Brocade Fabric OS v6.4.0a
Release Notes v2.0

June 29, 2010

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v6.4.0a Release Notes v1.0	Initial Release	June 4th, 2010
Brocade Fabric OS v6.4.0a Release Notes v2.0	Updated FICON Appendix, minor corrections in Important Notes, additional Bottleneck Detection details.	June 29th, 2010

Copyright © 2001 - 2010 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, Fabric OS, File Lifecycle Manager, MyView, and StorageX are registered trademarks and the Brocade B-wing symbol, DCX, and SAN Health are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: The information in this document is provided "AS IS," without warranty of any kind, including, without limitation, any implied warranty of merchantability, noninfringement or fitness for a particular purpose. Disclosure of information in this material in no way grants a recipient any rights under Brocade's patents, copyrights, trade secrets or other intellectual property rights. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

Notice: The product described by this document may contain "open source" software covered by the GNU General Public License or other open source license agreements. To find-out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit *http://www.brocade.com/support/oscd*.

Export of technical data contained in this document may require an export license from the United States Government.

Contents

Quick Look

If you are already using the most recent version of the Fabric OS v6.4.0 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 v6.4.0a since the release of Fabric OS v6.4.0
- An appendix related to FICON interoperability has been added at the end of the Release Notes

Overview

New Hardware Support

Brocade Fabric OS (FOS) v6.4.0 supports the following new hardware platforms:

- **Brocade FC8-64: 64-port 8Gb Fibre Channel blade for the DCX and DCX-4S**
  - Supports E, EX, F, FL and M-port types
  - Supports auto sensing 2/4/8 Gbps port speed
  - Needs special type of SFPs called mSFPs

- **VA-40FC: Virtual Access 40FC platform support on a major FOS release**
  - VA-40FC was originally launched on FOS v6.2.1_vfc focused release
  - Also supported on FOS v6.2.2 and FOS v6.3.1 maintenance releases

Summary of New Software Features

In addition to support for the new hardware, there are several new features and enhancements in FOS v6.4.0, including:

- FCIP Enhancements
  - IPsec support on FX8-24 blade
  - IPV6 support on 7800 and FX8-24 FCIP ports
  - VEX support on FX8-24
  - DSCP Marking support on FX8-24 and 7800
  - Support for up to 4 FX8-24 blades in DCX and DCX-4S
  - Troubleshooting Enhancements (tperf diagnostic CLI)
- Encryption Platform Enhancements
  - Concurrent Disk and Tape Encryption support on the same Encryption Engine
  - Disk device decommissioning support
  - Redundant Key ID metadata option in data replication environments
- Bottleneck Detection Enhancements
  - Support for congestion detection on E, EX and F-ports. This is in addition to the latency bottleneck detection feature introduced in FOS v6.3
  - Support for bottleneck detection alerts through SNMP traps and RAS logs
  - Support for switch-wide enablement of both latency and congestion bottleneck monitoring
- Enhanced Traffic Isolation Zones
  - Support for common devices in multiple TI zones with failover disabled or failover enabled
  - Allow devices in a failover disabled TI zone to communicate with local devices (devices attached to the same switch) that are not part of the same TI zone
  - Ensure that Domain Controller connectivity between switches in a fabric will not be affected by TI zone policies
- Lossless DLS Enhancements
  - Support for Lossless DLS with DPS (Exchange based routing)
  - Option to specify IOD (In Order Delivery) with port based and exchange based routing policies

- Access Gateway Enhancements
    - Ability to map individual NPIV WWN to N-port (also known as Device-based mapping)
    - Ability to balance WWN logins from a single NPIV-port across multiple N-ports of an Access Gateway
    - Ability to configure NPIV login limit for individual ports (this feature is supported both on Access Gateway and Switch ports)
- Virtual Fabrics Enhancements
    - Dynamic Area Addressing support for the Default Switch in DCX and DCX-4S
- Security Enhancements
    - Support FCAP authentication using third-party self signed certificates

- Fabric Watch Enhancements
    - New non-menu-driven CLI thConfig to configure thresholds for Fabric Watch classes
- FCoE/CEE Enhancements
    - Support for IGMP snooping functionality on Brocade 8000 and FCOE10-24 blade
- RAS/Diagnostics/Troubleshooting Enhancements
    - Frame Monitoring
        - Ability to monitor individual frame types such as SCSI Reservation, Basic Accept, Basic Reject, SCSI READ, SCSI Write, etc. and configure thresholds via fmConfig and thConfig CLIs
    - Super Ping
        - Enhancements to the FC ping functionality to provide more coverage of multiple data paths that exist between a source domain and destination device
    - Rolling Reboot Detection (RRD)
        - Ability to detect unexpected continuous reboot condition of switches

New Feature Descriptions

FCIP Enhancements

The following FCIP related enhancements are made in FOS v6.4.0:

- **IPsec support on FX8-24 blade**
  FOS v6.4.0 adds IPsec support for the FCIP tunnels on FX8-24 blade. IPsec is supported on the FCIP tunnels configured on 1GbE and 10GbE ports of the FX8-24 blade.

- **IPv6 support on 7800 and FX8-24 FCIP ports**
  FOS v6.4.0 adds IPv6 support for 1GbE/10GbE FCIP ports on the FX8-24 blade and on the 1GbE ports on the 7800 platform.

- **VEX support on FX8-24**
  FOS v6.4.0 release adds support for the VEX ports on the FX8-24 blade in both VF enabled and VF-disabled modes.

- **DSCP Marking support on FX8-24 and 7800**
  FOS v6.4.0 release enables DSCP marking support on FX8-24 blade and 7800 platform. The Differentiated Services Code Point (DSCP) is a way of classifying traffic to allow network administrators to determine the per-hop behavior of any given IP packet.

- **Support for four FX8-24 blades per chassis**
  FOS v6.4.0 has increased the support for the maximum number of FX8-24 blades supported in a DCX/DCX-4S chassis from 2 to 4.

- **Troubleshooting Enhancements - New tperf diagnostic CLI**
  FOS v6.4.0 adds support for a new FCIP diagnostic CLI tperf. This tperf CLI can be used to determine tunnel characteristics, generate High, Medium, Low priority traffics , generate random traffic patterns, enable payload CRC checks, test with different PDU sizes, etc.

Encryption Enhancements

The following software enhancements are made to the Encryption platforms (BES and FS8-18) in FOS v6.4.0:

- **Concurrent Disk and Tape Encryption support on the same Encryption Engine**
  This feature allows users to configure disk and tape containers on the same Encryption Engine (EE). In pre-FOS v6.4.0, users needed to dedicate an Encryption Engine either for disk encryption or tape encryption. This restriction is lifted in FOS v6.4.0. However, users must note that the encryption performance could be lower when both disk and tape encryptions are concurrently performed on the same Encryption Engine, when compared to a scenario where an Encryption Engine would be performing either disk or tape encryption exclusively.
- **Disk device decommissioning support**
  This feature provides the ability to render all encrypted data on a disk to be made irrecoverable before a disk is decommissioned. This is achieved by ensuring that the encrypted data on a disk cannot be decrypted by any means.
- **Redundant Key ID metadata option in data replication environments**
  FOS v6.4.0 has been enhanced to perform key recovery operation in data replication environments.

Bottleneck Detection Enhancements

FOS v6.4.0 **enhances bottleneck detection** capability by adding **support for congestion detection at E, Ex and F ports.** Bottleneck monitoring configuration has been greatly simplified in FOS v6.4.0 by allowing switch-level enablement of this feature for both latency and congestion bottleneck monitoring. New enhancements allow users to configure separate thresholds for detecting latency bottleneck and congestion bottleneck conditions. Bottleneck monitoring alerts can be configured on a per port basis and are delivered through SNMP traps and RAS logs.

FOS v6.3.1b introduced several changes and enhancements that are also included in FOS v6.4. These changes are not fully documented in existing Admin Guides or other materials but will be captured in future documentation and existing documentation updates and revisions. A brief summary of these enhancements follows:

- General improvements to Bottleneck Detection on both 4G and 8G platforms including **improved accuracy on reporting latency** and **reporting of latency values** in Bottleneck Detection events.
- **Identify credit lost condition** on 4G and 8G E_Ports and generate a RASLOG message (C2-5021) when detected. Unlike previous reporting that indicated when all credits for a VC were missing, this new capability reports on individual credit loss. This capability is enabled by default and is not configurable.
- New **option to configure the switch** "**edge hold time,**" allowing the switch to timeout frames for F_Ports sooner than for E_Ports. Proper use of this capability (disabled by default) reduces the likelihood of devices with high latencies causing frame drops in the core of the fabric and impacting other unrelated flows. Details on usage and recommended settings will be available in separate documentation.
- Support for **Class 3 frame transmit (Tx) timeout discard counters on 4G platforms** (previously 4G platforms only supported receive (Rx) timeout counters, reference Fabric Watch Administrator's Guide for details on use and configuration).

The Bottleneck Detection feature does not need any additional license and is available on all 4G and 8G capable platforms.

Enhanced Traffic Isolation Zones support

Several **enhancements** are made to the **TI zone functionality** in FOS v6.4.0. Though these enhancements are mainly targeted for FICON environments, they can be used in both FICON and Open Systems environments.

These changes include:

- Allow same device ports to be part of multiple TI zones with failover disabled or failover enabled.
- Allow devices in a failover disabled TI zone to communicate with local devices (devices attached to the same switch) that are not part of the same TI zone.
- Ensure that Domain Controller connectivity between switches in a fabric will not be affected by TI zone policies.

Lossless DLS Enhancements

- Lossless DLS enables Dynamic Load Sharing for optimal utilization of the ISLs without causing any frame loss. Note that "No frame loss" can be guaranteed only when a new additional path is used to do load rebalance. "No frame loss" cannot be guaranteed on an existing data path that encounters failure.
- **FOS v6.4.0 adds support for the Lossless DLS with DPS (Exchange based routing).** The In Order Delivery (IOD) capability can be enabled optionally for both Port Based Routing and Exchange Based Routing policies. In pre-FOSv6.4.0 Lossless DLS feature was supported only for Port Based Routing and IOD was always enabled.

Access Gateway Enhancements

The following enhancements are made to the Access Gateway functionality in FOS v6.4.0:

- **Device-based Mapping**
  This feature allows mapping of individual NPIV logins to individual N-ports of an Access Gateway. Even if an NPIV device logs in through a different F-port of an Access Gateway it stays mapped to the same N-port. This feature also supports the N-port failover policy.

- **WWN to N-port Load Balancing**
  FOS v6.4.0 implements a new WWN to N-port load balancing policy for Access Gateway. When enabled, this policy allows future allows NPIV logins to be automatically distributed uniformly within a port group.

- **Individual Port Level NPIV Limit Configuration**
  In FOS v6.4.0 individual ports can be configured with unique NPIV login limits. This feature provides more flexibility to deploy Virtual Machines based on real world needs by allowing more NPIV logins through some ports than others. This feature is supported in both Access Gateway and Switch modes.

Virtual Fabrics Enhancements

FOS v6.4.0 adds **support for the Dynamic Area Addressing for the Default Switch in DCX and DCX-4S when VF is enabled**. This enables several capabilities in the Default Switch in DCX and DCX-4S which could not be supported in pre-FOS v6.4.0 releases. These capabilities include ability to assign any area to a port without doing portswap, support for WWN based PID assignment in the Default Switch, port mirroring support for devices directly attached to FC8-48 and FC8-64 ports in the Default Switch and maximum NPIV limit support of 255 devices per port for FC8-48 and FC8-64 ports within the Default Switch.

RAS/Diagnostics/Troubleshooting Enhancements

Frame Monitoring
This feature **enhances configuration of existing filter based monitors** supported by APM (Advanced Performance Monitor) and Fabric Watch monitoring for filter based monitors. It provides a common interface *fmConfig* for defining frame monitors and configuring thresholds, and alerts for individual frame types. This feature allows users to monitor various types of frames such as SCSI Reservation, Basic Accept, SCSI Read, SCSI Write, etc. Alerting is supported via RASLOGs, SNMP traps and email alerts.

FC Ping Enhancements (Super Ping)
FOS v6.4.0 enhances the FC ping functionality to run sanity tests (ping) all data paths between a source domain and destination device.

Rolling Reboot Detection
FOS v6.4.0 implements the ability detect rolling reboot condition. Rolling reboot is an extremely rare and unexpected reboot condition where a switch reboots continuously. Once Rolling Reboot condition is detected, system stops booting FOS and enables users to login to the switch and gather supportsave information for failure analysis.

Security Enhancements

FOS v6.4.0 adds support for FCAP authentication using third-party self signed certificates. Starting with FOS v6.4.0 both Brocade issued certificates and/or third-party self signed certificates can be used for FCAP authentication. Prior to FOS v6.4.0 only Brocade issued certificates were supported.

Fabric Watch Enhancements

- FOS v6.4.0 introduces a **new non-menu-driven** CLI *thConfig* to configure thresholds for Fabric, Security, SFP, Filter and EE classes. The functionality supported by the thConfig CLI is equivalent fwConfigure CLI except that fwConfigure is menu driven. Users are encouraged to use thConfig CLI as fwConfigure CLI will be deprecated in future releases.
- Sysmonitor CLI has been enhanced to support flash and temperature monitoring in FOS v6.4.0.

CEE Enhancements

FOS v6.4.0 adds support for IGMP snooping functionality on Brocade 8000 and FCOE10-24 blade. This implementation supports IPv4 version of IGMP v1/v2. IGMP Snooping allows multicast data to be forwarded to only interested member ports of a VLAN.

Deprecated Features

- **FAL API**
  FOS v6.4.0 no longer includes FAL API support. Equivalent functionality is available through the following SMI-S agents:
  - SMI-S 120.11.0
  - DCFM 10.4 Professional Plus and DCFM 10.4 Enterprise editions.
    Option to install only SMI-S without DCFM client capabilities is also supported.

Optionally Licensed Software

There are no new licenses introduced in FOS v6.4.0. Optionally licensed features in Fabric OS v6.4.0 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).
- **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, VA-40FC (in switch mode), 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 license enables all eight FC ports on the Brocade 8000. This license should always be installed with the FCoE license.
- **7800 Port Upgrade** — This 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 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 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:
    - 10 1GbE ports and 1 10GbE port, or
    - 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 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 license
- Advanced Extension license
- Advanced FICON Acceleration license
- 10GbE FCIP license

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

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
- FICON Management Server (CUP) license

Supported Switches

Fabric OS v6.4.0 supports the Brocade 300, 5410/5424/5450/5460/5470/5480/NC-5480, 4100, 4900, 5000, 5100, 5300, VA-40FC, 7500/7500E, 7600, 48000, Brocade Encryption Switch (BES), DCX/DCX-4S, 8000, and the 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 and DCX/DCX-4S with one or more FCOE10-24 blades.

Access Gateway mode is also supported by Fabric OS v6.4.0, and is supported on the following switches: the Brocade 300, 5100, VA-40FC, 8000, 5450, 5460, 5470, 5480, NC-5480 and M5424.

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 and associated files
   - 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, VA-40FC, 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.

FOS Migration Considerations

This section contains important details to consider before migrating to or from this FOS release.

TSBs - Critical Issues to Consider Prior to Installing This FOS Release

Technical Support Bulletins (TSBs) are produced to provide detailed information about high priority defects or issues present in FOS releases. The following sections specify all current TSBs that have been identified as being a risk to or resolved with this specific version of Fabric OS. Please review carefully and refer to the complete TSB for relevant issues prior to migrating to this version of code. TSBs can be found at http://my.brocade.com under the "*Technical Documentation*" section of the "*documentation*" tab.

TSB Issues Outstanding in FOS v6.4.0a

Issues in the following list of TSBs are known to be potential risks to using FOS v6.4.0a and should be considered carefully prior to using this release of code:

TSB	Summary
None	There are no current TSBs outstanding for this FOS release.

TSB Issues Resolved in FOS v6.4.0a

Issues in the following list of TSBs are known FOS v6.4.x risks that are not exposures in FOS v6.4.0a. Note that the issues addressed in this list of TSBs may also be resolved in other FOS releases. Refer to the specific Release Notes for each release to verify resolution details.

TSB	Summary
None	There are no TSBs currently issued for FOS v6.4 releases.

Recommended Migration Paths to FOS v6.4.0a

Migrating from FOS v6.2.x

For units currently operating at FOS v6.2.x, it is recommended to use FOS v6.3.0d, 6.3.1b (or later) or v6.3.2 prior to migrating to FOS v6.4.0a.

Migrating from FOS v6.3.x

For units currently operating at FOS v6.3.x, there are no special steps required to migrate to FOS v6.4.0a.

FOS Upgrades and Downgrades

Upgrading to Fabric OS v6.4.0 is only allowed from Fabric OS v6.3. 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.

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 to FOS v6.4 will be disruptive to the IO through the switch.

A code load of DCX or DCX-4s with one or more FCOE10-24 blades will disrupt the traffic going through those FCOE10-24 blades.

Disable the ports in DCX Logical Switches that **use 10 bit addressing mode that have 8 bit areas in the range 0x70-0x8F before upgrading to FOS v6.4.0**. Otherwise firmware upgrade will fail with an error message. This step is necessary even if users do not plan to use FC8-64 blades after performing firmware upgrade to FOS v6.4.0. However, if areas 0x70-0x8F are not in use this step is not necessary. Please use portAddress CLI to find out the areas in use within a Logical Switch.

If **Bottleneck detection feature is currently enabled** on the switch running FOS v6.3.x, you must **disable it before upgrading to FOS v6.4.0**; otherwise, frame drops may occur due to increased Hot Code Load (HCL) time.

7800 platform and FX8-24 blade must be power cycled after upgrading from FOS v6.3 to FOS v6.4. This is necessary to load the new FPGA image that enables IPv6 capability for FCIP links to 7800 and FX8-24 blade. This step is mandatory even if IPv6 will not be used on the FCIP ports. Not performing this step will result in unpredictable behaviors on the FCIP links. Please note that in the case of FX8-24, only the FX8-24 blade needs to be power cycled and not the entire DCX/DCX-4S chassis.

Important Notes

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

DCFM Compatibility

FOS v6.4 is compatible with Brocade's Data Center Fabric Manager (DCFM) v10.4 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 legacy Brocade management products (Brocade Fabric Manager (FM) and Brocade Enterprise Fabric Connectivity Manager (EFCM)).

DCFM 10.4 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 and up to 1,000 switch ports. It 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 or departmental SANs for managing up to four physical or virtual fabrics (FOS, M-EOS and Mixed fabrics) and up to 2,560 switch ports. It supports Brocade backbone and 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.
- ***DCFM Enterprise*:** a management application designed for enterprise-class SANs for managing up to 24 physical or virtual fabrics and up to 9,000 switch ports. DCFM Enterprise supports all the

hardware platforms and features that DCFM Professional Plus supports, and adds support for the Brocade DCX Backbone and Fiber Connectivity (FICON) capabilities.

DCFM 10.4 now includes introductory support for FOS switches or fabrics using Administrative Domains (ADs). These details and more about DCFM's new enhancements can be found in the DCFM 10.4 Release Notes, DCFM 10.4 User Guide, and DCFM 10.4 Installation, Migration, & Transition Guide.

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 and later firmware versions**. 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. Similar issues are anticipated to be present when managing FOS v6.4 with FM.

WebTools Compatibility

FOS v6.4 is supported with JRE 1.6.0 Update 16.

SMI Compatibility

- FOS v6.4 is supported with SMI-S agent 120.11.0.
- FOS v6.4 is supported with SMI-S Agent integrated with DCFM 10.4

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.

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 5470	v6.3.1 and later
Brocade 5410, 5480, 5424	v6.2.0 and later
Brocade 8000	v6.1.2_CEE1 or later
Brocade 7800, DCX and DCX-4S with FCOE10-24 or FX8-24 blades	v6.3 and later
Brocade DCX and DCX-4S with FC8-64 blade	v6.4
Brocade DCX, 300, 5100, 5300	v6.1.0e and later [5]
VA-40FC	v6.2.1_vfc, v6.2.2, v6.3.1, v6.4
Brocade DCX-4S	v6.2.0 and later
Brocade DCX with FS8-18 blade(s), Brocade Encryption Switch	v6.1.1_enc and later
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 v6.4, but may not be directly attached via E_Port to any products running FOS v6.4. 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 9.7.2 is the minimum version of firmware that is supported to interoperate with FOS 6.4. 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.

Blade Support

Fabric OS v6.4.0 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. **Note:** FC8-64 is not supported on 48000.
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.

48000 Blade Support Matrix	
Encryption Blade (FS8-18), Extension Blade (FX8-24), FCoE/CEE Blade (FCOE10-24)	Not supported.

Fabric OS v6.4.0 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, 48 and 64-port 8Gbit port blades (FC8-16, FC8-32, FC8-48, FC8-64) and the 6-port 10G FC blade (FC10-6)	16, 32 and 48 port blades are supported with FOS v6.0 and above with any mix and up to 8/4 of each. 64 port blade is supported starting with FOS v6.4.0 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.
Encryption Blade (FS8-18)	Up to a maximum of 4 blades of this type.
Extension Blade (FX8-24)	Up to a maximum of 4 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). Cannot be used in a DCX/DCX-4S chassis with FC8-64 blade in FOS v6.4.0.

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, FC8-16, FC8-32, FC 8-48, *FC8-64*[1]	Port Blade	4 Power Supplies	Not Supported	2 Power Supplies	
FR4-18i, FC4-16IP[2], FA4-18	Intelligent Blade	4 Power Supplies	Not Supported	2 Power Supplies	
FS8-18, FX8-24, FCOE10-24	Intelligent Blade	N/A	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 blades, (1+1) 220VAC Power Supplies are required for redundancy.

[1] FC8-64 is not supported on 48K

[2] FC4-16IP is not supported on 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 v6.4 support both interopmodes 2 and 3 with the exception of the Brocade 4100 and 8000 and DCX/DCX-4S with one or more FC0E10-24 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 v6.4.

FOS Features (supported in interopmode 0)	**FOS v6.4**	
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*
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

FOS Features (supported in interopmode 0)	**FOS v6.4**	
IM = Interopmode	**IM 2**	**IM 3**
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
Lossless DLS	No	No

* 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.

SAS Version Requirements for FA4-18 and Brocade 7600

Note: The SAS firmware version compatible with FOS v6.4.0 will be announced at a future date.

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

Management Server Platform Capability support changes in FOS v6.4

FOS v6.4.0 no longer automatically enables the Management Server (MS) Platform capability when a switch attempts to join a fabric that has these services enabled. This prevents a FOS v6.4.0 switch from joining such a fabric, and ISL will be disabled with a RAS log message. To allow a FOS v6.4.0 switch to join such fabrics msPlMgmtActivate command should be used to enable the Management Server platform services explicitly.

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

- IPsec is not supported on XGE0 of FX8-24 blade in FOS v6.4.0. IPsec is supported on XGE1 and GE0 through GE9.
- IPsec is supported on FCIP tunnels that use only IPV4 connections.
- FICON networks with FCIP tunnels do not support DPS (aptpolicy 3) configurations. This applies to both emulating and non-emulating FCIP tunnels.
- The maximum supported MTU size for the Brocade 7800/FX8-24 is 1500 with FOS v6.4.0.
- 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 multiple FCIP tunnels are present on a switch and additional circuits (and the network bandwidth provided by those circuits) are added to an already active tunnel, there may be 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). FOS 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 and FX8-24) modes 2 and 3 are only supported in Open Systems environments.
- In order to perform the following operations it is necessary to delete the FCIP configuration on the affected ports first:
    - Switching modes between 1G/10G/Dual.
    - Moving VE/GE port between logical switches.
- ARL (Adaptive Rate Limiting) is not supported on 10G tunnels.
- "Inband Management" is not supported on the Brocade 7800.
- FOS v6.4.0 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 v6.4 will disrupt I/O traffic on FCIP links.
- Differences between the Brocade 7800/FX8-24 platforms and previous generation 7500/FR4-18i platforms include:
    - On the 7800, the GbE port does not directly correlate to a VE port
    - 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
    - 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 v6.4 for details
- 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.
- Latency measurements supported on FCIP Tunnels (Tested limit under FOS v6.3.1):
    - 1GbE - 200ms round trip time and 1% Loss
    - 10GbE – 100ms 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.
- After inserting a 4G SFP in GE ports of an FX8-24 blade or 7800 switch, sometimes "sfpshow" output might display "Can not read serial data!" . Removing and re-inserting the SFP should resolve this issue. It is recommended that users perform sfpshow immediately after inserting the SFP and ensure SFP is seated properly before connecting the cables.
- When running FOS v6.4.0, if any of the following features are enabled in the FCIP configuration, a downgrade operation will be blocked until the features are removed from the FCIP config:
    - IPv6
    - IPSec on the FX8-24
    - DSCP Markings
    - Advanced Compression options 2 and 3 on the FX8-24
    - VEX ports on the FX8-24

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.

- When operating in Converged Mode, tagged frames coming with a VLAN tag equal to the configured native VLAN are dropped.

- 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). Users can enable ethsw after upgrading firmware without FC traffic interruption.

- The Brocade 8000 does not support non-disruptive hot code loads (HCL). Upgrading the Brocade 8000 to FOS 6.4 or downgrading from v6.4 is disruptive to the IO thr*ough the switch.*

- A code load on a DCX or DCX-4s with one or more FCOE10-24 blades will disrupt the traffic going through those FCOE10-24 blades.

- HA Failover of CP blades in DC*X* 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.

- An FCOE10-24 blade installed in the highest numbered slot of a DCX or DCX-4S chassis does not send out FIP unsolicited advertisements. Therefore, it does not support FCoE functionality when installed in this slot.

- The Brocade 8000 and FCOE10-24 can handle 169 small FCoE frames in bursts. If you are using the Brocade 8000 or FCOE10-24, and you delete a large number of v-ports with HCM, some of the v-ports may not appear to be deleted. To correct this, disable and re-enable FCoE with the following CLI commands:

  ```
  switch:admin>fcoe --disable
  switch:admin>fcoe --enable
  ```

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.

- 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.

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 (BES) 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.
- 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:
  - 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.
  - 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.
- 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 (DCFM 10.3 or later) that supports this feature. Note, all nodes in the EG must be running FOS v6.3.0 or later for quorum authentication to be properly supported.
- 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 or later 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.
- 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.

- 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 v2.7 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 v6.3.1 or later release.

- HCL from FOS v6.3.x to v6.4 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 later 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 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:

  1. First, modify the LUN policy from “encrypt” to “cleartext” and commit. The LUN will become disabled.
  2. Enable the LUN using “cryptocfg --enable –LUN”. Modify the LUN policy from “clear-text” 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.

- TEMS key vault support troubleshooting tips:

  - Regarding TEMS key vault (KV) communication with a Brocade encryption group, the default communication port setting for the TEMS 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.

- When disk and tape CTCs are hosted on the same encryption engine, re-keying cannot be done while tape backup or restore operations are running. Re-keying operations must be scheduled at a time that does not conflict with normal tape I/O operations. The LUNs should not be configured with auto rekey option when single EE has disk and tape CTCs.
- Gatekeeper LUNs used by SYMAPI on the host for configuring SRDF/TF using in-band management must be added to their containers with LUN state as "cleartext", encryption policy as "cleartext" and without "-newLUN" option.
- For new features added to encryption in FOS v6.4.0, such as, disk device decommissioning, combined disk-tape encryption support on the same encryption engine, and redundant key ID metadata option for replication environments, all the nodes in the encryption group must be running FOS v6.4.0 or higher versions of FOS. Firmware downgrade will be prevented from FOS v6.4.0 to a lower version if one or more of these features are in use.
- Special Notes for HP Data Protector backup/restore application
    - Tape Pool encryption policy specification:
        - On Windows Systems, HP Data Protector can be used with tape pool encryption specification only if the following pool label options are used:
            - Pick from Barcode
            - User Supplied – Only 9 characters or less

          For other options, behavior defaults to Tape LUN encryption policy.
        - On HP-UX systems, HP Data Protector cannot be used with tape pool encryption specification for any of the pool options. The behavior defaults to Tape LUN Encryption Policy.
    - Tape LUN encryption policy specification:
        - No restrictions, tape LUN encryption policy specification can be used with HP Data Protector on HP-UX and Windows systems.
- The disk device decommission operation works properly only with Containers (CTC) without hyphen (-) in the container (CTC) name.

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.

Access Gateway

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

- Users who want to utilize Access Gateway's Device-based mapping feature in the ESX environments are encouraged to refer to the SAN TechNote GA-TN-276-00 for best implementation practices. Please follow these instructions to access this technote:
    - Log in to http://my.brocade.com
    - Go to Documentation > Tech Notes.
    - Look for the Tech Note on Access Gateway Device-Based Mapping in VMware ESX Server.

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.
- VEX edge to VEX edge device sharing will not be supported.

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. 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.

FCAP

- If VF is enabled on a switch, HTTPS and FCAP certificates should always be imported in the Default Switch. Certificates imported in a non-Default Switch will not be available after hafailover operation.

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

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 and FC8-64 blade support 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 or 64-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 in 10-bit dynamic area mode on DCX-4S.
- A maximum of 112 ports may be used for connectivity to loop devices in a single Logical Switch within a chassis in 10-bit dynamic area mode on DCX.
- 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

- 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.
- 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.

Zoning

- If the default zoning mode is set to All Access and more than 120 devices are connected to the fabric, you cannot enable All Access.

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 v6.3.1 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

- POST diagnostics for the Brocade 5100 have been modified in v6.3.1b/v6.4.0 and later releases to eliminate an "INIT NOT DONE" error at the end of an ASIC diagnostic port loopback test. This modification addresses BL-1020 Initialization errors encountered during the POST portloopbacktest. (Defect 263200)
- It is recommended that no more the 50 F_Port Top Talkers be enabled on a 48000 director in a large fabric (>4000 devices).
- It is recommended that for directors with more than 300 E_Ports, the switch be disabled prior to executing the "switchCfgTrunk" command (used to disable or enable trunking on the switch).
- During non-disruptive firmware upgrades, E_Ports in R-RDY mode may cause some frame drops on the E-port links.
- The ***portCfgFillWord*** command, applicable to 8G-capable ports, has been enhanced with FOS v6.3.1 and v6.4 to provide two new configuration options (Modes 2 and 3). The available settings include:

  Mode - Link Init/Fill Word

  Mode 0 – IDLE/IDLE

  Mode 1 – ARBF/ARBF

  Mode 2 – IDLE/ARBF

  Mode 3 – If ARBF/ARBF fails use IDLE/ARBF

  Although this setting only affects devices logged in at 8G, changing the mode is disruptive regardless of the speed the port is operating at. The setting is retained and applied any time an 8G device logs in. Upgrades to FOS v6.3.1 or v6.4 from prior releases supporting only modes 0 and 1 will not change the existing setting, but switches or ports reset to factory defaults with FOS v6.3.1 or v6.4 will be configured to Mode 0 by default. The default setting on new units may vary by vendor. Please use portcfgshow CLI to view the current portcfgfillword status for that port.

Modes 2 and 3 are compliant with FC-FS-3 specifications (standards specify the IDLE/ARBF behavior of Mode 2 which is used by Mode 3 if ARBF/ARBF fails after 3 attempts). For most environments, Brocade recommends using Mode 3, as it provides more flexibility and compatibility with a wide range of devices. In the event that the default setting or Mode 3 does not work with a particular device, contact your switch vendor for further assistance.

- For the configure command, in FOS v6.4.0, the default value that displays for Maximum Logins per switch is different than the value that displays in FOS v6.3.x. The default value has not changed; it was displayed incorrectly in FOS v6.3.x, and is now corrected.

Defects

Closed with Code Change in Fabric OS v6.4.0a

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change in Fabric OS v6.4.0.a

Defect ID: DEFECT000271043	**Technical Severity**: High
Summary: As a result of firmwaredownload, systemverifcation test, or blade insertion, occasionally blade FCoE10-24 may turn faulty 21	
Symptom: Slotshow indicates that FCoE10-24 is found to be in a faulty state	
Workaround: slotpoweroff/on the FCoE10-24 to clear the faulty state	
Feature: CEE-Infrastructure	**Function**: ANVIL DRIVER
Probability: Medium	
Found in Release: FOS6.4.0	**Service Request ID**:

Defect ID: DEFECT000290749	**Technical Severity**: High
Summary: FICON: FRU events are not generated on the operator's console for removal or insertion	
Symptom: No FRU event notification at the operator's console	
Feature: FICON	**Function**: Ficud
Probability: Medium	
Found in Release: FOS6.4.0	**Service Request ID**:

Defect ID: DEFECT000296886	**Technical Severity**: High
Summary: Rare corner case of Lossless being disabled after several downgrade and upgrade scenarios.	
Symptom: A DCX logical switch with port based routing, IOD (In-Order Delivery), DLS, and LosslessDLS enabled running Fabric OS v6.3.0b is updated to v6.4.0, Lossless gets disabled.	
Workaround: Re-enable Lossless / IOD on logical switches that were previously enabled.	
Feature: 8G Platform Services	**Function**: Routing
Probability: Low	
Found in Release: FOS6.4.0	**Service Request ID**:

Defect ID: DEFECT000297733	**Technical Severity**: High
Summary: With FMS enabled, after moving all ICL and 254 FC ports into a logical switch with zero based addressing, port 1/0 (area 00) is incorrectly disabled	
Symptom: Port 0 with area 0x00 is disabled	
Workaround:	
Feature: 8G Platform Services	**Function**: FOS Kernel Drivers
Probability: Medium	
Found in Release: FOS6.4.0	**Service Request ID**:

Defect ID: DEFECT000297793	**Technical Severity**: High
Summary: Data encryption, name server fails to show the existence of a specific virtual initiator	
Symptom: As a result of an external FC port experiencing an excessive number of encoding CRC errors the internal ports are faulted incorrectly by switch firmware, hence a data encryption virtual initiator associated with the internal port fails to appear in name server.	
Workaround: Remove the condition / cause of the excessive CRC errors (ie replace cable or SFP).	
Feature: Data Security	**Function**: Platform
Probability: Low	
Found in Release: FOS6.4.0	**Service Request ID**:

Defect ID: DEFECT000297978	**Technical Severity**: High
Summary: Zoned terminated while activating zoning from DCFM	
Symptom: Unexpected reboot and failover if attempt to push zone DB from DCFM in IM2/IM3 fabrics only.	
Workaround: Use CLI (or ECFM for non-TI/Redirect zones) in IM2/IM3	
Feature: FC Services	**Function**: Zoning
Probability: Medium	
Found in Release: FOS6.4.0	**Service Request ID**:
Where Else Fixed: FOS6.3.1 b	

Defect ID: DEFECT000298015	**Technical Severity**: High
Summary: After code upgrade, non Brocade branded SFPs got Mod_Val.	
Symptom: non-Brocade branded SFPs are in Mod_Val state after firmware upgrade. This impacts FOS v6.2.2x and FOS v6.3.1x only with 1 specific non-Brocade branded SFPs.	
Workaround: Use Brocade branded SFPs	
Feature: 4G Platform Services	**Function**: FOS Kernel Drivers
Probability: Low	
Found in Release: FOS6.4.0	**Service Request ID**:

Defect ID: DEFECT000298098	**Technical Severity**: High
Summary: FICON: NSD panic while running IRNDUP to SW48K	
Symptom: Missing interrupt (IFCC) while running IRNDUP	
Feature: FC Services	**Function**: Name Server
Probability: Medium	
Found in Release: FOS6.4.0	**Service Request ID**:

Defect ID: DEFECT000298730	**Technical Severity**: High
Summary: A LUN sized > 2TB cannot be configured for encryption with the -newLUN option	
Symptom: There is a potential for hosts to overwrite encryption metadata for encrypted LUNs where Read Capacity (16) is used to determine max LUN LBA (LUNs greater than 2TB in size).	
Workaround: Do not configure LUNs for encryption, using the -newLUN option if the LUN size is greater than 2TB.	
Feature: Data Security	**Function**: Disk Encryption
Probability: Medium	
Found in Release: FOS6.4.0	**Service Request ID**:

Defect ID: DEFECT000299991	**Technical Severity**: High
Summary: FICON: Webtools out of sync with CLI in not showing correct port status when FMS mode is enabled and port is moved between different logical switches from the DCFM	
Symptom: Webtools port status from Port Admin is not displaying correct port status where CLI does.	
Feature: WebMgmt	**Function**: WT Platform Support
Probability: Medium	
Found in Release: FOS6.4.0	**Service Request ID**:

Defect ID: DEFECT000300388	**Technical Severity**: High
Summary: WebTools: Name server tab unable to export name server data base from FCR configured switch.	
Symptom: After opening the name server tab and performing export the tables, export fails with an error message “For Input String N/A”.	
Feature: WebMgmt	**Function**: Name Server
Probability: Medium	
Found in Release: FOS6.4.0	**Service Request ID**:

Defect ID: DEFECT000301006	**Technical Severity**: High
Summary: Data Encryption, tape containers get stuck in login busy state after performing ISL disruption tests	
Symptom: Performing HA failover by toggling ISL between HA cluster members can cause containers to be not hosted with reason "login busy".	
Workaround: Do not connect target devices to BES directly, but connect them to an L2 switch.	
Feature: Data Security	**Function**: Tape Encryption
Probability: Medium	
Found in Release: FOS6.4.0	**Service Request ID**:

Defect ID: DEFECT000281212	**Technical Severity**: Medium
Summary: In AG mode, N-Port failover results in F-Ports with attached hosts getting stuck as G_Port	
Symptom: F-Ports get stuck as G-Ports after AG N-Port failover.This happens when there is a change in the base address for the N-Port due to failover, or when there is no wwn-area mapping for few devices and due to the login sequence of these devices, the PIDS assigned conflicted with the already allocated PID to another device, resulting in the F-Ports getting stuck as G-Port.	
Workaround: portdisable/enable	
Feature: Embedded Platform Services	**Function**: Other
Probability: Medium	
Found in Release: FOS6.2.0_bc	**Service Request ID**:

Defect ID: DEFECT000286529	**Technical Severity**: Medium
Summary: FICON: when CHPs are very busy, CUP may report many IFCCs	
Symptom: IFCCs on CUP exchange	
Feature: Field Escalation	**Function**: FICON
Probability: Low	
Found in Release: FOS6.3.0	**Service Request ID**:

Defect ID: DEFECT000288968	**Technical Severity**: Medium
Summary: When running 200 ms delay and 1% packet loss, after 4 days of run time, an IPSec enabled FCIP circuit bounced.	
Symptom: Tunnel bounce can occur.	
Feature: FCIP	**Function**: FCIP Port
Probability: Low	
Found in Release: FOS6.4.0	**Service Request ID**:

Defect ID: DEFECT000289418	**Technical Severity**: Medium
Summary: Tape drives fail when running over FCR with EX ports in Open mode. The REC accept payload is incorrect.	
Symptom: If host to tape I/O traverses FCR and includes an edge fabric, the tape drives would run for a bit and then fail due to REC ACC is not processed correctly if EX port is operating in IM3/Open mode.	
Workaround:	
Feature: Legacy FCR - 7500/FR4-18i	**Function**: FCR Daemon
Probability: High	
Found in Release: FOS6.3.0	**Service Request ID**: 419137

Defect ID: DEFECT000290784	**Technical Severity**: Medium
Summary: Abort in Read emulation if Attention status received between status and status accept	
Symptom: IFCCs during Tape Read processing.	
Workaround: Disable FICON Emulation	
Feature: FCIP	**Function**: FCIP I/O
Probability: Medium	
Found in Release: FOS6.3.1	**Service Request ID**:

Defect ID: DEFECT000298077	**Technical Severity**: Medium
Summary: FICON: IFCCs seen when enabling ICL ports wiht Lossless DLS enabled	
Symptom: IFCCs observed and traffic can be adversely affected.	
Workaround:	
Feature: 8G Platform Services	**Function**: Routing
Probability: Medium	
Found in Release: FOS6.4.0	**Service Request ID**:

Defect ID: DEFECT000298120	**Technical Severity**: Medium
Summary: Port based routing frame were out of order when FCP image pairs concurrently initiate exchanges as originators over GE ports	
Symptom: 3rd party device has very poor performance over FCIP link between two Brocade 7800 over 1G GE port. Same issue applies to FX8-24 blades.	
Workaround:	
Feature: FCIP	**Function**: FCIP Performance
Probability: Medium	
Found in Release: FOS6.3.1	**Service Request ID**: 429767
Where Else Fixed: FOS6.3.1 b	

Defect ID: DEFECT000298774	**Technical Severity**: Medium
Summary: Multiple critical CDR-1003 raslog during supportsave	
Symptom: After a non-disruptive upgrade from Fabric OS version v6.1.x to Fabric OS version 6.2.x, CDR-1003 CRITICAL messages may be posted during a supportSave operation on Brocade 4G platforms. With the fix in this release, the critical message is update to Warning and it can be ignored unless it's persistent and not happening during supportsave.	
Workaround: Ignore if CDR-1003 happens during supportsave and not persistent.	
Feature: 4G ASIC Driver	**Function**: ASIC Driver
Probability: High	
Found in Release: FOS6.3.1	**Service Request ID**:

Defect ID: DEFECT000299335	**Technical Severity**: Medium
Summary: FICON emulation, core hangs during error recovery	
Symptom: After an FCIP link failure, an FFDC will occur and some traffic across remaining FCIP links will continue to be disrupted.	
Feature: FCIP	**Function**: Emulation
Probability: High	
Found in Release: FOS6.4.0	**Service Request ID**:

Defect ID: DEFECT000300065	**Technical Severity**: Medium
Summary: Data Encryption, Manual HA failback command on FOS v6.4.0 fails	
Symptom: Manual failback command (cryptocfg –-failback -EE) issued from node other than failed over node fails with an error.	
Workaround: Issue the manual failback command from the node hosting the failed over containers.	
Feature: Data Security	**Function**: HA Cluster
Probability: Medium	
Found in Release: FOS6.4.0	**Service Request ID**:

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.
- 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.

  10-bit addressing mode is not supported in a FICON environment.

Area	Comments
FCIP	VEX ports are not supported on the 7800 and FX8-24 blade in a FICON environment
FCIP	When performing multiple cabling changes to the SAN fabric in a FICON Emulating FCIP Tunnel configuration with the Brocade 7800 or FX8-24 blade, either disable all of the FCIP Tunnels or issue the switch disable command on all FCIP interconnected switches to avoid IFCCs in a mainframe environment. Issuing either a switch disable or an FCIP Tunnel disable command will allow the FCIP FICON Emulation processing state-machine to execute an orderly cleanup process and allow normal activation of the new configuration. When all cabling and Traffic Isolation Zone manipulations have been completed, enable the switches or the FCIP Tunnels.
Firmware Downloads	Non-disruptive Hot Code Load is only supported on director class switches (48000, DCX, and DCX-4S). Comprehensive non-disruptive Hot Code Load is not supported on the 7500 or 7800 or a DCX, DCX-4S or 48000 with an FR4-18i or FX8-24 blades since the FCIP tunnels will go down for 10-15 seconds and all traffic in the tunnels will be disrupted.. 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 missing interrupt.
Interoperability	When connecting an 8G capable port in a Brocade switch to an IBM Virtualization Engine TS7700, the port must be configured to a minimum of 16 buffers to avoid IFCCs at the channel and loss of FICON paths to the control unit. This requires the Extended Fabric license on the Brocade switch.
Manageability	In a mixed fabric environment, an M-EOS switch must be principal switch if the fabric is in Interopmode 2 (McDATA Fabric Mode).

<table>
<tr><td>Manageability</td><td>It is suggested that Port Fencing be used to avoid taking ports down for normal fabric events. The recommended fencing criteria and settings are:

<table><tr><th>Criteria</th><th>Value</th></tr><tr><td>ITW (Invalid Transmission Words)</td><td>25</td></tr><tr><td>CRC (Cyclical Redundancy Check)</td><td>3</td></tr><tr><td>Protocol Errors</td><td>2</td></tr><tr><td>State Change</td><td>7</td></tr></table>
Note: In a FICON environment, the time base polling interval MUST be set to one minute for granular control and response. By default, Port Fencing time base is set to one hour.</td></tr>
<tr><td>Manageability</td><td>Firmware download is executed sequentially if ECFM is used for downloading code to FOS switches.</td></tr>
<tr><td>Manageability</td><td>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.</td></tr>
<tr><td>Manageability</td><td>The remote CUP may not work when the channel is connected to an 8G blade on a 48000 cascaded to a remote switch.</td></tr>
<tr><td>Manageability</td><td>FMS must be enabled on the local switch for the remote CUP to work.</td></tr>
<tr><td>Optics</td><td>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.</td></tr>
<tr><td>Serviceability</td><td>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.</td></tr>
<tr><td>Serviceability</td><td>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.</td></tr>
<tr><td>Serviceability</td><td>When the mainframe goes through a resetting event (Conflg POR, IPL, POR), in rare instances, some of the ports may come up in an "Invalid Attach" state. To recover these ports, vary the CHPIDs offline and back online. This is most likely caused by other ports on the system experiencing link level errors and should be debugged accordingly.</td></tr>
<tr><td>Traffic Isolation Zones</td><td>Enable Lossless DLS or Lossless DPS when activating Traffic Isolation (TI) Zones to avoid any traffic disruption.</td></tr>
<tr><td>Traffic Isolation Zones</td><td>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.</td></tr>
<tr><td>Traffic Isolation Zones</td><td>Deactivating TI Zone with failover disabled may caused IFCC's. Enable failover prior to deactivating TI Zone to avoid IFCCs.</td></tr>
</table>

Note: Please refer to the *Firmware Upgrades and Downgrades* section of this document when planning an upgrade to a fabric that includes the 7500 or 7800, or has any FR4-18i or FX8-24 blades in a 48k, DCX-4S, or DCX chassis .

Interoperability

Within a fabric, current major releases will work with previous major releases on the same platform. When cascading switches, it is recommended to keep all switches in the fabric at the same code level. Although not expressly prohibited, having two switches in the same fabric that differ by more than one major FOS release level is not recommended. For example, a switch at FOS v6.4.0a connected to another switch at v6.3.0d is OK. Connecting a switch running FOS v6.4.0a to a switch running FOS v6.1.0a is not recommended.

The following table indicates supported intra-fabric interoperability between hardware platforms, supported management software levels, and recommended firmware versions.

FICON Hardware/Firmware/Software Interoperability with FOS v6.4.0a

	DCFM	EFCM	DCX/ DCX-4S	48000	M6140/ Mi10K	5100/ 5300	4100/ 4900/ 5000[2]	7500/ 7500E[3]	7800
DCX/ DCX-4S	10.4.1	NS	S	S	S [1,4]	S	S	S	S
48000	10.4.1	NS		S	NS	S	S	S	S
M6140/ Mi10K	10.4.1	9.7.4			S	S[1]	NS	S[1]	S[1]
5100/ 5300	10.4.1	NS				S	S	S	S
4100/ 4900/ 5000[2]	10.4.1	9.7.4					S	NS	NS
7500/ 7500E[3]	10.4.1	NS						S	NS
7800	10.4.1	NS							S

Table Notes:
S=Supported
NS = Not Supported

FR4-18i Extension blade is only interoperable with 7500 or 7500E extension switches.
FX8-24 Extension blade is only interoperable with 7800 extension switch.

FC8-64, FS8-18, FCOE10-24 and FA4-18i are not supported in a FICON environment.

All platforms operating with FOS v6.4.0a unless otherwise specified.

[1] - Supported with Mi10K/M6140 running M-EOS v9.9.7
[2] - 4100, 4900, & 5000 running FOS v6.2.0e
[3] - Brocade Accelerator for FICON option requires 7500 or 7500E Upgrade license
[4] - DCX-4S does not support interop with M-EOS platforms (M6140/Mi10k)