CEE (Brocade 8000 and FCOE10-24)

- The Brocade 8000 balances the FCoE bandwidth across all six port groups (each port group contains four ports). To get optimum performance for FCoE traffic it is recommended that the user distribute server CNA connections across these six port groups.

- Hot plugging a CP with firmware level less than FOS v6.3.0 into a DCX or DCX-4S with an active FCOE10-24 blade will result in the new standby CP not coming up.

- Brocade recommends that Converged Mode be enabled on all interfaces connected to CNAs.

- When operating in Converged Mode, tagged traffic on the native VLAN of the switch interface is processed normally. The host should be configured not to send VLAN tagged traffic on the switch's native VLAN.

- The Converged Network Adapter (CNA) may lose connectivity to the Brocade 8000/FCOE10-24 if the CNA interface is toggled repeatedly over time. This issue is related to the CNA and rebooting the CNA restores connectivity.

- Although the Brocade 8000 and FCOE10-24 support the configuration of multiple CEE maps, it is recommended to use only one CEE map on all interfaces connected to CNAs. Additionally, CEE maps are not recommended for use with non-FCoE traffic. QoS commands are recommended for interfaces carrying non-FCoE traffic.

- It is recommended that Spanning Tree Protocol and its variants be disabled on CEE interfaces that are connected to a server.

- The Fabric Provided MAC Address (FPMA) and the Fibre Channel Identifier (FCID) assigned to a VN_Port cannot be associated with any single front-end CEE port on which the FLOGI was received.

- LLDP neighbor information may be released before the timer expires when DCBX is enabled on a CEE interface. This occurs only when the CEE interface state changes from active to any other state. When the DCBX is not enabled, the neighbor information is not released until the timer expires, irrespective of the interface state.

- The FCoE Login Group Name should be unique in a fabric wide FCoE Login Management Configuration. The merge logic is designed to modify the Login Group Name during merge when Login group names in participating configurations conflict with each other. The current OUI of 00051E is being used by Brocade, while assigning the WWNs to 8000s, DCXs and DCX4Ss, which would make only the last 3 bytes as different for any two 8000s, DCXs or DCX4Ss. Considering this assignment method, the merge logic would rename the login group by including the last 3 bytes of WWN in the login group name, so that they are unique in the merged configuration.

- For switches having different OUI indices from the 8 assigned to Brocade (for ex: 00051E and 006069), WWNs can differ in more than 3 bytes. In this case, after normal merge and a rename as per above described logic, login group names can be the same for WWNs differing only in OUIs. The merge logic would drop one of the Login Groups to satisfy the requirement to keep the Login Group Name unique in the fabric wide configuration.

- Ethernet switch services must be explicitly enabled using the command "*fosconfig –enable ethsw*" before powering on an FCOE10-24 blade. Failure to do so will cause the blade to be faulted (fault 9).

- In order to support non-disruptive firmware upgrades on the DCX/DCX-4S, a new service "ethsw" is being introduced to enable Ethernet switching on FCOE10-24 in FOS v6.3. LAN switching is disabled by default in FOS v6.3. The user must explicitly enable Ethernet switch service to prevent FC traffic interruption using the command "*fosconfig –enable ethsw*".

- Upgrading from FOS v6.x to FOS v6.3 is non-disruptive. User can enable ethsw after upgrade without FC traffic interruption.

- The Brocade 8000 does not support non-disruptive hot code loads (HCL). Upgrading the Brocade 8000 from FOS v6.1.2_cee1 to FOS v6.3 or from FOS 6.3 to a later FOS version will be disruptive to the IO through the switch.

- A code load of DCX or DCX-4s with one or more FCOE10-24 blades from FOS 6.3 to another version will disrupt traffic through the blade.

- Upgrades from FOS 6.3 to future releases will be non-disruptive to data traffic and will have behavior similar to a CP failover. "ethsw" remains unchanged.

- Downgrade from FOS v6.3 to FOS v6.1.2_CEEx is **disruptive** if *"ethsw'* is enabled on FOS v6.3.

- Downgrade from FOS v6.3 to FOS v6.1.2_CEEx is non-disruptive if "*ethsw*" has never been enabled with FOS v6.3

- HA Failover of CP blades in DCX or DCS-4s will also result in disruption of traffic through the FCOE10-24 blades.

- Connecting a Brocade 8000 to an FCR-capable switch with fcrbcast config enabled will cause a storm of broadcast traffic resulting in termination of iswitchd.

- When rebooting a DCX or DCX-4S with an FCOE10-24 blade, Qlogic CNA and LSAN zoning, the switch will become very unresponsive for a period of time. This is due to the CNA sending excessive MS queries to the switch.

Virtual Fabrics:

- On Virtual Fabrics capable platforms, the Virtual Fabrics feature must be enabled in order to utilize the related capabilities including Logical Switches and Logical Fabrics. On units that ship with FOS v6.3 installed, the Virtual Fabrics feature is enabled by default on capable platforms.

- When creating Logical Fabrics that include switches that are not Virtual Fabrics capable, it is possible to have two Logical Switches with different FIDs in the same fabric connected via a VF incapable switch. Extra caution should be used to verify the FIDs match for all switches in the same Logical Fabric.

- In order to support non-disruptive Hot Code Load on a Brocade 5100 with VF enabled, the total zoning DB size for the entire chassis should not exceed 1MB.

- A switch with Virtual Fabrics enabled may not participate in a fabric that is using Password Database distribution or Administrative Domains. The Virtual Fabrics feature must be disabled prior to deploying in a fabric using these features.

- Virtual Fabrics is not supported on Brocade 7800.

- VF dedicated ISLs are supported on FX8-24 blade. XISLs are not supported.

- On a Brocade 5100 with Virtual Fabrics enabled, ports may be re-initialized causing frame drops during a hot code load if the switch has a zoning database that is 1MB or larger in size. To prevent this from occurring, ensure the zoning DB is less than 1MB when activating new firmware.

Licensing Behavior:

- When operating a switch with Fabric OS v6.3, some licenses may display as "Unknown." This is due to changes in licensing requirements for some features that no longer require a license key that may still be installed on a switch.

- If a Universal temporary license is enabled for a slot-based license feature, the license expiration date displays as "NA" in Web Tools. Use the **licenseshow** command to display the correct expiration date.

Encryption Behavior for the Brocade Encryption Switch and FS8-18:

- The "*cryptocfg –manual_rekey –all*" command should not be used in environments with multiple encryption engines (FS8-18 blades) installed in a director-class chassis when more than one encryption engine has access to the same LUN. In such situations, use the "*cryptocfg –manual_rekey <CTC> <LUN Num> <Initiator PWWN>*" command to manually rekey these LUNs.

- In the event an HA Cluster is configured within an Encryption Group with containers configured for "auto" Failback Mode, the following procedure must be followed when upgrading from FOS v6.2.x to v6.3.0c. Note: This procedure is only required under the above-mentioned conditions:
    1. Before the firmware upgrade, change the Failback Mode to "manual" for all containers configured as "auto"
        a. Take note of which Encryption Engines currently own which containers
    2. Upgrade all nodes in the Encryption Group to v6.3.0c one node at a time
    3. After all nodes have been successfully upgraded, using the notes taken in step 1a, manually invoke the failback of the containers to the correct Encryption Engine using the following command:
        "cryptocfg –failback –EE <WWN of hosting node> [slot num] <WWN of second node in HAC> [slot num]"
    4. Once the manual failback completes, change the Failback Mode back to "auto" from "manual" if it was changed in step 1

- When adding Nodes to an Encryption Group, ensure all Node Encryption Engines are in an Enabled state.

- When host clusters are deployed in an Encryption environment, please note the following recommendations:
    o If two EEs (encryption engines) are part of a HAC, configure the host/target pair such that they form a multipath from both EEs. Avoid connecting both the host/target pairs to the same EE. This connectivity does not give full redundancy in case of EE failure resulting in HAC failover.
    o Since quorum disk plays a vital role in keeping the cluster in sync, please configure the quorum disk to be outside of the encryption environment.

- During an online upgrade from FOS v6.2.0x to v6.3.0, it is expected to see the IO link status reported as "Unreachable" when the cryptocfg command is invoked. However, once all the nodes are upgraded to v6.3.0, the command will accurately reflect the status of the IO Link. The IO link status should be disregarded during the code upgrade process.

- The "–key_lifespan" option has no effect for "cryptocfg –add –LUN", and only has an effect for "cryptocfg --create –tapepool" for tape pools declared "-encryption_format native". For all other encryption cases, a new key is generated each time a medium is rewound and block zero is written or overwritten. For the same reason, the "Key Life" field in the output of "cryptocfg --show -container -all –stat" should always be ignored, and the "Key life" field in "cryptocfg --show –tapepool –cfg" is only significant for native-encrypted pools.

- The Quorum Authentication feature requires a compatible DCFM release that supports this feature. Note, all nodes in the EG must be running FOS v6.3.0 for quorum authentication to be properly supported.

- In a DCX or DCX-4S with FOS 6.3.0 and FS8-18 encryption blades installed, you must set the quorum size to zero and disable the system card on the blade prior to downgrading to a FOS version earlier than FOS 6.3.0.

- The System Card feature requires a compatible DCFM release that supports this feature. Note, all nodes in the EG must be running FOS v6.3.0 for system verification to be properly supported.

- The Brocade Encryption switch and FS8-18 blade do not support QoS. When using encryption or Frame Redirection, participating flows should not be included in QoS Zones.

- Brocade encryption devices can be configured for either disk or tape operation. The ability to configure multiple Crypto-Target Containers defining different media types on a single encryption engine (Brocade Encryption Switch or FS8-18 Blade) is not supported. FS8-18 Encryption Blades can be configured to support different media types within a common DCX/DCX-4S chassis.

- When using Brocade Native Mode, in LKM installations, manual rekey is highly recommended. If auto rekey is desired, the key expiry date should be configured only when the LUN is created. Never modify the expiry date after configuring a LUN. If you modify the expiry time, after configuring the LUN the expiration date will not update properly.

- SKM is supported with Multiple Nodes and Dual SKM Key Vaults. Two-way certificate exchange is supported. Please refer to the Encryption Admin Guide for configuration information. If using dual SKMs on BES/FS8-18 Encryption Group, then these SKM Appliances must be clustered. Failure to cluster will result in key creation failure. Otherwise, register only one SKM on the BES/FS8-18 Encryption Group.

- When the tape key expires in the middle of write operation on the tape, the key is used to append the data on the tape media. When the backup application rewinds the media and starts writing to Block-0 again and if the key is expired then a new key is created and used henceforth. The expired key thereafter is marked as read only and used only for restore of data from previously encrypted tapes.

- For dual LKM configuration on the Brocade Encryption Switch (BES) or a DCX/DCX-4S with FS8-18 blades as the primary and secondary key vaults, these LKM appliances must be clustered (linked). Failure to cluster will result in key creation failure. Otherwise, register only one LKM on the BES/FS8-18 Encryption Group. Please refer to the Encryption Admin Guide for configuration information.

- The RKM Appliance A1.6, SW v2.5 is supported. The procedure for setting up the RKM Appliance with BES or a DCX/DCX-4S with FS8-18 blades is located in the Encryption Admin Guide.

- Support for registering a 2nd RKM Appliance on BES/FS8-18 is blocked. If the RKM Appliances are clustered, then the virtual IP address hosted by a 3rd party IP load balancer for the RKM Cluster must be registered on BES/FS8-18 in the primary slot for Key Vault IP.

- With Windows and Veritas Volume Manager/Veritas Dynamic Multipathing, when LUN sizes less than 400MB are presented to BES for encryption, a host panic may occur and this configuration is not supported in the FOS v6.3.0 release.

- HCL from FOS v6.2.x to v6.3.0 is supported. Cryptographic operations and I/O will be disrupted but other layer 2 traffic will not.

- Relative to the BES and a DCX with FS8-18, all nodes in the Encryption Group must be at the same firmware level of FOS v6.2 or v6.3 before starting a rekey or First Time Encryption operation. Make sure that existing rekey or First Time Encryption operations complete before upgrading any of the encryption products in the Encryption Group. Also, make sure

that the upgrade of all nodes in the Encryption Group to FOS v6.3.0 completes before starting a rekey or First Time Encryption operation.

- To clean up the stale rekey information for the LUN, follow one of the following two methods:

   Method 1:

- First, modify the LUN policy from "encrypt" to "cleartext" and commit. The LUN will become disabled.

- Enable the LUN using "cryptocfg --enable –LUN". Modify the LUN policy from "cleartext" to "encrypt" with "enable_encexistingdata" to enable the first time encryption and do commit. This will clear the stale rekey metadata on the LUN and the LUN can be used again for encryption.

   Method 2:

   1. Remove the LUN from Crypto Target Container and commit.

   2. Add the LUN back to the Crypto Target Container with LUN State="clear-text", policy="encrypt" and "enable_encexistingdata" set for enabling the First Time Encryption and commit. This will clear the stale rekey metadata on the LUN and the LUN can be used again for encryption

- nCipher / Thales key vault support troubleshooting tips:

   o Regarding NCKA key vault (KV) communication with a Brocade encryption group, the default communication port setting for the NCKA KV is 37208, however, the Brocade encryption members and leader use 9000 so this needs to be reset on NCKA. Additionally, the following is a checklist of things to review if the initial attempt to connect to the KV fails:

      ▪ Check physical and logical connection via a ping on port 9000, this should be the first check.

      ▪ For the group leader node, the kac client cert and the kv cert files are to be identical.

      ▪ For group member nodes the kv file is to be the same as the kv file on the group leader node.

      ▪ Crosscheck to ensure the private key file corresponds to the kac public cert file on any node.

- Host encrypted tape I/O may fail to start when the Primary LKM of an LKM key vault cluster is down. When the primary LKM is down, key creation requests can be rejected by the secondary LKM. NetApp is aware of this issue and is tracking it internally with their defect management tool. The workaround in this case is to wait until the offline LKM comes back online and retry.

- In an environment with a mixed FW version (FOS 6.2.x + 6.3.0) Encryption Group, the IO link state reported for 6.2.x nodes is unreachable. During a rolling upgrade from 6.2.0x release to 6.3.0, it is expected to see the IO link status reported as "Unreachable" when the cryptocfg –show -loc command is invoked. However, once all the nodes are upgraded to the 6.3.0 release, then the show command will accurately reflect the status of the IO Link. The IO link status while performing the rolling upgrade from 6.2.0 to 6.3.0 release can be ignored until all nodes have been upgraded to 6.3.0.

```
Mace39:root> cryptocfg --show -loc


   EE Slot:            0
      SP state:          Online
      Current Master KeyID:   43:f1:bd:dc:91:89:f2:f1:6a:a1:48:89:7b:d0:5f:59
      Alternate Master KeyID: 3a:a4:5b:86:90:d5:69:26:29:78:f8:3b:f9:b2:9c:b9
      HA Cluster Membership:  hac39_115
      EE Attributes:
         Link IP Addr   : 10.32.50.36
         Link GW IP Addr: 10.32.48.1
         Link Net Mask  : 255.255.240.0
         Link MAC Addr  : 00:05:1e:53:8a:86
         Link MTU       : 1500
         Link State     : UP
         Media Type     : DISK
         System Card Label   :
         System Card CID     :

   Remote EE Reachability :
```

Node WWN/Slot State	EE IP Addr	EE State	IO Link
10:00:00:05:1e:53:77:80/0	**10.32.53.107**	**EE_STATE_ONLINE**	**Non-Reachable**
10:00:00:05:1e:53:b7:ae/0	**10.32.53.105**	**EE_STATE_ONLINE**	**Non-Reachable**

Adaptive Networking/Flow-Based QoS Prioritization:

- When using QoS in a fabric with 4G ports or switches, FOS v6.0 or later must be installed on all products in order to pass QoS info. E_Ports from the DCX to other switches must come up AFTER 6.0 is running on those switches.

- Flow based QoS is NOT supported on FC8 blades in the Brocade 48000.

- Any products that are not capable of operating with FOS 6.0 may NOT exist in a fabric with Flow based QoS. Major problems will occur if previous generation 2G products exist in the fabric.

- The resolution for defect 250438 included in this release changes the default behavior of the Adaptive Networking QoS feature. Please refer to the *Documentation Updates* section of this document for further details.

- QoS is supported on AG switches with FOS 6.3.0. The fabric switches should be running 6.3 in order to support QoS. If the fabric switch is 6.2, QoS must be disabled on either switch or AG.

Access Gateway

- When running Adaptive Networking in AG mode note the following:
  - o QoS takes precedence over ingress rate limiting
  - o Ingress Rate Limiting is not enforced on trunked ports.

FCR

- IPFC over FCR is now disabled by default. Switches that are upgraded to FOS v6.3 will retain their configuration settings for IPFC over FCR. The change to the default configuration only applies to new units shipping with FOS v6.3 or units running v6.3 that are reset to a default configuration. Use *fcrbcast - - enable* to explicitly enable IPFC over FCR.

- Broadcast frame forwarding is not supported in an FCR fabric with a Brocade 8000. By default, broadcast frame forwarding is disabled on the FC router. If your edge fabric includes a Brocade 8000, do not enable broadcast frame forwarding on the FC router because this can degrade FCR performance when there is excessive broadcast traffic.

- With FC8 blades, the switch must be disabled to change the backbone fabric ID

- With routing and dual backbone fabrics, the backbone fabric ID must be changed to keep the IDs unique.

- When using FC Routing in a backbone to edge configuration with an Mi10K in the edge fabric, users may experience slow throughput for hosts attached to the Mi10K. Users may encounter this following a bounced IFL connection between the backbone and edge fabric. This slowdown can be resolved by disabling/enabling the Mi10K ports for the hosts that are impacted.

- Mi10K Directors operating with firmware prior to M-EOSn v9.9.5 may experience repeated system faults when attached as an FCR edge switch to a Brocade 7800 EX Port. To avoid this, ensure that the Mi10K is operating with M-EOSn v9.9.5 or later when in an edge fabric that will be attached to a Brocade 7800 FCR Backbone.

FC FastWrite

- When an FC FastWrite Initiator is moved to a port that doesn't have FC FastWrite enabled, I/O will recover and revert to the slow path route (non FC FastWrite). This is a behavioral change from FOS v6.2.x.

Traffic Isolation over FCR

- All switches and Fibre Channel Routers both in edge and backbone fabrics must be running FOS v6.1.0 or later in order to support this feature.

- In order for Traffic Isolation over FCR to function properly, the associated TI zones in each fabric (both edge fabrics and backbone fabric) need to have failover ENABLED.

- TI over FCR is only supported in edge-to-edge configurations. There is no support for TI in backbone to edge routing configurations.

Integrated Routing

- To allow Hot Code Load on a Brocade 5100 when using Integrated Routing, the edge switch connected to the 5100 must be running Fabric OS v6.1 or later code.

- Integrated Routing EX_Ports are only supported in the base switch on a switch with VF enabled.

- Integrated Routing and TopTalkers (Fabric Mode) are not concurrently supported in FOS v6.3. To use Integrated Routing, be sure to disable Fabric Mode TopTalkers prior to configuring EX_Ports first.

Native Connectivity

- FOS-based platforms operating in interopmodes 2 or 3 should never be deployed in a fabric without at least one M-series switch. FOS switches in interopmode 3 (McDATA Open Fabric Mode) do not support configuration of zoning without an M-series switch in the fabric. When migrating from M-series to B-series switches, all B-series switches should be configured to interopmode 0 (Brocade Native mode) once the last M-series switch has been removed from the fabric.

- M-EOSc switches may exhibit a behavior where they block all attached devices with a reason indication of "Blocked Temporarily, Internal". Users that experience this may have power cycled the M-series switch while it was participating in a fabric with Frame Redirection zoning, a capability used for FOS-based application or encryption services . If the switch is still participating in the fabric with Frame Redirection, issue the "cfgsave" command from a Brocade FOS-based switch with the Frame Redirection zone in its defined zone database. If the M-EOS switch is no longer attached to the fabric with Frame Redirection zoning, issue the "Config.Zoning.deleteSplZoneSet" command via CLI to the M-EOS switch.

FCS Automatic Distribution

- When using the FCS Automatic Distribution feature in Fabric OS v6.0 or later, all switches in the fabric must be running FOS v6.0 or later. If any switches are running FOS v5.x or earlier, only manual distribution can be used.

- FOS v6.0 or later will only allow FCS automatic distribution when in strict mode, requiring only switches with FOS v6.0 or later.

FCAP

- Due to limitations with the certificates, FCAP authentication cannot be supported on user defined logical switches. FCAP will continue to function with existing certificates for non-VF and the default logical switch of VF enabled switches. (Note: authutil is not restricted from other logical switches, at this time, so this can still be enabled on unsupported LS.)

- pkicert(1.06) utility may cause evm errors, so each new switch should be isolated from fabric, in non-vf mode, to install new certificates.

- For FIPS mode, certificates need to be installed prior to FIPS activation.

FICON

- Refer to *Appendix: Additional Considerations for FICON Environments* for details and notes for deployment in FICON environments

FL_Port (Loop) Support

- The FC8-48 blade supports attachment of loop devices in the DCX and DCX-4S.

- Virtual Fabrics must be enabled on the chassis and loop devices may only be attached to ports on a 48-port blade assigned to a non-Default Logical Switch operating with the default 10-bit addressing mode (they may not be in the default Logical Switch).

- A maximum of 144 ports may be used for connectivity to loop devices in a single Logical Switch within a chassis.
- Loop devices continue to be supported when attached to ports on the FC8-16, FC8-32, FC4-16 and FC4-32 blades with no new restrictions.

Port Mirroring

- On the Brocade 5300, the port mirroring feature has a limitation where all port mirror resources must stay within the same ASIC port group. The resources are the configure mirror port, Source Device, and Destination Device or ISL, if the Destination Device is located on another switch. The ASIC port groups are 0-15, 16-31, 32-47, 48-63, and 64-79. The routes will be broken if the port mirror resources are spread across multiple port groups.

- Port Mirroring is not supported on the Brocade 7800.

10G Interoperability

- 10G interop between FC10-6 and McDATA blades is not supported due to a HW limitation, however the FC10-6 is supported in a chassis running in Interopmode 2 or 3 (FC10-6 to FC10-6 connections only). An FC10-6 blade will not synchronize with a McDATA 10G blade. However, the inability to synchronize will not negatively impact the system.

Port Fencing

- For Port Fencing, once the trigger threshold is exceeded (e.g. for ITWs or CRCs or LRs), Fabric Watch will wait for approximately six seconds to see if the port is going offline. If it is still online at the next poll cycle, FW will fence the port. Extensive testing has shown that ports that are in the process of going offline may exhibit bursts of errors. Waiting the additional six seconds to check the port status helps prevent false positives and unnecessarily fencing a port (e.g. during a server reboot).

- When using the Port Fencing feature, you must first run the fwalarmsfilterset command. This command enables the port and allows you to receive Port Fencing messages.

- The state changes counter used by Fabric Watch in FOS v6.3 has been updated to ignore any toggling of F-ports due to planned internal mechanisms such as throttling and trunking. There are some FOS CLI commands such as portcfgspeed, portCfgTrunkPort etc that implicitly disable/enable ports after configuration.

- Fabric Watch monitors state change for LISL ports though it is not being displayed in Fabric Watch CLI commands.

- The Port Fencing feature is not supported for Loss of Sync (LOS) and Link Failure (LF) areas of Port/F-port/E-port classes. State change area can be used in place of LOS/LF areas for Port Fencing.

ICLs

- If a DCX with an 8-link ICL license is connected to a DCX with a 16-link license, the DCX with the 16-link license will report enc_out errors. The errors are harmless, but will continue to increment. These errors will not be reported if a DCX with a 16-link license is connected to a DCX-4S with only 8-link ICL ports.

- If ICL ports are disabled on only one side of an ICL link, the enabled side may see enc_out errors.

Extended Fabrics and R_RDY Flow Control

Beginning with Fabric OS v5.1, Brocade supported the Extended Fabrics feature in conjunction with R_RDY flow control (R_RDY flow control mode can be enabled via portCfgISLMode command). R_RDY flow control mode that uses IDLE primitives does not

support Brocade frame-based Trunking for devices such as Time Division Multiplexor (TDM.) In order to overcome this limitation and provide support for frame-based Trunking with Extended Fabrics, Fabric OS v6.2.0 and later has been enhanced to support interoperability with these distance extension devices.

Fabric OS v6.3.0 allows Extended Fabrics E_Ports to operate in VC_RDY mode using either ARB or IDLE primitives as fill words. This allows frame-based Trunking to be supported on Extended Fabrics E-ports even when IDLE primitives are configured for these ports when operating in native VC_RDY mode. Prior to this change, frame-based Trunking was supported only when ARB primitives were used in VC_RDY mode. With Fabric OS v6.2 or later, frame-based Trunking is supported on Extended Fabrics E_Ports regardless of whether IDLE or ARB primitives are used when operating in native VC_RDY mode.

Implementation

The portcfglongdistance CLI parameter "VC Translation Link Init" is now overloaded to specify if the long distance link should use IDLE or ARB primitives. By default, vc_init is enabled. If vc_init is enabled, the long distance link will use ARB primitives. If vc_init is disabled, the link will use IDLE primitives.

Note:

Buffer to Buffer Credit Recovery feature is not supported on Extended Fabrics E_Port when it is configured to use IDLE primitives. The user must disable buffer to buffer credit recovery feature using the command portcfgcreditrecovery and specifying the disable option; otherwise, the link will continuously reset.

The Adaptive Networking SID/DID Traffic Prioritization QoS feature is not supported on Extended Fabrics E_Ports when IDLE primitives are configured on these ports. This is because in this mode only data Virtual Channels are available while QoS related virtual channels are not available.

When connecting to an extension device that does not support ARB primitives (such as some TDM products), the following configuration must be used:

    portcfgqos -disable <port>
    portcfgcreditrecovery –disable <port>
    portCfgLongDistance <port> <LD|LD> 0 <distance>

The fabric parameter "fabric.ops.mode.longdistance" is now deprecated and should not be used.

Miscellaneous

- After issuing an *hafailover* command on a Brocade DCX, DCX-4S, or 48000 running FOS v6.3, the console log may generate continuous "Unknown LSR type" messages. The switch must be rebooted to terminate these messages.

- During non-disruptive firmware upgrades, E_Ports in R-RDY mode may cause some frame drops on the E-port links.

Documentation Updates

This section provides information on last-minute additions and corrections to the documentation. The most recent Fabric OS v6.3.0 documentation manuals are available on the Brocade Partner Network: *http://partner.brocade.com/*. The updates noted in this section are in addition to those included in the Fabric OS v6.3.0a and v6.3.0b Release Notes.

Brocade Fabric OS Command Reference (Publication Number 53-1001337-01)

- On page 215, replace the **priority** operand description for the **fabricPrincipal** command and associated man page with the following text. Note the corrected priority values.

  -priority|-p priority

    Sets the principal selection priority of the switch. The specified priority value is used in the principal switch selection protocol when the fabric rebuilds. Not all of these values can be assigned.

    0x00 Reserved. This value cannot be assigned.

    0x01 Highest priority. This is a user-defined value.

    0x02 Switch was Principle prior to sending or receiving BF (build fabric). This value is generated by the switch to initiate a fabric reconfiguration. This value cannot be assigned.

    0x3 - 0xFE Priority value range. Choose a value in this range to indicate priority. Higher numbers mean lower priority.

    0xFF Switch is not capable of acting as a principal switch. This is a user-defined value. Use **--enable** with a new priority to revert this condition.

Defects

Closed with Code Change in Fabric OS v6.3.0c

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of December 18, 2009 in Fabric OS v6.3.0c

Defect ID: DEFECT000265272	**Technical Severity**: Critical
Summary: Brocade 48000 with FR4-18i cannot see new device across LSAN after upgrade from FOS v5.x non-disruptively all the way to FOS v6.2.x.	
Symptom: Customer unable to bring new devices on line, bounce host port causes path lose between host and target. internal raslog has: [BL-5238], , Pinball Consistency check failure: error = -2, rsc = 1, data1 = -1, data2 = 11, OID:0x43310881, marathon_fcr.c, line: 2296, comp:emd, ltime:2009/09/17-18:47:02:676934; This only applies 4G routers and problem only shows after upgrade to FOS v6.2.x.	
Feature: Field Escalation	**Function**: ASIC Driver
Probability: High	
Found in Release: FOS6.2.0	**Service Request ID**: 402497
Where Else Fixed: FOS6.2.2	

Defect ID: DEFECT000270541	**Technical Severity**: Critical
Summary: On DCX, FCR fails to route traffic on 8G EX ports after code upgrade from FOS v6.1 to FOS v6.2, followed by hafailover and ports activities	
Symptom: DCX running FOS v6.1 with 8G EX ports (Integrated routing, IR) as pre-condition, upgrade to FOSv6.2 based code, if there is additional hafailover, then add new device, bounce device ports could trigger route problem, cause host cannot see device.	
Feature: Field Escalation	**Function**: FCR
Probability: High	
Found in Release: FOS6.2.0	**Service Request ID**: 409197
Where Else Fixed: FOS6.2.2	

Defect ID: DEFECT000269315	**Technical Severity**: High
Summary: Switch panic occurred when 3rd party management application performed repeat FCP LUN emulation queries.	
Symptom: When a 3rd party device gives a bad response to a FCP LUN request, or does not respond at all, FCPD will retry query and stuck the thread. Any new FCP LUN request that comes in from management application will spawn a new thread to handle it. Eventually, FCPD spawns up to the maximum number of allowed threads and the switch panics.	
Feature: Field Escalation	**Function**: Fabric Services
Probability: Low	
Found in Release: FOS6.2.1	**Service Request ID**: 407027
Where Else Fixed: FOS6.2.2	

Closed with Code Change in Fabric OS v6.3.0c

Defect ID: DEFECT000270712	**Technical Severity**: High
Summary: Host failed to discover tapes due to a VI/VT database mismatch between the switches that are part of the same Encryption Group	
Symptom: Host will not able to discovery Tape devices that are part of the same EG	
Workaround: Issue "cryptocfg --commit" again to sync up the VT/VI database across nodes in the EG.	
Feature: Data Security	**Function**: Tape Encryption
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000271290	**Technical Severity**: High
Summary: Brocade 5424 - SERDES settings do not get push correctly on v6.3.0x	
Symptom: Incorrect SERDES settings used.	
Feature: Embedded Platform Services	**Function**: Superhawk2
Probability: Medium	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000273043	**Technical Severity**: High
Summary: When running FCoE feature related scripts over multiple SMIA clients the Common Access Library Daemon (CALD) detects a memory increase on the Brocade 8000 switch. Other FOS based products do not exhibit the same behavior when running the same scripts.	
Symptom: 34MB memory increase seen in Common Access Library Daemon (CALD) when running 10 SMIA clients over FCoE.	
Feature: CEE-MANAGEABILITY	**Function**: CAL INTERFACE
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000267497	**Technical Severity**: Medium
Summary: When CP restarts DPC-0, sassvrd sees ECONNRESET on DPC1 connection and BP freezes for 10 seconds	
Symptom: On one DPC failure, second DPC on the same switch also experience disruption.	
Feature: FA4-18 Platform Services	**Function**: MISC
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000268872	Technical Severity: Medium
Summary: The command fcoe loginshow displays unexpected values when a third party CNA is moved between switches.	
Symptom: Unexpected values are seen in response to the loginshow command.	
Feature: CEE-FCOE	Function: FCOE DRIVER
Probability: High	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000269956	Technical Severity: Medium
Summary: OPT 322202 - IPC failure message displayed on one of the nodes when using the cryptocfg --show -groupmember -all command	
Symptom: Customer will not be able to use "cryptocfg --show -groupmember -all" CLI to know the health of the EG, EEs in the EG when this very remote corner case is hit. However there is no impact to health of EG or EE states in the EG and no impact to any datapath. The health of EG can be determined alternately by issuing "cryptocfg --show -groupcfg" and "cryptocfg --show -localEE" CLIs on each of the Node in the EG	
Workaround: Issue "cryptocfg --show -groupcfg" and "cryptocfg --show -localEE" commands instead to know the health of EG	
Feature: Data Security	Function: Tape Encryption
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000270309	Technical Severity: Medium
Summary: Running FOS commands give error: shmInit: shmget failed: No space left on device	
Symptom: Unable to execute FOS commands on default switch after performing multiple cfgenable with TI zones	
Feature: FC Services	Function: Name Server
Probability: Low	
Found in Release: FOS6.3.0	
Where Else Fixed: FOS6.2.2	

Defect ID: DEFECT000270368	Technical Severity: Medium
Summary: 1GB FCIP tunnel with 2 rate limited circuits is unable to move full I/O workload to remaining circuit when 1 circuit fails.	
Symptom: In a multi circuit FCIP tunnel configuration circuit failover over 1G tunnels may not failover to other available circuits.	
Feature: FCIP	Function: FCIP Performance
Probability: Medium	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000270562	Technical Severity: Medium
Summary: FICON XRC Emulation - READTRACK_STATUS_ACCEPT flag cleared on Tunnel Down and Selective Reset causes Abort Sequences later	
Symptom: Slow read track performance when XRC emulation is enabled, MVS IO errors are generated when an invalid selective reset frame is sent to the controller.	
Workaround: Disable FICON XRC Emulation	
Feature: FCIP	Function: FCIP Performance
Probability: High	
Found in Release: FOS6.2.0	

Defect ID: DEFECT000271177	Technical Severity: Medium
Summary: Additional information of the EE status in the current command that displays the overall status of the EG, nodes and RKM(cryptocfg --show --groupcfg)	
Symptom: Customer will have to invoke "cryptocfg --show -groupcfg", "cryptocfg --show -groupmember -all" or "cryptocfg --show -localEE" on all nodes to know the overall state of EG including EE state across EG. There is no one place where Customer will get the EE state across EG in the same command which provides the EG health	
Feature: Data Security	Function: Infrastructure
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000271220	Technical Severity: Medium
Summary: Unexpected termination of raslogd triggered switch panic or hafailover.	
Symptom: When auditing is on for security class, a race condition in raslogd triggered switch to panic.	
Workaround: disable auditing via: Auditcfg --disable	
Feature: Field Escalation	Function: RAS Logging / Tracing
Probability: Low	
Found in Release: FOS6.1.0	Service Request ID: 409971

Defect ID: DEFECT000272183	Technical Severity: Medium
Summary: IFCCs encountered when processing Read Channel Extender Capabilities with XRC Emulation	
Symptom: IFCCs when IPLing systems with SDM LPARs	
Workaround: Disable FICON XRC Emulation	
Feature: FCIP	Function: FCIP I/O
Probability: Low	
Found in Release: FOS6.2.0	

Closed with Code Change in Fabric OS v6.3.0c

Defect ID: DEFECT000272203	Technical Severity: Medium
Summary: RNID frame type field from the host is corrupted internally when the host is connected over FCIP.	
Symptom: Corrupted RNID request is received from the host and rejected. As a result, the switch is unable to get FICON CHPID online to VSM (Virtual Tape Subsystem) over an emulated or non-emulated VE tunnel. E-Port between switches functions correctly.	
Workaround: Disable FICON Tape Emulation	
Feature: FCIP	**Function**: FCIP Port
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000272842	Technical Severity: Medium
Summary: Switch does not broadcast Unsolicited FIP Discovery Advertisements	
Symptom: If the CNA expects UAs from the FCF even if the solicited advertisement had the "D" bit set, it will logout of the FCF after about 20 seconds.(Tomcat does not logout, Emulex logs out)	
Feature: CEE-FCOE	**Function**: FCOE Daemon
Probability: Low	
Found in Release: FOS6.3.1	

Defect ID: DEFECT000274208	Technical Severity: Medium
Summary: After upgrade to FOS v6.2.x, 4G AP blade observes credit problem on virtual channel 0	
Symptom: Customer after upgrade to FOS v6.2.x, experience frame drop on SAS, FCIP, FC FastWrite and observe host cannot see target, FCIP tunnel do not come up problems.	
Workaround: Port bounce, POR of Brocade 7600. If it is 48K with an FA4-18 blade then port bounce, slotpower off/on of FA4-18 or POR.	
Feature: Field Escalation	**Function**: ASIC Driver
Probability: High	
Found in Release: FOS6.2.1	**Service Request ID**: 412817

Defect ID: DEFECT000274953	Technical Severity: Medium
Summary: Rekey sessions supposed to be pending cannot be persisted when the EE hosting node fails over	
Symptom: Customer will have to restart the rekey individually for those LUNs for which the rekey sessions could not be automatically started if HA Cluster failover happens before keys were successfully created for all LUNs under rekey.	
Workaround: Start the rekey sessions for LUNs on individual basis	
Feature: Data Security	**Function**: Re-key
Probability: Low	
Found in Release: FOS6.3.0	

Closed with Code Change in Fabric OS v6.3.0c

Defect ID: DEFECT000275108	Technical Severity: Medium
Summary: Restore Master Key from recovery cards does not put EE Online when all EEs in the EG were zeroized	
Symptom: When a customer zeroizes all EEs in the EG and restores the Master Key from recovery smart cards will not put EE online	
Workaround: Restore MK the second time.	
Feature: Data Security	Function: Security Processor
Probability: Low	
Found in Release: FOS6.3.0	

Closed with Code Change in Fabric OS v6.3.0b

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of December 7, 2009 in Fabric OS v6.3.0b

Defect ID: DEFECT000259050	**Technical Severity**: Critical
Summary: FICON emulation failing.	
Symptom: MVS IOS444I error messages when trying to vary paths online to extended DASD devices.	
Workaround: Disable FICON XRC Emulation	
Feature: Field Escalation	**Function**: FCIP
Probability: Low	
Found in Release: FOS6.2.0	**Service Request ID**: 389217
Where Else Fixed: FOS6.3.0	

Defect ID: DEFECT000261125	**Technical Severity**: High
Summary: In a large fabric with 50+ switches, firmware download (HCL) on Brocade DCX failed on the standby CP.	
Symptom: In a large fabric with 50+ switches, non-disruptive Firmwaredownload may fail on a standby CP of a DCX switch.	
Workaround: Run firmwaredownload again.	
Feature: FIRMWARE DOWNLOAD	**Function**: Firmware Download
Probability: Low	
Found in Release: FOS6.3.0	
Where Else Fixed: FOS6.2.2	

Defect ID: DEFECT000261231	**Technical Severity**: High
Summary: RASLOG flood occurs with internal RASLOG with following weblinkerfcg message on multiple switches in fabric: "weblinkerfcg:1024 attempts to send message type(26) to invalid dest(IPSIPC:1024/0), comm.c, line: 453, comp:weblinker, ltime:2009/07/28-11:39:	
Symptom: Due to excessive internal messages from one of the applications, other important RASLOG messages may be lost from the limited log space on each switch.	
Feature: FCIP	**Function**: FCIP CP
Probability: High	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000261418	Technical Severity: High
Summary: Panic Reboot on Brocade DCX after using fwshow command.	
Symptom: Switch reboot occurs after running the command "fwshow --disable --port".	
Feature: Field Escalation	Function: Management Services
Probability: High	
Found in Release: FOS6.2.0	Service Request ID: 394347
Where Else Fixed: FOS6.2.2, FOS6.2.1 b	

Defect ID: DEFECT000261593	Technical Severity: High
Summary: Switch went to faulty state after which supportsave takes very long time to complete	
Symptom: Brocade 7600 becomes faulty and supportSave takes very long time.	
Feature: FA4-18 Platform Services	Function: ASIC Driver
Probability: High	
Found in Release: FOS6.2.1	

Defect ID: DEFECT000261797	Technical Severity: High
Summary: Brocade SMI failed to discover all switches over EX port	
Symptom: After hafailover, application fails to discover some switches over EX port due to, SMI reports "LOGIN FAILED" after GPL2 query targeted to translate domain is rejected.	
Feature: Field Escalation	Function: FCR
Probability: Medium	
Found in Release: FOS6.2.0	Service Request ID: 392369
Where Else Fixed: FOS6.2.2, FOS6.2.1 a	

Defect ID: DEFECT000261946	Technical Severity: High
Summary: Upgrade from 6.2.0g to 6.3.0 ldap certificates are missing	
Symptom: Customer may not be able to log into switch when using LDAP authentication.	
Workaround: Log into serial console and reimport the ldap certificate(s). The degree to which the user will be locked out would depend on how the LDAP environment was setup.	
Feature: FOS Security	Function: LDAP
Probability: High	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000263464	**Technical Severity**: High
Summary: Device connectivity lost when zone enabled on Brocade 7800	
Symptom: Lost device connectivity	
Feature: Striker/Spike Platform Services	**Function**: Routing
Probability: High	
Found in Release: FOS6.3.1	

Defect ID: DEFECT000264398	**Technical Severity**: High
Summary: Common Access Layer Daemon (CALD) panics due to segmentation fault	
Symptom: A fabric that contains switches running firmware older then FOS v5.2.x could send an internal query to directors that was not properly set up to handle switches with more than 256 ports. This query can result in the switch with greater than 256 ports.	
Feature: Field Escalation	**Function**: Management Embedded
Probability: Medium	
Found in Release: FOS6.2.0	
Where Else Fixed: FOS6.2.2, FOS6.2.1 b	

Defect ID: DEFECT000265414	**Technical Severity**: High
Summary: Kernel panic when performing POR on DCX	
Symptom: Switch crash and reboot.	
Feature: 8G ASIC Driver	**Function**: C2 ASIC driver
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000265511	**Technical Severity**: High
Summary: Brocade 7800 DP crashed after connecting 10G ports to Anue impairment box	
Symptom: Tunnel does not come up.	
Feature: FCIP	**Function**: FCP TCP/IP Stack
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000265695	**Technical Severity**: High
Summary: Strict fabric wide policy conflict occurs after HA failover	
Symptom: Switch segmented out of fabric.	
Feature: FC Services	**Function**: ESS
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000265697	**Technical Severity**: High
Summary: Block port is not being displayed in IPL file after host blocks port in-band	
Symptom: IPL file is not updated.	
Feature: FICON	**Function**: Ficud
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000265834	**Technical Severity**: High
Summary: RLIR in IM2 fabric is using domain with offset stripped	
Symptom: RLIR or DRLIR generated by FOS did not contain domain offset of 0x60 in PID & TAG fields when running IM2 mode.	
Feature: FICON	**Function**: MS-FICON
Probability: High	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000267476	**Technical Severity**: High
Summary: 7800 panic during overnight workload	
Symptom: 7800 switch crashed and FCIP I/O stopped.	
Feature: Striker/Spike Platform Services	**Function**: Blade Driver
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000267481	**Technical Severity**: High
Summary: Internal FICON error when doing port swap.	
Symptom: Internal FICON error	
Feature: FICON	**Function**: Other
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000269111	Technical Severity: High
Summary: No NPIV devices (including AG) can log into ports of the 7800 when port is changed from EX port to NPIV after non-disruptive upgrade	
Symptom: NPIV ports cannot login.	
Feature: Striker/Spike Platform Services	Function: Spike Platform Module
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000269604	Technical Severity: High
Summary: FICON Emulation not handling Abort Sequence correctly and causing DSO FICON CRC Errors	
Symptom: IO Errors during XRC RRS processing and eventual suspend of the session that encounters the error.	
Workaround: Disable FICON XRC Emulation	
Feature: FCIP	Function: FCIP I/O
Probability: Low	
Found in Release: FOS6.2.0	

Defect ID: DEFECT000246346	Technical Severity: Medium
Summary: During stress testing, after multiple VLAN configuration changes, logins from the CNA are unsuccessful.	
Symptom: Multiple VLAN configuration changes result in FLOGI being ignored.	
Feature: CEE-FCOE	Function: FCOE Daemon
Probability: Medium	
Found in Release: FOS6.1.3_cee	

Defect ID: DEFECT000246883	Technical Severity: Medium
Summary: Pre-FIP LOGO with Invalid WWNN (non-existent fabric device) is accepted	
Symptom: Incorrect device logout.	
Feature: CEE-FCOE	Function: FCOE DRIVER
Probability: High	
Found in Release: FOS6.1.3_cee	

Defect ID: DEFECT000247639	**Technical Severity**: Medium
Summary: Switch responds to FIP FLOGI when SP bit is on and FP bit is off	
Symptom: Incorrect FIP FLOGI response sent by switch.	
Feature: CEE-FCOE	**Function**: FCOE DRIVER
Probability: Low	
Found in Release: FOS6.1.3_cee	

Defect ID: DEFECT000248213	**Technical Severity**: Medium
Summary: FIP FLOGI accepted when host supports only spma	
Symptom: Incorrect FIP FLOGI request is accepted rather than rejected.	
Feature: CEE-FCOE	**Function**: FCOE DRIVER
Probability: Low	
Found in Release: FOS6.1.3_cee	

Defect ID: DEFECT000255703	**Technical Severity**: Medium
Summary: Brocade 8000 floods FCP traffic on two ports to CNAs	
Symptom: Brocade 8000 sends FCP traffic to the wrong CNA.	
Feature: CEE-FCOE	**Function**: FCOE DRIVER
Probability: High	
Found in Release: FOS6.1.2_cee	**Service Request ID**: 384593

Defect ID: DEFECT000257211	**Technical Severity**: Medium
Summary: Weblinker.fcg terminates several times during third party host scan.	
Symptom: When third party host scan was run, http daemon died and restart several times may trigger temporary management service interruption.	
Feature: Field Escalation	**Function**: Web Management
Probability: Medium	
Found in Release: FOS6.2.0	**Service Request ID**: 386535
Where Else Fixed: FOS6.2.2	

Closed with Code Change in Fabric OS v6.3.0b

Defect ID: DEFECT000258696	Technical Severity: Medium
Summary: Switch responds with advertisement to solicitation with SP bit on	
Symptom: Customer will see a response to a solicitation with SP bit on.	
Feature: CEE-FCOE	Function: FCOE DRIVER
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000259855	Technical Severity: Medium
Summary: When FCoE max login has been reached, need to change debug log to customer visible RASLOG, to indicate FCoE login has been reached.	
Symptom: Customer may not know the reason for login reject in case FCoE login limit has been reached.	
Feature: CEE-FCOE	Function: FCOE DRIVER
Probability: Medium	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000261132	Technical Severity: Medium
Summary: In a large fabric with more than 56 switches, edge Brocade DCX panics due to termination of msd during fabric reconfiguration.	
Symptom: While doing switchdisable; agshow; switchenable loop on a large fabric with AG device, switch panics.	
Feature: Fabric Infrastructure	Function: MANAGEMENT SERVER
Probability: Low	
Found in Release: FOS6.3.0	
Where Else Fixed: FOS6.2.2, FOS6.2.1 a	

Defect ID: DEFECT000261754	Technical Severity: Medium
Summary: Observing ffdc data files during continuous interface flap	
Symptom: Interface flapping/ bad cable shows to many ras log messages	
Workaround: Shut down the port and replace the faulty cable and enable the port	
Feature: CEE-Infrastructure	Function: ANVIL DRIVER
Probability: High	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000263948	**Technical Severity**: Medium
Summary: FIP: when CNA send FIP ver=0, switch should not validate MAC descriptor field for backwards compatibility	
Symptom: Switch rejects login due to backward incompatibility.	
Feature: CEE-FCOE	**Function**: FCOE DRIVER
Probability: Medium	
Found in Release: FOS6.3.1	

Defect ID: DEFECT000264578	**Technical Severity**: Medium
Summary: Supportsave did not remove ffdc files. Continued to get ffdc files warning	
Symptom: Supportsave command did not clear FFDC files. FFDC file warning message persisted until a second support save was taken.	
Feature: RAS	**Function**: FFDC/Supportsave
Probability: Low	
Found in Release: FOS6.3.0	**Service Request ID**: 399193
Where Else Fixed: FOS6.2.2	

Defect ID: DEFECT000265225	**Technical Severity**: Medium
Summary: Unsupported SFP amber flashing state is cleared by plugging an optical cable into the SFP. Actual port status is not affected.	
Symptom: An unsupported SFP installed in an FX8-24 can have the amber LED extinguished if a cable is plugged into the SFP. The actual port status is not changed but the visible indication of a fault (flashing amber) is extinguished.	
Feature: Striker/Spike Platform Services	**Function**: Spike Platform Module
Probability: Medium	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000265396	**Technical Severity**: Medium
Summary: Web Tools shows iodset off but CLI shows it is enabled.	
Symptom: Incorrect IOD configuration state is displayed through Web Tools.	
Workaround: Using CLI to view the configured IOD state when IOD is enabled with Lossless DLS	
Feature: WebMgmt	**Function**: WT Platform Support
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000265398	**Technical Severity**: Medium
Summary: Brocade Encryption Switch went faulty during rekey operation	
Symptom: Brocade Encryption Switch faulted, rekey failed and required a power cycle.	
Feature: Data Security	**Function**: Re-key
Probability: Low	
Found in Release: FOS6.2.1	**Service Request ID**: 401091

Defect ID: DEFECT000265399	**Technical Severity**: Medium
Summary: BES did not rejoin Encryption Group after reboot	
Symptom: Encryption switch cannot rejoin Encryption Group resulting in split.	
Feature: Data Security	**Function**: Infrastructure
Probability: Low	
Found in Release: FOS6.2.1	**Service Request ID**: 401091

Defect ID: DEFECT000265530	**Technical Severity**: Medium
Summary: I/O traffic get flooded in to port 16	
Symptom: Incorrect port showing I/O traffic.	
Feature: CEE-Infrastructure	**Function**: ANVIL DRIVER
Probability: Medium	
Found in Release: FOS6.3.1	

Defect ID: DEFECT000265563	**Technical Severity**: Medium
Summary: Web Tools launch fails with license error/doget failed from DCFM	
Symptom: While launching the Web tools, in some corner cases HTTP request for authentication may result in failure. A subsequent Web tools session clears this issue.	
Feature: WebMgmt	**Function**: Webstart
Probability: Medium	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000265753	**Technical Severity**: Medium
Summary: Improve BES error handling when the backend tape target is not responsive	
Symptom: Host cannot recover if backend tape target become not responsive during BES initiated commands.	
Feature: Data Security	**Function**: Tape Encryption
Probability: Medium	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000267358	Technical Severity: Medium
Summary: sfpshow: smart data is not refreshed by polling loop for GE type ports	
Symptom: Newer smart data (for GE type ports) such as SFP temperature and power are not updated by the automatic polling loop that occurs roughly every 5 minutes.	
Feature: Striker/Spike Platform Services	Function: Spike Platform Module
Probability: High	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000267415	Technical Severity: Medium
Summary: Supportsave does not capture all the FID with index greater than 3	
Symptom: Information for FID with index greater than 3 is not captured in supportSave.	
Feature: VF Infrastructure	Function: LS Config CLI
Probability: Medium	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000268955	Technical Severity: Medium
Summary: links on the AG (port 19) went into a disabled state with the reason: "NPIV not supported by Fabric port". However, the edge switch port (7/27) had NPIV enabled.	
Symptom: port on AG switch become disabled.	
Feature: Access Gateway Services	Function: Daemon
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000269138	Technical Severity: Medium
Summary: In the Element Manager, under switch admin, we selected FCoE Login and got an error message of "FCoE Login Management is disabled in the switch; make sure you enable it to view the chassis".	
Symptom: "FCoE Login" tab name causes confusion. It needs to be changed to "FCoE Login Group".	
Feature: WebMgmt	Function: WT Platform Support
Probability: High	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000269286	Technical Severity: Medium
Summary: portdisable xge0 did not actually disable the port although RAS log and switchshow show it is disabled, the FCIP tunnels are still up and running.	
Symptom: xge0 port on FX8-24 is not properly disabled when running portdisable CLI.	
Feature: Striker/Spike Platform Services	Function: BFOS
Probability: Medium	
Found in Release: FOS6.3.1	

Closed with Code Change in Fabric OS v6.3.0a

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of September 28, 2009 in Fabric OS v6.3.0a

Defect ID: DEFECT000263579	Technical Severity: Critical
Summary: Switch panic occurred when management application performed repeat FCP LUN emulation queries through SMI interface or application polling a switch that had password changed multiple times.	
Symptom: Switch panic is experienced. Switch console logs Out of Memory kill.	
Workaround: Disable SMI agents.	
Feature: Field Escalation	**Function**: Panic / OOM
Probability: High	
Found in Release: FOS6.2.1	**Service Request ID**: 399773

Defect ID: DEFECT000247761	Technical Severity: High
Summary: Sysshutdown on Brocade 5480 may cause panic and reboots	
Symptom: Switch panic during sysshutdown	
Workaround: Use CLI "shutdown" command.	
Feature: Embedded Platform Services	**Function**: Bulova
Probability: High	
Found in Release: FOS6.2.0	**Service Request ID**: 375389

Defect ID: DEFECT000254576	Technical Severity: High
Summary: Brocade FR4-18i heartbeat dead causes reboot.	
Symptom: Processor on FR4-18i blade reboots while traffic is running over FCIP links. May cause CP failover to take place, only traffic on the FR4-18i blade is disrupted.	
Feature: Field Escalation	**Function**: FCIP Flipper/ASIC
Probability: Low	
Found in Release: FOS6.2.0	**Service Request ID**: 374539

Defect ID: DEFECT000259327	Technical Severity: High
Summary: After changing domain offset followed by 'hafailover'-"Unknown LSR type" messages started scrolling continuously on console log for Brocade DCX-4S, DCX and 48000 switches running in Interopmode2.	
Symptom: After changing the domain offset, followed by 'hafailover' on CP1, CP0 immediately started posting "Unknown LSR type" messages continuously on console log.	
Workaround: Run hafailover to failover to other CP.	
Feature: FC Services	**Function**: FSPF
Probability: Low	
Found in Release: FOS6.3.0	

Closed with Code Change in Fabric OS v6.3.0a

Defect ID: DEFECT000262164	Technical Severity: High
Summary: Under heavy traffic on 10G tunnel, continuous tunnel modification can cause traffic to halt	
Symptom: FCIP I/O traffic disruption during tunnel modification.	
Workaround: Slot power off/on the Brocade FX8-24 blade.	
Feature: FCIP	**Function**: Compression
Probability: Medium	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000262167	Technical Severity: High
Summary: I/O fails to across VE link when failover is done on a trunked EX port	
Symptom: Medusa I/O on a host connected to storage across a VE link times out and stops when replication software I/O is running across the same link.	
Feature: Striker/Spike Platform Services	**Function**: VEX
Probability: High	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000262247	Technical Severity: High
Summary: Zoning fails with "Transaction Commit failed. Loss of an E-port to a neighboring Mi10k in the middle of a zone push operation caused the zoning request to fail. Zoning fails with "Transaction Commit failed. Reason code 2 (26) - "Aca Was Rejected: Remote Switch Busy, Retry in a few seconds"	
Symptom: Zoning fails with "Transaction Commit failed. Reason code 2 (26) - "Aca Was Rejected: Remote Switch Busy, Retry in a few seconds"	
Workaround: FC Services	
Feature: Zoning	**Function**: Low
Probability: 396077	**Risk of Fix**: (Not Checked)
Found in Release: v6.2.0d	**Service Request ID**: FOS6.2.0
Publications	

Defect ID: DEFECT000262261	Technical Severity: High
Summary: Traffic cannot run across edge to edge topology when compression and FastWrite are enabled.	
Symptom: I/O traffic is unable to run.	
Feature: FCIP	**Function**: FCIP I/O
Probability: High	
Found in Release: FOS6.3.0	

Closed with Code Change in Fabric OS v6.3.0a

Defect ID: DEFECT000262333	Technical Severity: High
Summary: SFP power supply values are not displayed correctly after doing a non-disruptive firmware upgrade to FOS v6.2.1 or FOS v6.3.0	
Symptom: SFP voltage may show incorrect values	
Workaround: Execute the same command again to get the correct values.	
Feature: 8G Platform Services	Function: FOS Kernel Drivers
Probability: Medium	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000262419	Technical Severity: High
Summary: Under impairment, network configuration with high compressible data may result in tunnel bounce	
Symptom: FCIP tunnel may go up and down in an impairment network configuration with highly compressible data I/O.	
Workaround: Tunnel will recover after going down.	
Feature: FCIP	Function: FCP TCP/IP Stack
Probability: Medium	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000262516	Technical Severity: High
Summary: Tunnel did not come up due to configuration mismatch for tape pipelining, one side shows "Write only" and other side shows "Write/Read"	
Symptom: VE tunnel configuration not coming up.	
Feature: FCIP	Function: FCIP CLI
Probability: Medium	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000262891	Technical Severity: High
Summary: Ports go offline with link reset	
Symptom: High CPU load from external SAN management application such as doing supportsave from Brocade DCFM is causing laser flt / link reset on port.	
Feature: 4G ASIC Driver	Function: PORT
Probability: High	
Found in Release: FOS6.2.1	Service Request ID: 397469

Defect ID: DEFECT000263397	Technical Severity: High
Summary: Brocade DCX running FOS v6.2.1 & M6140 running M-EOS v9.9.0 - Nameserver database counts do not match for FOS and M-EOS switches in same fabric	
Symptom: Host cannot see device due to name server has no entries about the device. This happens when there is a HBA capable of RHBA command and EOS (McDATA) switch in the same fabric.	
Feature: FC Services	Function: FDMI
Probability: Medium	
Found in Release: FOS6.2.1	Service Request ID: 398757

Closed with Code Change in Fabric OS v6.3.0a

Defect ID: DEFECT000264566	Technical Severity: High
Summary: Switch panic triggered by size-64 kernel message buffer being used up in virtual fabric with logical ISL configured	
Symptom: Switch panic will be observed. Configuration requires VF with LISL configured. Prior to panic, cat /proc/slabinfo as root will show a large number on size-64 block: slabinfo: size-64 7583624 7583624	
Workaround: Configure only DISLs between switches.	
Feature: Logical Fabric	**Function**: Kernel Driver
Probability: High	
Found in Release: FOS6.2.1	

Defect ID: DEFECT000264640	Technical Severity: High
Summary: Configdownload does download some of the FCoE setting in FOS v6.3.0 that prevents factory install	
Symptom: Prohibit factory install; missing entries are: fcoe.et.cfg:0x0, fcoe.fcmap:0x0 fcoe.fip.advintvl:0x0, fcoe.lg:0x0, fcoe.rcs.gen_number:0x0	
Feature: CEE-FCOE	**Function**: FCOE PROTOCOL
Probability: High	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000264650	Technical Severity: High
Summary: History Buffer is updated according to Port Address rather than Port Number	
Symptom: Port reference provided to FICON host by the Director History Buffer for port parameter changes is incorrect. In reading the switch configuration to gather updates for port parameter changes, FICON host may reference a different port than the one that has changed state.	
Feature: FICON	**Function**: Ficud
Probability: High	
Found in Release: FOS6.3.1	

Defect ID: DEFECT000247754	Technical Severity: Medium
Summary: Brocade switch gets nsd panic in interopmode 3 when running FOS v6.2.	
Symptom: Customer may notice NSd panic	
Feature: Field Escalation	**Function**: Fabric Services
Probability: High	
Found in Release: FOS6.2.0	

Defect ID: DEFECT000253083	Technical Severity: Medium
Summary: Transient detected error on internal link causes blade to be faulted	
Symptom: Port blade will be faulted with "reason=5"	
Workaround: Slotpoweroff and slotpoweron clears the fault	
Feature: 8G ASIC Driver	**Function**: C2 ASIC driver
Probability: Medium	
Found in Release: FOS6.2.0	**Service Request ID**: 378361

Closed with Code Change in Fabric OS v6.3.0a

Defect ID: DEFECT000260664	Technical Severity: Medium
Summary: After downgrading from FOS v6.3.0 to 6.2.0x, the bit count in fwconfigure – Eport – StateChange is 63.	
Symptom: Once the user has a specific Eport StateChange configuration, if the command "fwconfigure – eport – ST" is run after downgrading FOS v6.3.0 to 6.2.0x, the threshold is set at 63. This value is not allowable in FOS v6.2.x since port fencing does not support State change in FOS v6.2.x.	
Feature: Fabric Infrastructure	**Function**: Fabric Watch
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000261654	Technical Severity: Medium
Summary: During non-disruptive upgrade of FOS v6.3.0 on a Brocade5300 switch, "Software 'verify' error seen on console	
Symptom: Software verify error when upgrading between two firmware versions.	
Feature: Fabric Infrastructure	**Function**: Fabric Watch
Probability: Low	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000261978	Technical Severity: Medium
Summary: Retransmit and Out of order counters in portshow fciptunnel output do not show correct values.	
Symptom: Portshow fciptunnel dose not show correct counter value.	
Feature: FCIP	**Function**: FCIP CLI
Probability: High	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000261982	Technical Severity: Medium
Summary: For some reason, if the first tunnel, the first circuit is not numbered 0, portshow fciptunnel all -c will add the line with "16 0 unknwn Disable ----- 0s 0.00 0.00 0 0/0 0"	
Symptom: Incorrect tunnel/circuit number shown.	
Feature: FCIP	**Function**: FCIP CLI
Probability: Medium	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000262329	Technical Severity: Medium
Summary: Configdefault does not delete the FCIP configurations even after chassis reboot.	
Symptom: FCIP configuration cannot be restored to the default setting via configdefault.	
Feature: FCIP	**Function**: FCIP CP
Probability: Medium	
Found in Release: FOS6.3.0	

Closed with Code Change in Fabric OS v6.3.0a

Defect ID: DEFECT000263562	Technical Severity: Medium
Summary: Brocade switch drops frames received from host when the switch is unable to determine a valid state for the back end tape	
Symptom: Frames from host to tape device are dropped by the switch.	
Feature: Field Escalation	**Function**: Encryption
Probability: Medium	
Found in Release: FOS6.2.0	

Defect ID: DEFECT000263775	Technical Severity: Medium
Summary: Switch View:In Striker face plate image, 10GE ports should be renamed as XGE ports.	
Symptom: Different naming for the same port may mislead the user.	
Feature: WebMgmt	**Function**: Switch Explorer/Switch View
Probability: High	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000263805	Technical Severity: Medium
Summary: Ifname for xGIGE ports should show as in CLI.	
Symptom: The ifName value returned for xGIGE port does not match with the CLI output.	
Feature: Mgmt Embedded - SNMP	**Function**: Other
Probability: Medium	
Found in Release: FOS6.3.1	

Defect ID: DEFECT000264469	Technical Severity: Medium
Summary: Support of large ITL nexus in tape to handle multiplex/multistream environment	
Symptom: If the IT (target containers with initiator) is greater than 200, decreased performance is seen for some containers.	
Workaround: Reduce the number of IT configuration (target containers with initiators) to 200.	
Feature: OS Services	**Function**: Linux Kernal
Probability: Medium	
Found in Release: FOS6.3.0	**Service Request ID**: 394589

Defect ID: DEFECT000264871	Technical Severity: Medium
Summary: NS does not send subsequent PLOGI ACC following a sequence where NPIV device sends LOGO before link down.	
Symptom: NPIV tape devices may not be seen by any of the hosts	
Feature: FC Services	**Function**: Name Server
Probability: Medium	
Found in Release: FOS6.3.0	**Service Request ID**: 397897

Closed with Code Change in Fabric OS v6.3.0a

Defect ID: DEFECT000264971	Technical Severity: Medium
Summary: Unlike FC ports, GE ports will stick at No_Sync when you swap Invalid/Non-Brocade branded SFP to Valid Brocade SFP.	
Symptom: GE ports will not come on line if unsupported SFP have been plugged in previously.	
Workaround: Portdisable and portenable after inserting supported SFP.	
Feature: Striker/Spike Platform Services	**Function**: BFOS
Probability: Medium	
Found in Release: FOS6.3.0	

Defect ID: DEFECT000265149	Technical Severity: Medium
Summary: SFP hot-plug: Copper SFP can get into illegal state: Port State=Online and Port Phys=No_Light and link led=OFF	
Symptom: Copper SFP on 7800 shows no LED light, while port is online and working.	
Feature: Striker/Spike Platform Services	**Function**: Spike Platform Module
Probability: Low	
Found in Release: FOS6.3.0	

Appendix: Additional Considerations for FICON Environments

This appendix includes supplemental information for users deploying FOS-based platforms in FICON environments.

- The DCX-4S is only supported for FICON in Brocade Native Mode (interopmode 0) and therefore is not supported for interoperability with M-EOS platforms.

- For FICON environments, The 8-link ICL license was only qualified for DCX-4S to DCX-4S or DCX-4S to DCX configurations. It is not FICON qualified for DCX to DCX configurations.

- Note: Multiple 10 Gb/sec ISLs and FCIP links can load-share between cascaded FICON directors/switches but do not load balance in a FICON configuration.

Area	Comments

8Gb/sec Links	Depending on the fulfillment method, the default fill word may be set to IDLE or ARB(FF). The fill word is changed using the portcfgfillword command. Although the fill word is always IDLE when ports log in at less than 8Gb/sec, executing the portcfgfillword command is disruptive regardless of what speed at which the ports log in. Brocade recommends ARB(FF) except for the following devices which require the fill word to be set to IDLE:
	
	    • IBM SVC
	    • EMC DASD

Firmware Downloads	Non-disruptive Hot Code Load is only supported on director class switches (48000, DCX, and DCX-4S). Non-disruptive Hot Code Load is not supported on the 5100, 5300, 7500, and 7800. IFCCs may result if traffic is not stopped while downloading firmware.
Firmware Downloads	Replacement of a CP card in the Brocade 48000 may cause disruption of I/O traffic. Brocade recommends that the CP be replaced during a scheduled downtime to prevent disruption in FICON environments.
Firmware Downloads	The CUP device must be varied offline to all MVS partitions before starting a code load. The CUP device can be varied back online after the code load completes. Failure to vary off the CUP devices may result in a CP panic.
Manageability	In a mixed fabric environment, an M-EOS switch must be principal switch if the fabric is in Interopmode 2 (McDATA Fabric Mode).
Manageability	It is suggested that Port Fencing be used to avoid taking ports down for normal fabric events. The recommended fencing criteria and settings are: {fencing_table}

Fencing criteria table:

Criteria	Value
ITW (Invalid Transmission Words)	25
CRC (Cyclical Redundancy Check)	3
LOS (Loss of Sync)	2
Protocol Errors	2

Area	Comments
Manageability	Firmware download is executed sequentially if ECFM is used for downloading code to FOS switches.
Manageability	As a "Best Practice" for deploying FOS switches/directors into a FICON environment, verify the FOS version shipped with the most current FOS recommendation. It is recommended to update all FOS switch/directors to the same FOS levels for production.
Manageability	The remote CUP may not work when the channel is connected to an 8G blade on a 48000 cascaded to a remote switch.
Manageability	FMS must be enabled on the local switch for the remote CUP to work.
Optics	Brocade recommends using 50 micron multimode fiber optic cabling rated at 2000 MHz-km (OM3 fiber) for connecting to 8 Gb/sec short wavelength (SX) small form factor pluggable optics (SFPs). Other 50 micron and 62.5 micron multimode fiber may be used as an alternative, but distance limitations may exist.
Serviceability	Performance of optical links depends upon the cleanliness of the cables and connectors, especially at 8 Gb/sec or higher speeds. Consult with your switch and cable vendors for proper cable maintenance.
Serviceability	The 48 port blade (FC8-48) is supported as follows: • The switch, or logical switch, must be configured for Brocade Native mode (interopmode 0). • It is only supported on VF enabled chassis on the DCX. • It is not supported in the default switch on the DCX.
Traffic Isolation Zones	Enable Lossless DLS when activating Traffic Isolation (TI) Zones to avoid any traffic disruption.
Traffic Isolation Zones	Traffic Isolation (TI) Zoning with FICON supports enabling or disabling of the failover option. Assistance from service support should be sought before attempting to enable this feature.