Brocade Fabric OS v7.4.0a Release Notes v2.0

July 17, 2015

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v7.4.0a Release Notes v1.0	Initial Release	May 29, 2015
Brocade Fabric OS v7.4.0a Release Notes v2.0	Add Appendix for FICON Environments, add defect 000554782 to the Closed With Code Change table, and add additional instructions for removing APM monitors under Obsoleted FOS Features section	July 17, 2015

Contents

Overview

FOS v7.4.0a is a patch release based on FOS v7.4.0. All hardware platforms and features supported in FOS v7.4.0 are also supported in FOS v7.4.0a. Besides defect fixes, FOS v7.4.0a adds support for following existing hardware and enhancement.

- Brocade Encryption Switch (BES) and FS8-18 blade
- E-port connections between two FC16-64 blades

New Hardware Support

Brocade Fabric OS v7.4 does not introduce support for any new hardware platforms. FOS v7.4 adds support for the following new hardware:

- Brocade-branded 4GB external USB flash drive

Summary of New Software Features

FOS v7.4 includes support for many new software features and enhancements including:

- IP Extension features for Brocade 7840
- FCIP enhancements for Brocade 7840
- MAPS (Monitoring and Alerting Policy Suite) enhancements
- Flow Vision enhancements
- ClearLink Diagnostics (D_Port) enhancements
- Peer Zoning support
- Target Driven Zoning support
- Lossless DLS enhancement
- FCR enhancements
- Security enhancements
- Time Server enhancements
- SNMP enhancements
- RDP Enhancements
- Firmware download enhancements
- RAS enhancements
- Zoning enhancements
- FICON enhancements
- Miscellaneous enhancements

Obsoleted FOS Features

The following features supported in FOS v7.3 and earlier releases are obsolete beginning with FOS v7.4:

- Fabric Watch
- Advanced Performance Monitoring (APM)

Users running Fabric Watch for switch monitoring in FOS v7.3 are advised to convert to MAPS monitoring before upgrading to FOS v7.4. Converting Fabric Watch to MAPS before upgrading to FOS v7.4 can preserve Fabric Watch threshold configurations. If users choose to upgrade to FOS v7.4 without converting to MAPS, Fabric Watch will stop functioning after the firmware upgrade and the Fabric Watch thresholds cannot be automatically migrated for use by MAPS. Please refer to the Fabric OS MAPS Administrator's Guide for step-by-step migration instructions.

Users running APM in FOS v7.3 are required to remove all monitors before upgrading to FOS v7.4 by using the following commands:

1. Enter perfdeleemonitor to remove all End-to-end monitors.
2. Enter perfcfgsave to save this change.
3. Enter fmmonitor --delmonitor to remove all filter monitors.
4. Enter fmmonitor --delete *frametype* to remove the specified user-defined frametype.
5. Enter perfttmon --delete to remove all switch level Top Talker monitors.
6. Enter perfttmon --delete fabricmode to remove fabric mode Top Talker monitors.

After upgrading to FOS v7.4, the APM monitors will stop functioning. Users can use the Flow Vision features as part of Fabric Vision for performance monitoring. Please refer to the Fabric OS Flow Vision Administrator's Guide for detailed instructions on removing APM monitors and Flow Vision feature configurations.

Brocade Fabric Vision licenses are required for MAPS and Flow Vision. The combination of Brocade Fabric Watch license and Brocade APM license enables the MAPS and Flow Vision features. For switches with only Fabric Watch licenses or only APM licenses, users can acquire and install the missing license to acquire MAPS and Flow Vision features.

New Feature Descriptions

New Hardware Support

FOS v7.4 adds support for the following new hardware:

- Brocade-branded 4GB external USB flash drive

IP Extension features for Brocade 7840

FOS v7.4 introduces IP Extension support for the Brocade 7840. Users can use this capability to extend IP storage for replication and disaster recovery in much the same way as Fibre Channel storage while taking advantage of the compression, encryption, QoS, and trunking features available in the Brocade 7840.

A Brocade 7840 running FOS v7.4 can support both FCIP Extension and IP Extension at the same time. IP Extension includes the following:

- Support for system configuration for IP Extension
- Support for GbE port configuration for IP Extension
- Tunnel configuration for IP Extension
- Adaptive Rate Limiting
- TCP/IP Features
- Traffic Control List

Support System Configuration for IP Extension

FOS v7.4 supports users configuring Brocade 7840 for both FCIP Extension and IP Extension (hybrid mode). By default, Brocade 7840 supports FCIP Extension only. Changing a Brocade 7840 between FCIP-only and hybrid mode requires a switch reboot.

Support GE Port Configuration for IP Extension

FOS v7.4 supports users configuring the front end 1/10 GbE ports as LAN ports on a Brocade 7840 for hybrid mode. These ports are used to connect to IP storage devices on the LAN side. FOS v7.4 supports static Link Aggregation Group (LAG) configuration so that multiple LAN ports can be assigned to the same LAG group.

Tunnel configuration for IP Extension

FOS v7.4 supports user configuration of IP tunnels on a Brocade 7840 in the same way as FC tunnels are configured. IP tunnels and FC tunnels are all represented under virtual E-port (VE). Each VE is configured as a FC-only tunnel or as both FC and IP tunnels. Trunking, QoS, and compression are supported on IP tunnels as they are for FC tunnels.

Adaptive Rate Limiting (ARL)

FOS v7.4 supports all ARL features available on the FCIP Extension for IP Extension. The static distribution of unused bandwidth is hierarchical.

TCP/IP Features

FOS v7.4 supports the following TCP/IP features for IP Extension.

- LAN side jumbo frames
- IPv4 and IPv6 for LAN side
- Maximum 512 TCP connections per Data Processor (DP)
- Maximum 512 TCP open requests per second per DP
- Maximum 64 UDP flows per DP
- DSCP/VLAN L2CoS marking
- Segment Preservation
- Each LAN TCP window will be 64K by default. If TCP window scaling is requested, the maximum advertised window is 256K. The maximum window per connection is 2M irrespective of the advertised window.

- Untagged and single tagged packets are supported.
- Stacked/double (IEEE 802.1ad) tagged packets from hosts are not supported. Packets will be dropped.

Traffic Control List

FOS v7.4 supports Traffic Control List (TCL) to manage and route IP flows. Each TCL is identified by a unique user configured name. FOS v7.4 supports maximum 128 TCLs. System generated default TCL will drop all the incoming packets.

FCIP Enhancements to Brocade 7840

Base Switch Support for 7840

FOS v7.4 enhances Virtual Fabric support on 7840 switches to include the base switch, i.e., to support XISL. Users can configure E_port (ISL over FC), EX_port (IFL over FC), and VE_port (ISL over GE) in base switch. The maximum number of logical switches supported — including the base switch — remains four.

FCIP Hot Code Load (HCL)

FOS v7.4 enhances FCIP HCL support in the following conditions, which were excluded in FOS v7.3.

- Support concurrent FCIP HCL on all 7840 switches in the configuration
- Support multiple sites for FCIP HCL

Monitoring and Alerting Policy Suite (MAPS) Enhancements

FOS v7.4 has a number of important MAPS feature enhancements. These include:

- Basic monitoring without Fabric Vision license
- Monitor NPIV device login limits
- Monitor backend ports
- Monitor FCIP circuit QoS
- Monitor FCIP circuit RTT and jitter on Brocade 7800 and FX8-24 blade
- Fabric Performance Impact monitoring enhancement
- Slow drain device quarantine action for Fabric Performance Impact monitoring
- Port toggle action
- FICON notification action
- Alert quiet time support
- Usability enhancements

Monitoring without Fabric Vision license

FOS v7.4 introduces a new basic monitoring capability in MAPS. The basic monitoring capability allows end users without Fabric Vision licenses on their switches to use MAPS to monitor overall switch status, FRU health, and switch resource categories under the new pre-defined MAPS policy dflt_base_policy.

Monitor NPIV device login limits

FOS v7.4 introduces MAPS monitoring of NPIV login limits. FOS has limits on the number of NPIV devices that can login to a physical F_port. MAPS monitors the percentage of logged in NPIV devices relative to the maximum number of NPIV logins allowed on the F_port to alert users before the limit is reached.

Monitor backend ports

FOS v7.4 introduces back-end port error monitoring in MAPS. Users can take early recovery actions if any of the monitored back-end errors have crossed specified thresholds. Typical recovery actions include SerDes tuning on a switch or reseating blades. For detailed instructions on these actions, please contact your support provider for additional assistance.

Monitor FCIP circuit QoS

FOS v7.4 enhances FCIP QoS monitoring in MAPS to add monitoring of Fibre Channel QoS parameters at circuit level. The circuit QoS monitoring combined with the tunnel QoS monitoring available since FOS v7.3 provides additional granularity to monitor the FCIP link performance.

Monitor FCIP circuit RTT and jitter on 7800 and FX8-24

MAPS monitors circuit round trip time (RTT) and jitter statistics in FOS v7.3 on Brocade 7840. FOS v7.4 supports these two FCIP circuit monitoring elements on Brocade 7800 and FX8-24 blade so that they are available to 8G FC extension platforms.

Fabric Performance Impact monitoring enhancement

FOS v7.4 enhances Fabric Performance Impact (FPI) monitoring to add a new IO_LATENCY_CLEAR state so that end users can receive notification when latency conditions are cleared. FOS v7.4 enhances FPI monitoring by adding latency counter monitoring on all ports to detect potential transient spikes of latency conditions. In addition, FOS v7.4 moves port TX, RX, and UTIL monitoring systems to the FPI category from the Port Health category in FOS v7.3 and earlier releases so that all potential congestion conditions are reported under the FPI category.

Slow drain device quarantine action for Fabric Performance Impact monitoring

FOS v7.4 introduces a new MAPS action that automatically isolates slow drain devices when they are detected by FPI monitoring. This frees up buffer credits for normal devices that are sharing the same links and mitigates the effect due to presence of slow drain devices in the fabric.

Port toggle action for Fabric Performance Impact monitoring

FOS v7.4 introduces Port Toggle as an action which automatically recovers slow drain device conditions when they are detected by FPI monitoring. A port toggle, (which is a port disable followed by a port enable) can recover the ports from some slow drain device conditions or force traffic failover to an alternate path.

FICON notification action

FOS v7.4 introduces FICON notification as a new action that enables MAPS events to be sent to FMS with detailed event information upon rule violations. FMS CUP can translate these MAPS events into FICON-specific Health Summary Check reports.

Alert quiet time support

FOS v7.4 introduces a quiet time support for RASLOG and EMAIL alert actions. This feature allows end users to configure within a rule a period of time not to receive duplicated alerting actions after the first alert has already been sent.

Usability enhancements

FOS v7.4 has a number of usability enhancements to MAPS. These include:

- Allow *none* to be used as an email address to clear previously configured email addresses in the CLI command *mapsconfig*.
- Enhanced Temperature Sensor monitoring so that actions are triggered on change of Temperature Sensor (TS) states.
- Modified FRU monitoring so that the states being monitored are more accurate and useful for operations.
- An upper limit to the number of rules that can be created in a policy. The maximum number of rules in a policy is dependent on the character length of each rule name.

Flow Vision Enhancements

FOS v7.4 provides the following enhancements to Flow Vision:

All F_Port Flow Monitoring

FOS v7.4 introduces a system predefined learning flow named sys_mon_all_fports to monitor performance on all F_ports in a switch. Flow learning on all F_ports provides a continuous, automatic, and comprehensive view of application traffic patterns for all device connections.

Scalability Improvement

FOS v7.4 increases the scalability limit supported by Flow Vision. In particular, the total number of sub-flows supported by chassis switches is increased to 2048 and by fixed port switches is increased to 512.

Identify All Devices in a Flow

FOS v7.4 supports displaying all zoned devices in a flow by introducing a new option -allzoned to the Flow Vision command. This will identify all zoned devices for a flow defined on an E_Port or F_Port.

Fabric Flow Dashboard

FOS v7.4 introduces support of a Flow Dashboard that provides information for a flow from all the available data points in the fabric through which it can pass. With all relevant data summarized for a flow of interest, users are able to more easily troubleshoot and identify the root cause of various issues that may occur.

ClearLink Diagnostic (D_Port) Enhancements

FOS v7.4 implements the following D_Port feature enhancements.

Link Power (dB) Loss Calculation

FOS v7.4 supports calculating TX and RX power loss of a link with D_Port tests. D_Port tests include the power loss calculation to provide additional details on the health of physical media of links.

Dynamic D_Port and On-demand D_Port with DWDM

FOS v7.4 enhances D_port pre-provision feature to allow administrators to pre-provision certain ports connected to DWDM links. With the pre-provisioned list, dynamic D_port and on-demand D_port tests can start automatically on those ports with the optical loopback test skipped.

CLI Command Hierarchical Help Display

FOS v7.4 enhances the help page for D_port CLI commands so that only the relevant sub-options are displayed when a command action is specified for the portCfgDport and portDportTest commands.

Peer Zoning Support

FOS v7.4 introduces support for Peer Zoning as defined in the FC-SW-6 and FC-GS-7 standard. In a Peer Zone configuration, membership in a zone is differentiated into principal members and non-principal or peer members. Peer Zoning configuration allows communication between a principal member and any peer member but does not allow communication between two peer members or between two principal members. By adopting Peer Zoning, users can simplify zoning configuration and management, improve performance, and increase scalability.

Target Driven Zoning support

FOS v7.4 introduces the Target Driven Zoning feature that allows end devices to create Peer Zone configurations through inband commands. This feature enables zoning to be configured by management software on storage devices and reduces the manual configuration needed on switches.

Lossless DLS enhancement

FOS v7.4 introduces a routing enhancement to support lossless Dynamic Load Sharing (DLS) in a 2-hop topology. This enhancement allows adding links or switches in existing paths that are up to 2 hops between a host and a target, including the new link that is coming online, to ensure lossless and in-order frame delivery.

FCR enhancements

FOS v7.4 has a number of enhancements in FCR. These enhancements include:

Location Embedded LSAN zone

FOS v7.4 introduces the location-embedded LSAN zone feature. A location-embedded LSAN zone specifies in the LSAN zone name the remote fabric ID that shares devices. The corresponding FCR switch will use this information in the LSAN zone names to store only these entries for the locally connected edge fabric. As a result. users are now able to configure more LSAN zones across a backbone fabric.

Increase Number of Imported Proxy Devices

FOS v7.4 increases the maximum number of proxy devices that can be imported into each edge fabric to 4000. This limit applies to the cumulative number of all proxy devices created on all translate domains in the edge fabric. FOS versions prior to v7.4 support 2000 proxy devices as the limit for this number.

Sort WWNs in *lsanzoneshow* CLI

FOS v7.4 supports sorting WWNs in the CLI command lsanzoneshow output. A new -o or -sort option is added to the CLI command to display entries in sorted order by WWNs for each LSAN zone listing.

Support Port Range for *portcfgexport* and *portcfgvexport* CLI

FOS v7.4 supports port range as input parameters for the portcfgexport and portvexport CLI commands so that multiple ports can be configured as EX-port or VEX-port at the same time.

Support Peer Zoning with FCR

FOS v7.4 supports Peer Zoning in LSAN zones if users have configured a peer zone in an edge fabric. Peer zoning rules and RSCN distribution will be enforced by edge fabric switches.

Support New Domain ID Range for Front and Translate Phantom Domains

FOS v7.4 supports assigning for an FCR the front domain ID in the range of 160 through 199 and the translate domain ID in the range of 200 through 239. Users can use the CLI command *fcrConfigure --resetPhantomDomain* to use the new range to avoid conflicting with the real switch domain IDs.

Security Enhancements

FOS v7.4 has a number of important security enhancements:

Obfuscation of RADIUS Shared Secrets

FOS v7.4 supports obfuscation of the RADIUS shared secrets so that they are not stored as plaintext. With this option, stored shared secrets are not visible as plaintext in configUpload files and SupportSave files.

Import/Export Syslog Server Certificates

FOS v7.4 adds the support of importing and exporting a syslog server certificate to support syslog over TLS. A syslog server CA certificate can be imported from a remote host or exported to a remote host.

Password Policy Enhancement for Root Password Change

FOS v7.4 adds a new option in the switch account password policy to allow root password change by root account login sessions without prompting for the existing (old) password.

secCryptoCfg CLI Command

FOS v7.4 supports a new CLI secCryptoCfg command to configure the set of acceptable cryptographic algorithms for the SSH and HTTPS protocols on a switch. Administrators can use this new CLI command to mandate various cryptographic algorithms conform to their policies.

Default Account Password Change

FOS v7.4 modifies the behavior of default switch account password change. Login to admin account would only prompt changes to the default admin and user account passwords. The default root and factory account passwords change would only be prompted when login to the switch as root.

Time Server Enhancements

FOS v7.4 enhances Time Server to support Network Time Protocol (NTP) server configuration distribution to Access Gateway switches. This enhancement allows AGs, including cascaded AG connections, to receive the same NTP server configuration from a connected fabric.

SNMP Enhancements

FOS v7.4 implements the following SNMP enhancements.

Log Messages for SNMPv3 Authentication

FOS v7.4 logs SNMP authentication success and failure as audit log messages to track the authentication results for SNMPv3 requests.

SNMPv3 Individual Inform Tag

FOS v7.4 enhances SNMPv3 configuration to allow SNMP informs to be enabled or disabled at individual receiver host level. With this enhancement, users can configure some receivers to get SNMP informs, while other receivers get SNMP traps.

Disable SNMP Write Access

FOS v7.4 changes the default SNMP configuration to have SNMP write disabled. This affects the default switch configuration loaded with FOS v7.4 on a new switch from factory.

Obsoletes Fabric Watch and Advanced Performence Monitoring MIBs

FOS v7.4 obsoletes the following MIBs associated with Fabric Watch and Advanced Performance Monitoring feature: swFwSystem, swBlmPerfMnt, swTopTalker.

RDP Enhancements

FOS v7.4 enhances the Read Diagnostic Parameter (RDP) support which includes the following:

- Enable polling to refresh RDP data cache at a default 4 hour interval.
- Include signal power loss information in the *sfpShow --link* or *sfpShow --pid* options.
- Include corrected and uncorrected FEC blocks in *portShow --link* or *portShow --pid* options.

Firmware Download Enhancements

FOS v7.4 introduces the following important enhancements for firmware download.

Staged Firmware Download

FOS v7.4 supports staged firmware download so that users can download firmware package to a switch first and choose to install and activate the downloaded firmware at a later time.

Firmware Clean Installation

FOS v7.4 supports firmware clean installation. This installs a firmware package without retaining the existing configuration or maintaining HA. With this feature, customers receiving a new switch from factory can install firmware in a single step to the desired version that their networks are running, without going through multiple steps of non-disruptive firmware download.

Firmware Auto Sync Enhancement

FOS v7.4 enhances the firmware auto sync feature to support automatic synchronization of firmware versions on a standby CP with a version different from the active CP. If an active CP runs FOS v7.4 or higher:

- A standby CP with firmware version as early as FOS v6.4 can be upgraded automatically.
- A standby CP with firmware version later than FOS v7.4 can be downgraded automatically.

Firmware Integrity Check

FOS v7.4 introduces a firmwareCheck CLI command to check the integrity of firmware packages already installed on the switch. If any of the files or packages as part of firmware has been changed, the firmware integrity check will fail and notify users which package has failed the check.

Challenge-Response Authentication

FOS v7.4 introduces support for SSH servers configured with "keyboard-interactive" as defined in IETF RFC 4256 as authentication method to be used with SCP or SFTP for firmware download, support save, and config upload/download commands. With this SSH server configuration, FOS v7.4 only supports account passwords as a form of challenge-response authentication.

RAS Enhancements

FOS v7.4 supports the following RAS enhancements:

WWN Card Replacement Enhancements

FOS v7.4 enhances the procedure for field replacement of WWN cards in chassis based systems. WWN cards are chassis FRUs that contain chassis WWNs and other information. Each chassis has two WWN cards for redundancy. FOS v7.4 enhances WWN card handling so that certain error or data corruptions associated with WWN cards can be recovered in the field.After users replace a single defective WWN card with a new one, some data can be restored from the current/non-defective WWN card to the newly replaced WWN card. In addition, the system periodically checks the integrity of the WWN cards and logs RASLOG error messages if problems are detected.

Show RASLOG Messages within a Timeframe

FOS v7.4 adds options to errdump and errshow CLI command so that only RASLOG messages within the specified beginning and end time will be shown, instead of all RASLOG messages.

Audit Log Enhancements

FOS v7.4 enables audit log by default for all classes of messages. FOS v7.4 increases the maximum number of audit log messages stored on a switch to 1024 from 256.

Clihistory Identify Command Virtual Fabric FID

FOS v7.4 enhances cliHistory so that FID contexts will be shown along with the command line. With this enhancement, clihistory in a support save file includes the FID information for support and debug usage.

Zoning Enhancements

FOS v7.4 adds the following enhancements to standard zoning to simplify zoning configuration:

List Zones with Specific Alias

FOS v7.4 adds support to zoneshow command to display only the zone configurations that match a given alias instead of the entire zone database. Administrators can use this enhancement to quickly locate certain zone configurations that contain a specific alias or alias prefix.

Sort zoneShow Command Output by WWN

FOS v7.4 enhances the *zoneShow --sort* command output in sorted order for both (D,I) and WWN members.

Indicate offline members in zoneShow output

FOS v7.4 provides a new option *--validate* to the zoneshow command to indicate members in the configuration but not online in the fabric. Administrators can use this enhancement to quickly discover the online and offline members in a zone configuration.

Traffic Isolation (TI) Zoning Enforcement enhancement

FOS v7.4 enhances TI zoning rule enforcement so that devices connected to the same local switch are also enforced by the TI zoning rule.

TI Failover Disabled Zone Message

FOS v7.4 adds a RASLOG message ZONE-1060 to warn users if the TI zone dedicated path is the only path available between two domain IDs.

FICON Enhancements

FOS v7.4 adds the following FICON related enhancements :

MAPS notification to FMS CUP

FOS v7.4 supports a new MAPS FICON notification action. With this action, MAPS rule violations can trigger notifications to the FMS host as Health Summary Code reports.

ConfigUpload and ConfigDownload of FMS Mode

FOS v7.4 enhances configUpload and configDownload to ensure that a configDownload can turn ON the FMS mode in a logical switch that had FMS mode OFF.

D_Port Support in Port Descriptor

FOS v7.4 reports the state of an FC port in D_Port mode to the HOST with the Port Information Block (PIB).

Miscellaneous Enhancements

Login to Logical Switch IP

FOS v7.4 enhances Logical Switch IP address support so that logins using the logical switch IP address automatically set the user VF context to the logical switch associated with the IP address.

Dynamic Switch Port Names

FOS v7.4 introduces a dynamic port name feature to automatically assign port names on a switch based on a default standard format and port types. Users can enable and disable the “Dynamic port name feature” with the configure CLI command.

Port Index Support for CLI Command portErrShow and portTestShow

FOS v7.4 enhances the portErrShow and portTestShow command to support port index as inputs, in addition to the existing slot/port as input.

Link Reset on Loss of Sync

FOS v7.4 enhances credit recovery on backend links for 8G platforms by performing link reset (LR) on loss of sync (LOS) events. This enhancements applies to a port where a loss of sync is detected and the peer port of the backend link is on a 8G platform.

Enhance switchShow CLI Output

FOS v7.4 modifies switchshow -portname command output to display the port PWWN of the switch ports along with the port names.

portLoginShow Command with History Option

FOS v7.4 enhances the portLoginShow CLI to display details of the device that last logged out from a port. This enhancement supports the port login types of “fe” for FLOGI devices and “fd” for FDISC devices. Users can use the -history option to show the device logout information.

Port Peer Beacon Support EX-Port

FOS v7.4 enhances port peer beacon (LCB) feature to support links with EX-ports.

BufOpMode for FC Gen5 Blades

FOS v7.4 adds support of Buffer Optimization Mode (BufOpMode) for FC Gen5 core blades and port blades. The BufOpMode enables non-local switching in an edge ASIC chip where both E-port and F-port exist.

portStatsShow Command Display TXQ Latency

FOS v7.4 enhances the portStatsShow CLI command to display the ASIC transmit queue (TXQ) latency information for each virtual channel (VC).

Support De-bouncing of Loss of Signal for Fixed Speed and Auto Negotiate Ports

FOS v7.4 expands loss of signal de-bouncing for both fixed-speed and auto-negotiated ports in any port state. FOS v7.4 adds a “mode 2” option for the portcfglosstov CLI command to enable for both fixed-speed ports and auto-negotiate ports.

Backend Link Failure Blade Fault Option

FOS v7.4 enhances back-end link failure handling. With this enhancement, when back-end link failure is detected, the link is re-initialized first and the blade is faulted only when re-initialization fails. In addition, a blade would not be faulted if there is another online port within the trunk.

DLS Support on Embedded Switches

FOS v7.4 supports DLS on the embedded platforms. Earlier FOS versions do not support dynamic load sharing (DLS) on the FC embedded platforms.

New portChannelShow CLI Command

FOS v7.4 adds a CLI command portChannelShow to display a DPS group for one or all reachable domains.

Support preserving port2area and area2port mappings with configUpload and configDownload

FOS v7.4 supports uploading and downloading the port2area and area2port mapping tables in a configuration file for all logical switches in a chassis through the new -map option with the existing configUpload and configDownload CLI command.

Optionally Licensed Software

Fabric OS v7.4 includes all basic switch and fabric support software, as well as optionally licensed software that is enabled via license keys.

Optionally licensed features 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).

Note: If a port on 16G FC blades or a 16G switch is configured to operate at 10G speed, Extended fabrics license is not needed to enable long distance connectivity on that port.

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 — All Advanced Performance Monitoring features are obsolete in FOS v7.4. This license remains to provide end users with Fabric Watch license to upgrade to Fabric Vision capabilities.

Brocade Fabric Watch — All Fabric Watch features are obsolete in FOS v7.4. This license remains to provide end users with Advanced Performance Monitoring license to upgrade to Fabric Vision capabilities.

Brocade Fabric Vision — Enables MAPS (Monitoring and Alerting Policy Suite), Flow Vision, and ClearLink (D_Port) to non-Brocade devices. MAPS enables rules based monitoring and alerting capabilities, provides comprehensive dashboards to quickly troubleshoot problems in Brocade SAN environments. Flow Vision enables host to LUN flow monitoring, application flow mirroring for non-disruptive capture and deeper analysis, and test traffic flow generation function for SAN infrastructure validation. D_Port to non-Brocade devices allows extensive diagnostic testing of links to devices other than Brocade switches and adapters.

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

Enhanced Group Management — This license enables full management of devices in a data center fabric with deeper element management functionality and greater management task aggregation throughout the environment. This license is used in conjunction with Brocade Network Advisor application software and is applicable to all FC platforms supported by FOS v7.0 or later.

Note: This capability is enabled by default on all Gen 5 65XX model switches and DCX 8510 platforms, and on DCX and DCX-4S platforms that are running Fabric OS v7.0.0 or later. Gen 5 embedded switches receive this capability by default with FOS v7.2.1 and later. Individual upgrade is required when upgrading directly to FOS v7.2.1 on Gen 5 embedded switches. Subsequent group operations on Gen 5 embedded switches including group upgrade are supported.

Adaptive Networking with QoS — This license was deprecated beginning with FOS v7.2. All functionality enabled by the license is now part of base FOS firmware capabilities.

Server Application Optimization — This license was deprecated beginning with FOS v7.2. All functionality enabled by the license is now part of base FOS firmware capabilities.

Integrated Routing — This license allows any port in a DCX 8510-8, DCX 8510-4, Brocade 6510, Brocade 6520, DCX-4S, DCX, 5300, 5100, 7800, 7840, or Brocade Encryption Switch to be configured as an Ex_port or VEx_port (on some platforms) supporting Fibre Channel Routing.

Encryption Performance Upgrade — This license provides additional encryption processing power. For the Brocade Encryption Switch or a DCX/DCX-4S/DCX 8510-8/DCX 8510-4, the Encryption Performance License can be installed to enable full encryption processing power on the BES or on all FS8-18 blades installed in a DCX/DCX-4S/DCX 8510-8/DCX 8510-4 chassis.

DataFort Compatibility — This license is required on the Brocade Encryption Switch or DCX/DCX-4S/DCX 8510-8/DCX 8510-4 with FS8-18 blade(s) to read and decrypt NetApp DataFort-encrypted disk and tape LUNs. DataFort Compatibility License is also required on the Brocade Encryption Switch or DCX/DCX-4S/DCX 8510-8/DCX 8510-4 Backbone with FS8-18 Encryption Blade(s) installed to write and encrypt the disk and tape LUNs in NetApp DataFort Mode (Metadata and Encryption Algorithm) so that DataFort can read and decrypt

these LUNs. DataFort Mode tape encryption and compression is supported beginning with the FOS v6.2.0 release on DCX platforms. Availability of the DataFort Compatibility license is limited; contact your vendor for details.

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, High, 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, 7840, and the DCX/DCX-4S/DCX 8510-8/DCX 8510-4 for the FX8-24 on an individual slot basis.

10GbE FCIP/10G Fibre Channel — This license enables the two 10GbE ports on the FX8-24 and/or the 10G FC capability on FC16-xx blade ports supported on DCX 8510 platforms except for the FC16-64 blade. On the Brocade 6510, Brocade 6520 this license enables 10G FC ports. This license is not applicable to Brocade 7840 or Brocade 6505.

On FX8-24:

With this license installed and assigned to a slot with an FX8-24 blade, 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

On FC16-xx:

Enables 10G FC capability on an FC16-xx blade in a slot that has this license.

On Brocade 6510, Brocade 6520:

Enables 10G FC capability on Brocade 6510 and Brocade 6520.

This license is available on the DCX/DCX-4S/DCX 8510-8/DCX 8510-4 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, 7840, and the DCX/DCX-4S/DCX 8510-8/DCX 8510-4 for the FX8-24 on an individual slot basis.

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.

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.)

ICL 8-Link — 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.

ICL POD License — This license activates ICL ports on core blades of DCX 8510 platforms. An ICL 1st POD license only enables half of the ICL ports on CR16-8 core blades of DCX 8510-8 or all of the ICL ports on CR16-4 core blades on DCX 8510-4. An ICL 2nd POD license enables all ICL ports on CR16-8 core blades on a DCX 8510-8 platform. (The ICL 2nd POD license does not apply to the DCX 8510-4.)

Enterprise ICL (EICL) License — The EICL license is required on a Brocade DCX 8510 chassis when that chassis is connected to four or more Brocade DCX 8510 chassis via ICLs either as ISLs or IFLs.

This license requirement does not depend upon the total number of DCX 8510 chassis that exist in a fabric, but only on the number of other chassis connected to a DCX 8510 via ICLs. This license is recognized/displayed when operating with FOS v7.0.1 but enforced with FOS v7.1.0 or later.

Note: The EICL license supports a maximum of nine DCX 8510 chassis connected in a full mesh topology or up to twelve DCX 8510 chassis connected in a core-edge topology. Refer to the Brocade SAN Scalability Guidelines document for additional information.

WAN Rate Upgrade 1 License — The WAN Rate Upgrade 1 license provides the additional WAN throughput up to 10 Gbps on Brocade 7840. The base configuration of Brocade 7840 without the WAN Rate Upgrade 1 license provides WAN throughput up to 5 Gbps.

WAN Rate Upgrade 2 License — The WAN Rate Upgrade 2 license provides unlimited WAN throughput (other than the hardware limit) on Brocade 7840. The WAN Rate Upgrade 2 licenses also enable the use of two 40GbE ports on Brocade 7840. The 40GbE ports cannot be configured without the WAN Rate Upgrade 2 license. A WAN Rate Upgrade 1 license must be installed on a Brocade 7840 before a WAN Rate Upgrade 2 license is installed. A WAN Rate Upgrade 1 license cannot be removed before the WAN Rate Upgrade 2 license has been removed.

Note: The WAN Rate Upgrade 1 and WAN Rate Upgrade 2 licenses apply only to Brocade 7840. They control the aggregate bandwith for all tunnels on a Brocade 7840. The entire capacity controlled by the licenses can be assigned to a single tunnel subject to hardware limitation, or a portion of the capacity can be assigned to multiple tunnels. The total bandwidth aggregated for all tunnels should not exceed the limits established by the licenses.

Temporary License Support

The following licenses are available in FOS v7.4 as Universal Temporary or regular temporary licenses:

- Fabric (E_Port) license
- Extended Fabric license
- Trunking license
- High Performance Extension license
- Advanced Performance Monitoring license (feature not supported)
- Fabric Watch license (feature not supported)
- Integrated Routing license
- Advanced Extension license
- Advanced FICON Acceleration license
- 10GbE FCIP/10GFibre Channel license
- FICON Management Server (CUP)
- Enterprise ICL license
- Fabric Vision license
- WAN Rate Upgrade 1 license
- WAN Rate Upgrade 2 license

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

Temporary and Universal Temporary licenses have durations and expiration dates established in the licenses themselves. FOS will accept up to two temporary licenses and a single Universal license on a unit. 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.

Supported Switches

FOS v7.4 supports the following platforms:

- 300, 5100, 5300, 7800, VA-40FC, Brocade Encryption Switch, DCX, DCX-4S
- 6510, 6505, 6520, 7840, DCX 8510-8, DCX 8510-4
- FC8-16, FC8-32, FC8-48, FC8-64, FX8-24, FS8-18, FCOE10-24
- FC16-32, FC16-48, FC16-64, FC8-32E, FC8-48E
- 5410, M5424, 5430, 5431, 5432, 5450, 5460, 5470, 5480, NC-5480
- 6545, 6546, 6547, 6548, M6505

Access Gateway mode is also supported by Fabric OS v7.4, and is supported on the following switches: the Brocade 300, 5100, VA-40FC, 5410, 5430, 5431, 5432, 5450, 5460, 5470, 5480, NC-5480, M5424, 6545, 6546, 6547, 6548, M6505, 6510, 6505.

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 FCOE10-24 blade conforms 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 FCOE10-24 blade:

- IEEE 802.1Qbb Priority-based Flow Control
- IEEE 802.1Qaz Enhanced Transmission Selection
- IEEE 802.1 Working Group) DCB Capability Exchange Protocol (Proposed under the DCB Task Group of IEEE 802.1
- 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
   - For dual CP platforms running FOS v6.2 and above, the supportsave command gathers information from both CPs and any AP blades installed in the chassis
   - 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 Encryption Switch, VA-40FC, 300, 5100, 5300, 6510, 6505, 6520 — On the switch ID pull-out tab located on the bottom of the port side of the switch
   - Brocade 7800, 7840 — 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 DCX, DCX 8510-8 — Bottom right of the port side
   - Brocade DCX-4S, DCX 8510-4 — 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 and DCX 8510-8/DCX 8510-4. For the Brocade DCX/DCX-4S and DCX 8510-8/DCX 8510-4 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 **licenseIdShow** command to display the License Identifier.

FOS Migration Considerations

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

FOS Upgrade and Downgrade Special Considerations

DCX/DCX-4S/DCX8510-8 units with FCOE10-24 blades running any FOS v7.3.x can be non-disruptively upgraded to FOS v7.4.0a. This upgrade is non-disruptive to both FC and FCoE traffic (when using FCOE10-24 blades). In FOS versions prior to v7.1.0, firmware upgrade is disruptive to FCoE traffic.

Any firmware activation on Brocade 7800, or DCX, DCX-4S, DCX 8510-8, DCX 8510-4 with FX8-24 will disrupt I/O traffic on the FCIP links.

For FCIP, the best practice is to always operate the switch or blade at both ends of the tunnel with the same level of Fabric OS, down to the maintenance release. Fabric OS upgrades should be done on both ends of the FCIP tunnel concurrently.

Firmware downgrade from FOS v7.4 to FOS v7.3.0c or earlier verisons on Brocade 7840 should be avoided. Otherwise, the Brocade 7840 may become faulty. (Downgrading to FOS v7.3.0b5 can be used as a workaround.)

Disruptive upgrades to Fabric OS v7.4.0a are allowed and supported from FOS v7.2.x (up to a two-level migration) using the optional "-s" parameter with the *firmwaredownload* command.

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.

Recommended Migration Paths to FOS v7.4.0a

Migrating from FOS v7.3

- Any 8G or 16G platform running any FOS v7.3.x firmware can be non-disruptively upgraded to FOS v7.4.0a.

Migrating from FOS v7.2

- Any 8G or 16G platform operating at FOS v7.2.x must be upgraded to FOS v7.3.x before non-disruptively upgrading to FOS v7.4.0a.
- Disruptive upgrade to FOS v7.4.0a from FOS v7.2 is supported.
- Firmware clean install to FOS v7.4.0a from FOS v6.4 or later without retaining any configuration is supported.

Important Notes

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

Brocade Network Advisor Compatibility

Brocade Network Advisor greatly simplifies the steps involved in daily operations while improving the performance and reliability of the overall SAN and IP networking environment. Brocade Network Advisor unifies, under a single platform, network management for SAN, LAN and converged networks. Brocade Network Advisor provides a consistent user experience, across the entire Brocade portfolio of switches, routers and adapters.

Brocade Network Advisor provides health and performance dashboards, with an easy-to-use graphical user interface and comprehensive features that automate repetitive tasks. With Brocade Network Advisor, storage and network administrators can proactively manage their SAN environments to support non-stop networking, address issues before they impact operations, and minimize manual tasks.

Brocade Network Advisor is available with flexible packaging and licensing options for a wide range of network deployments and for future network expansion. Brocade Network Advisor 12.4.0 is available in

- SAN-only edition
- IP-only edition
- SAN+IP edition.

For SAN Management, Network Advisor 12.4.0 is available in three editions:

- **Network Advisor 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 two FOS fabric at a time and up to 300 switch ports. It provides support for Brocade FC switches, Brocade HBAs / CNAs, and Fibre Channel over Ethernet (FCoE) switches.
- **Network Advisor Professional Plus**: a SAN management application designed for medium-size businesses or departmental SANs for managing up to thirty-six physical or virtual fabrics (FOS) and up to 2,560 switch ports. It supports Brocade backbone and director products (DCX 8510-4/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) / DCB switches, and Brocade HBAs / CNAs.
- **Network Advisor Enterprise**: a management application designed for enterprise-class SANs for managing up to one hundred physical or virtual fabrics and up to 15,000 switch ports. Network Advisor SAN Enterprise supports all the hardware platforms and features that Network Advisor Professional Plus supports, and adds support for the Brocade DCX Backbone (DCX 8510-8/DCX) and Fiber Connectivity (FICON) capabilities.

More details about Network Advisor's new enhancements can be found in the *Network Advisor 12.4.0 Release Notes*, *Network Advisor 12.4.0 User Guide*, and *Network Advisor 12.4.0 Installation, Migration, & Transition Guides*.

Notes:

- Brocade Network Advisor 12.4.0 or later is required to manage switches running FOS 7.4.0 or later.
- The Brocade Network Advisor seed switch should always have the highest FOS version used in the fabric.

WebTools Compatibility

FOS v7.4.0 is qualified and supported with Oracle Java version 7 update 76 and Java version 8 update 40. Please refer to the "Other Important Notes and Recommendations" section for more details.

SMI Compatibility

It is important to note that host SMI-S agents cannot be used to manage switches running FOS v7.4.

If users want to manage a switch running FOS v7.4 using SMI-S interface, they must use Brocade Network Advisor's integrated SMI agent.

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.
- To ensure that a configuration is fully supported, always check the appropriate SAN, storage or blade server product support page to verify support of specific code levels on specific switch platforms prior to installing on your switch. Use only FOS versions that are supported by the provider.
- 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	
4900, 7500, 7500e, 5000, 200E, 48K Brocade 4012, 4016, 4018, 4020, 4024, 4424	v6.2.2 or later [5]
Brocade 5410, 5480, 5424, 5450, 5460, 5470, NC-5480	v6.2.0 or later [5]
Brocade DCX, 300, 5100, 5300	v6.1.0e and later [1 5 7]
VA-40FC	v6.2.1_vfc [5], v6.2.2 or later [5]
Brocade DCX-4S	v6.2.0 or later [5 7]
Brocade DCX with FS8-18 blade(s), Brocade Encryption Switch	v6.1.1_enc or later [5]
Brocade 7800, DCX and DCX-4S with FCOE10-24 or FX8-24 blades	V6.3.0 or later
Brocade 8000[9]	V6.1.2_CEE [1] or later
Brocade DCX/DCX-4S with FA4-18 blade(s)	DCX requires v6.0.x or later [5] DCX-4S requires 6.2.x or later [4 7]
Brocade DCX 8510-8/DCX 8510-4	FOS v7.0 or later
Brocade DCX 8510-8/DCX 8510-4 with FC16-64 blade	FOS v7.3.0 or later
Brocade DCX 8510-8 with FCOE10-24 blade	FOS v7.3.0 or later
Brocade 6510	FOS v7.0 or later
Brocade 6505	FOS v7.0.1 or later
Brocade 6520	FOS v7.1 or later
Brocade 7840	FOS v7.3.0 or later
5430	FOS v7.1 or later [9]
5431, 6547, M6505	FOS v7.2 or later [9]
6548, 5432	v7.2.1 or later [9]
6545, 6546	v7.3.1 or later [9]
48000 with FA4-18 blade(s), Brocade 7600	V6.2.2 or later [5]
Mi10k, M6140 (McDATA Fabric Mode and Open Fabric Mode)	Not Supported

Multi-Protocol Router Interoperability	
Brocade 7500 and FR4-18i blade	V6.2.2 and higher [3 5 7]
McDATA SANRouters 1620 and 2640	Not Supported

NOS (VDX Platform) Interoperability	
Brocade VDX6710, VDX6720, VDX6730	NOS v2.1.1 or later [6]
Brocade VDX8770	NOS 3.0 or later
Brocade VDX6740	NOS 5.0 or later

Notes:

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

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

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

[4.] FA4-18 is not supported in a DCX/DCX-4S that is running FOS v7.0 or later

[5.] If operating with **FOS v6.2.2e** or earlier, Adaptive Networking QoS must be disabled when connecting to 16G FC platform. Otherwise, ISL will segment.

[6.] Connectivity to FC SAN is established via VDX6730 connected to FCR running FOS v7.0.1 or later. FCR platforms supported include 5100, VA-40FC, 5300, 7800, DCX, DCX-4S, DCX 8510-8, DCX 8510-4, 6510, 6520 (requires FOS v7.1 or later). For higher FCR backbone scalability (refer to separate "Brocade SAN Scalability Guidelines" documentation for details), please use 5300, 6520, DCX, DCX-4S, DCX 8510-8, and DCX 8510-4.

[7.] FR4-18i and FC10-6 are not supported on DCX/DCX-4S on FOS v7.1 or later.

[8.] Brocade 8000 is not supported with FOS v7.2 or later.

[9.] Represents the earliest major FOS version. These embedded platforms running respective dedicated FOS versions can also interoperate with FOS v7.3.

Zoning Compatibility Note:

Users are recommended to upgrade to the following versions of firmware when interoperating with a switch running FOS v7.0 or later in the same layer 2 fabric to overcome some of the zoning operations restrictions that otherwise exist:

Main code level	Patch code levels with full zoning compatibility
FOS v6.2	FOS v6.2.2d or later
FOS v6.3	FOS v6.3.2a or later
FOS v6.4	FOS v6.4.1 or later

If there are switches running FOS versions lower than the above listed patch levels in the same fabric as a switch with FOS v7.0 or later, then cfgsave and cfgenable operations **initiated** from these switches will fail if the zoning database is greater than 128KB. In such scenarios zoning operations such as cfgsave/cfgenable can still be performed successfully if initiated from a switch running FOS v7.0 or later.

SNMP Support

FOS v7.4.0 documents the supported MIBs in the Fabric OS MIB Reference document.

For information about SNMP support in Fabric Operating System (FOS) and how to use MIBs, see the Fabric OS Administrator's Guide.

Obtaining the MIBs

You can download the MIB files required for this release from the downloads area of the MyBrocade site. To download the Brocade-specific MIBs from the Brocade Technical Support website, you must have a user name and password. Use the following steps to obtain the MIBs you want.

1. On your web browser, go to http://my.brocade.com.
2. Login with your user name and password.
3. Click the downloads tab.
4. On the downloads tab, under Product Downloads, select All Operating Systems from the Download by list.
5. Select Fabric Operating System (FOS), and then navigate to the release.
6. Navigate to the link for the MIBs package and either open the file or save it to disk.

NOTE: Distribution of standard MIBs has been stopped. Download the required standard MIBs from the http://www.oidview.com/ or http://www.mibdepot.com/ website.

Blade Support

DCX/DCX-4S Blade Support

Fabric OS v7.4 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)	Supported with FOS v6.0 and above (FC8-64 requires FOS v6.4) with any mix and up to 8/4 of each. No restrictions around intermix.
FC10-6	Not supported on FOS v7.1 or later
Intelligent blade	Up to a total of 8/4 intelligent blades. See below for maximum supported limits of each blade.
Virtualization/Application Blade (FA4-18)	Not supported on FOS v7.0 or later
FCIP/FC Router blade (FR4-18i)	Not supported on FOS v7.1 or later
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/L2 CEE blade FCOE10-24	Up to a maximum of 4 blades of this type. Not supported in the same chassis with other intelligent blades or the FC8-64 port blade.
FC16-32, FC16-48, FC16-64, FC8-32E, FC8-48E	Not supported

Table 1 Blade Support Matrix for DCX and DCX-4S with FOS v7.4

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

DCX 8510-8/DCX 8510-4 Blade Support

Fabric OS v7.4 software is fully qualified and supports the blades for the DCX 8510-8 and DCX 8510-4 noted in the table below.

DCX 8510-8/DCX 8510-4 Blade Support Matrix	
FC16-32, FC16-48 16G FC blades	FOS v7.0 or later.
FC16-64 blade[2,3]	FOS v7.3 or later.

DCX 8510-8/DCX 8510-4 Blade Support Matrix	
FC8-64 64 port 8Gbit port blade	With any mix and up to 8/4 of each. No restrictions around intermix. **Note:** FC8-16, FC8-32, FC8-48 blades are *not* supported on DCX 8510 platforms.
FC8-32E, FC8-48E1	FOS v7.0.1 or later.
Intelligent blade	Up to a total of 8/4 intelligent blades. See below for maximum supported limits of each blade.
FCIP/FC Router blade (FR4-18i)	Not supported.
Virtualization/Application Blade (FA4-18)	Not Supported
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/L2 CEE blade FCOE10-24	Supported at slot 1 position only on DCX 8510-8 with FOS v7.3.0. Supported in the same chassis with FC16-32 and FC8-32E blades only. Not supported with any other port blades or intelligent blades in the same chassis. Not supported in DCX 8510-4 chassis.

Table 2 Blade Support Matrix for DCX 8510-8 and DCX 8510-4 with FOS v7.4

Note: The iSCSI FC4-16IP blade is not qualified for the DCX 8510-8/DCX 8510-4.

1. Note that 16G SFP+ is not supported in FC8-32E and FC8-48E blades

2. 8510 core blade QSFPs, part numbers 57-1000267-01 and 57-0000090-01, are not supported in FC16-64. The QSFPs supported in FC16-64, part number 57-1000294-01, are not supported on 8510 core blades either.

3. E_port connections on FC16-64 blade have the following restriction: connecting a QSFP port between a FC16-64 blade and an ICL QSFP port on a core blade is not supported.

Power Supply Requirements for Blades in DCX/DCX-4S				
Blades	**Type of Blade**	**DCX/DCX-4S** @110 VAC (Redundant configurations)	**DCX/DCX-4S** @200-240 VAC (Redundant configurations)	**Comments**
FC10-6[1], FC8-16, FC8-32, FC 8-48, FC8-64	Port Blade	2 Power Supplies	2 Power Supplies	Distribute the Power Supplies evenly to 2 different AC connections for redundancy.
FR4-18i[1]	Intelligent Blade	Not Supported	2 Power Supplies	

[1] Note that FC10-6 and FR4-18i are not supported with FOS v7.1 or later.

Power Supply Requirements for Blades in DCX/DCX-4S				
Blades	**Type of Blade**	**DCX/DCX-4S** @110 VAC (Redundant configurations)	**DCX/DCX-4S** @200-240 VAC (Redundant configurations)	**Comments**
FS8-18, FX8-24, FCOE10-24	Intelligent Blade	Not Supported	DCX: 2 or 4 Power Supplies DCX-4S: 2 Power Supplies	• For DCX with three or more FS8-18 Blades, (2+2) 220 VAC Power Supplies are required for redundancy. • For DCX with one or two FS8-18 Blades, (2) 220 VACPower Supplies are required for redundancy. • For DCX-4S, (2) 220 VAC Power Supplies provide redundant configuration with any supported number of FS8-18 Blades. • For both DCX and DCX-4S with FX8-24 blades, (1+1) 220 VAC Power Supplies are required for redundancy.

Table 3 Power Supply Requirements for DCX and DCX-4S

Typical Power Supply Requirements Guidelines for Blades in DCX 8510-8 (For specific calculation of power draw with different blade combinations, please refer to Appendix A: Power Specifications in the 8510-8 Backbone Hardware Reference Manual)					
Configured Number of Ports	**Blades**	**Type of Blade**	**DCX 8510-8** @110 VAC (Redundant configurations)	**DCX 8510-8** @200-240 VAC (Redundant configurations)	**Comments**
Any combination of 8Gb or 16Gb ports with QSFP ICLs	FC8-64, FC16-32, FC16-64, FC8-32E	Port Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies
256 16Gb ports + QSFP ICLs	FC16-32, FC16-48 (Maximum of fully populated FC16-32 blades), FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies Max 8 FC16-32 port blades
256 8Gb ports + QSFP ICLs	FC8-32E, FC8-48E (Maximum of fully populated FC8-32E blades)	Port Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies Max 8 FC8-32E port blades

Typical Power Supply Requirements Guidelines for Blades in DCX 8510-8 (For specific calculation of power draw with different blade combinations, please refer to Appendix A: Power Specifications in the 8510-8 Backbone Hardware Reference Manual)					
Configured Number of Ports	**Blades**	**Type of Blade**	**DCX 8510-8** @110 VAC (Redundant configurations)	**DCX 8510-8** @200-240 VAC (Redundant configurations)	**Comments**
192 16Gb Ports & max 2 intelligent blades (FX8-24 / FS8-18/combination) with QSFP ICLs	FC16-32, FC16-48, FC16-64, FX8-24, FS8-18	Port / Intelligent Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies Max four FC16-48 port blades and max 2 Intelligent blades
192 8Gb Ports & max 2 intelligent blades (FX8-24 / FS8-18/ combination) with QSFP ICLs	FC8-32E, FC8-48E, FX8-24, FS8-18	Port / Intelligent Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies Max four FC8-48E port blades and max 2 Intelligent blades
336 16Gb ports + QSFP ICLs	FC16-48 (Maximum of seven FC16-48 blades, with one empty port blade slot)	Port Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies Max 7 FC16-48 port blades
336 8Gb ports + QSFP ICLs	FC8-48E (Maximum of seven FC8-48E blades, with one empty port blade slot)	Port Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies Max 7 FC8-48E port blades
384 16Gb ports + QSFP ICLs	FC16-48	Port Blade	Not Supported	4 Power Supplies	200-240 VAC: For DCX 8510-8, four (2+2)1 220 VAC Power Supplies are required
384 16Gb ports + QSFP ICLs	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies

[1] When 2+2 power supply combination is used, the users are advised to configure the MAPS setting for switch Marginal State to be one Bad Power Supply.

Typical Power Supply Requirements Guidelines for Blades in DCX 8510-8 (For specific calculation of power draw with different blade combinations, please refer to Appendix A: Power Specifications in the 8510-8 Backbone Hardware Reference Manual)					
Configured Number of Ports	**Blades**	**Type of Blade**	**DCX 8510-8** @110 VAC (Redundant configurations)	**DCX 8510-8** @200-240 VAC (Redundant configurations)	**Comments**
384 8Gb ports + QSFP ICLs	FC8-48E	Port Blade	4 Power Supplies	4 Power Supplies	200-240 VAC: For DCX 8510-8, four (2+2)[1] 220 VAC Power Supplies are required
Any combination of 8Gb or 16Gb ports and intelligent blades with QSFP ICLs	FC16-32, FC16-48, FC8-64, FC8-32E, FC8-48E, FS8-18,FX8-24	Intelligent Blade / Combination	Dependent on configuration. Requires power calculation for specific configuration	2 or 4 Power Supplies, depending on configuration	For DCX 8510-8, four (2+2)[1] 220 VAC Power Supplies are required when any special purpose blade are installed
512 16Gb ports	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies
512 16Gb ports + QSFP ICLs	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200-240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies

Table 4 Power Supply Requirements for DCX 8510-8

Typical Power Supply Requirements Guidelines for Blades in DCX 8510-4 (For specific calculation of power draw with different blade combinations, please refer to Appendix A: Power Specificationsin the 8510-4 Backbone Hardware Reference Manual)					
ConfiguredNumber of Ports	**Blades**	**Type of Blade**	**DCX 8510-4** @110 VAC (Redundant configurations)	**DCX 8510-4** @200-240 VAC (Redundant configurations)	**Comments**
96 ports max with QSFP ICLs	FC16-32, FC8-32E	Port Blade	2 Power Supplies	2 Power Supplies	1+1 redundancy with 110 or 200-240 VAC power supplies
Any combination of 8Gb or 16 Gb ports and intelligent blades with QSFP ICLs	FC16-32, FC16-48, FC16-64, FC8-32E, FC8-48E, FC8-64, FS8-18, FX8-24	Intelligent Blade / Combination	Not Supported	2 Power Supplies	200-240 VAC: 1+1 Power Supplies

Table 5 Power Supply Requirements for DCX 8510-4

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

Adaptive Networking/Flow-Based QoS Prioritization

- Any 8G or 4G FC platform running FOS v6.2.2e or lower version of firmware cannot form an E-port with a 16G FC platform when Adaptive Networking QoS is enabled at both ends of the ISL. Users must disable QoS at either end of the ISL in order to successfully form an E-port under this condition.

  Users can disable QoS via portcfgQos --disable command. Please consult Fabric OS Command Reference manual for details related to portcfgQoS command.

- When using QoS in a fabric with 4G ports or switches, FOS v6.2.2 or later must be installed on all 4G products in order to pass QoS info. E_Ports from the DCX to other switches must come up AFTER 6.2.2 is running on those switches.
- When FOS is upgraded from v7.1.x to v7.2.0 or later:
  - If the Adaptive Networking license was NOT installed in v7.1.x, all ports will have QOS disabled following the firmware upgrade and links will come up in normal mode.
  - If the Adaptive Networking license was installed in v7.1.x, there will be no change in port QOS mode following the upgrade.
  - If the remote port supports QOS and QOS is not explicitly disabled on the local or remote port, the link will come up in QOS mode. Otherwise, the link will come up in normal mode.

- If FOS v7.2 or later is factory installed (or by firmwarecleaninstall), Adaptive Networking features are always available. This matches the behavior of the Brocade 6520 and all products shipping with prior versions of FOS and with the Adaptive Networking license factory installed.
    - Ports will come up in AE mode by default
    - If the remote port supports QOS and is not explicitly disabled, the link will come up in QOS mode. Otherwise, the link will come up in normal mode.

Access Gateway

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:

1. Log in to http://my.brocade.com
2. Go to Documentation > Tech Notes.
3. Look for the Tech Note on Access Gateway Device-Based Mapping in VMware ESX Server.

D_Port

- The 16Gb QSFP optics used in FC16-64 blade do not support electrical loopback and optical loopback tests. Support is limited to:
    - Link traffic tests across the 16Gb QSFPs
    - Roundtrip link latency measurements
    - Link distance measurements for links that are longer than 100 meter
- D_Port support with HBA/Adapter from Qlogic and Emulex begins with FOS v7.3.0a. FOS v7.3.1a or earlier FOS versions require the Fabric Vision license to support D_Port with 3rd party vendor HBAs. FOS v7.4.0 adds the support for D_Port with 3rd party vendor HBAs with the combination of Fabric Watch license and Advanced Performance Monitoring license. Please refer to Qlogic and Emulex documentation for specific adapter models and firmware levels required.

Edge Hold Time

- Edge Hold Time (EHT) default settings for FOS v7.x have changed from those in some FOS v6.4.x releases. The following table shows the Default EHT value based on different FOS release levels originally installed at the factory:

Factory Installed Version of FOS	Default EHT Value
FOS v7.X	220 ms
FOS v6.4.3x	500 ms
FOS v6.4.2x	500 ms
FOS v6.4.1x	220 ms
FOS v6.4.0x	500 ms
Any version prior to FOS v6.4.0	500 ms

  Gen 5 platforms and blades are capable of setting an EHT value on an individual port basis. On 8G platforms EHT is set on an ASIC-wide basis, meaning all ports on a common ASIC will have the same EHT setting. Extra care should be given when configuring EHT on 8G platforms or Gen 5 platforms with 8G blades to ensure E_Ports are configured with an appropriate Hold Time setting.

  When using Virtual Fabrics and creating a new Logical Switch when running FOS v7.1.0 or later, the default EHT setting for the new Logical Switch will be the FOS default value of 220ms. However, with FOS v7.1.0 and later, each Logical Switch can be configured with a unique EHT setting that is independent of other

Logical Switches and the Default Switch. Any Gen 5 ports (Condor3 based) assigned to that Logical Switch will be configured with that Logical Switch's EHT setting. Any 8G ports (Condor2 based) will continue to share the EHT value configured for the Default Switch.

For more information on EHT behaviors and recommendations, refer to the Brocade SAN Fabric Resiliency Best Practices v2.0 document available on www.brocade.com.

Encryption Behavior for the Brocade Encryption Switch (BES) and FS8-18

- SafeNet's KeySecure hosting NetApp's LKM (SSKM) is supported for data encryption operations with SSKM operating in PVM mode. Please see SSKM documentation for operating in PVM mode for details. Operation in HVM mode is not supported
- RASlog SPC-3005 with error 34 may be seen if the link key used by a BES/FS8-18 is re-established. Please refer to the LKM/SSKM Encryption Admin Guide for the workaround. Also, please ensure that two (2) SSKM's are present in the deployment for workaround to be performed.
- For crypto tape operations, please ensure to use Emulex FC HBA firmware/drivers 2.82A4/7.2.50.007 or higher. Use of lower level firmware/drivers may result in hosts not being able to access their tape LUNs through a crypto target container.
- Adding of 3PAR Session/Enclosure LUNs to CTCs is now supported. Session/Enclosure LUNs (LUN 0xFE) used by 3PAR InServ arrays must be added to CryptoTarget (CTC) containers with LUN state set to "cleartext", encryption policy set to "cleartext". BES/FS8-18 will not perform any explicit enforcement of this requirement.
- 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.
- The RSA DPM Appliance SW v3.2 is supported. The procedure for setting up the DPM Appliance with BES or a DCX/DCX-4S/DCX 8510 with FS8-18 blades is located in the Encryption Admin Guide.
- Support for registering a 2nd DPM Appliance on BES/FS8-18 is blocked. If the DPM Appliances are clustered, then the virtual IP address hosted by a 3rd party IP load balancer for the DPM 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.
- Hot Code Load from FOS v7.3.x to FOS v7.4 is supported. Cryptographic operations and I/O will be disrupted but other layer 2 FC traffic will not be disrupted.
- 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.
- BES/FS8-18 will reject the SCSI commands WRITE SAME, ATS(Compare and Write/Vendor Specific opcode 0xF1) and EXTENDED COPY, which are related to VAAI (vStorage APIs for Array Integration) hardware acceleration in vSphere 4.1/5.x. This will result in non-VAAI methods of data transfer for the underlying arrays, and may affect the performance of VM related operations.
- VMware VMFS5 uses ATS commands with arrays that support ATS. BES/FS8-18 does not support this command set. Use of a workaround procedure is required in order to configure encryption in a VMFS 5 environment. Please refer to Brocade Tech Note "Deployment Options for VMware VMFS-5 with Brocade Encryption" for details.
- XIV storage arrays that have been upgraded to firmware 11.2x or later required to support encryption on thin provisioned LUNs will report all XIV data LUNs as TP=Yes.

FCIP (Brocade 7800 and FX8-24)

- Any firmware activation will disrupt I/O traffic on FCIP links.
- Latency measurements supported on FCIP Tunnels:1GbE & 10GbE - 200ms round trip time and 1% loss.
- After inserting a 4G SFP in GE ports of an FX8-24 blade or 7800 switch, sometimes "sfpshow" output might display "Cannot 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 v7.2.0 or later, if the new FCIP Circuit Group feature is configured on any FCIP Circuits, a downgrade operation to pre-FOS v7.2.0 will be blocked until the feature is removed from the FCIP configuration(s).

Extention (Brocade 7840)

- Brocade 7840 does not support FCIP connection to Brocade 7800 or FX8-24.
- FOS v7.4 does not support 10G speed on the 24 16G FC ports on Brocade 7840.
- FOS v7.4 does not support VEX port on Brocade 7840.
- Running offline diagnostic tests results in FCIP tunnels down. Reboot the switch after offline diagnostic tests to recover the tunnels.
- Brocade 7840 supports Brocade 10 Gbps Tunable DWDM 80KM SFP+ optical transceiver. Following CLI command can be used to configure the transceiver usage in Brocade 7840.
- portcfgge ge_num --set -channel <channel_num>

  The channel number can have a value of 1 through 102. The detailed explanation of the values are provided in the product data sheet at the following link:

  http://www.brocade.com/downloads/documents/data_sheets/product_data_sheets/10gbe-tunable-dwdm-80km-sfp-ds.pdf
- When Brocade Network Advisor (BNA) v12.3.2 is used to download firmware on Brocade 7840, BNA reports success of firmware download prematurely when 7840 has not reached High Availability state. Customers for 7840 using BNA to download firmware should wait for extra fifteen minutes after BNA reports success to resume a work load.
- Firmware downgrade from FOS v7.4 to FOS v7.3.0c or earlier should be avoided. Otherwise, the Brocade 7840 may become faulty. (Downgrading to FOS v7.3.0b5 can be used as a workaround.)
- FOS v7.4 does not support HCL with IP Extension.
- Fast deflate compression is supported only with FC traffics only, not with IP Extension.
- IP fragmentation is not supported on the LAN side ports.
- When running IPSec, it is recommended that both sides of the extension tunnel are running the same FOS version.

FCoE/DCB/CEE (FCOE10-24)

- When upgrading a DCX/DCX-4S with one or more FCOE10-24 blades from FOS v6.x to FOS v7.0.0 or later, the user should carefully review Chapter 5 of the FOS v7.0.0 Converged Enhanced Ethernet Administrator's Guide.
- Ethernet L2 traffic with xSTP Hello timer set to less than or equal to 3 seconds may experience momentary traffic disruption during HA failover.
- 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.
- 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 FCOE10-24 if the CNA interface is toggled repeatedly over time. This issue is related to the CNA and rebooting the CNA restores connectivity.
- The FCOE10-24 support only one CEE map on all interfaces connected to CNAs. Additionally, CEE map is not recommended for use with non-FCoE traffic. QoS commands are recommended for interfaces carrying non-FCoE traffic.
- Before upgrading to FOS v6.4.1_fcoe/v6.4.1_fcoe1/v7.0.0 or later, if the CEE map "default" value already exists, the same "default" value is preserved after upgrading to FOS v6.4.1_fcoe/v6.4.1_fcoe1/v7.0.0 or later. However, if the CEE map "default" is not configured before upgrading to FOS v6.4.1_fcoe/v6.4.1_fcoe1/v7.0.0 or later, then after upgrading to FOS v6.4.1_fcoe/v6.4.1_fcoe1/v7.0.0 or later, the following CEE map "default" will be created automatically:

  cee-map default

  priority-group-table 1 weight 40 pfc

  priority-group-table 2 weight 60

  priority-table 2 2 2 1 2 2 2 2
- When upgrading from FOS v6.3.x or v6.4.x to FOS v6.4.1_fcoe/v6.4.1_fcoe1/v7.0.0 or later, the CEE start up configuration dcf.conf file will be incompatible with the FCoE provisioning changes implemented in v6.4.1_fcoe and later releases. Users can save the dcf.conf file as a backup and apply it once the firmware upgrade is completed to get the DCX/DCX-4S to the same startup configuration as in the older release.
- It is recommended that Spanning Tree Protocol and its variants be disabled on CEE interfaces that are connected to an FCoE device.
- 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. If there is a login group name conflict, the merge logic would rename the login group by including the last three bytes of the switch WWN in the login group name. As long as the OUI of the switch WWNs are identical this merge logic guarantees uniqueness in any modified login group name (switches with the same OUI will have unique last 3 bytes in WWN). However, if the participating switches have different OUIs but identical last three bytes in the switch WWNs, then the merge logic will fail to guarantee uniqueness of login group names. This will result in one of the login groups being dropped from the configuration. This means, no device can login to the login group that is dropped as a result of this name conflict. Users must create a new login group with a non-conflicting name to allow device logins.
- 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.
- Upgrading firmware on a DCX or DCX-4S with one or more FCOE10-24 blades from FOS v6.4.1_fcoe1 to FOS v7.0 or later will be non-disruptive to FCoE traffic through FCOE10-24 blades and FC traffic.
- Upgrading firmware on a DCX or DCX-4S with one or more FCOE10-24 blades from FOS v6.3.x, v6.4.x, and v6.4.1_fcoe to FOS v7.0 or later will be disruptive to any traffic through the FCOE10-24 blades.
- 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.

- The FCOE10-24 can handle 169 small FCoE frames in bursts. If you are using the 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 slot/port

  switch:admin>fcoe --enable slot/port

- When a FCOE10-24 blade is powered off during configuration replay, the interface specific configuration won't get applied. Later when FCOE10-24 blade is powered on, all physical interfaces will come up with default configurations. User can execute "copy startup-config running-config" command to apply the new configuration after powering on the FCOE10-24 blade.
- When IGMP Snooping is disabled on a VLAN, all configured IGMP groups are removed from that VLAN. User has to reconfigure the IGMP groups after enabling the IGMP snooping on that VLAN.
- FOS v7.3 adds the support of FCOE10-24 blade in DCX 8510-8 chassis with following limitations:
  - Only one FCOE10-24 blade is supported at the fixed slot 1 position. Inserting the blade into other slot positions, however, will not fault the blade.
  - An FCOE10-24 blade can co-exist with FC16-32 and FC8-32E blades only in a DCX 8510-8 chassis.
  - Only supports FCoE direct attach.
  - Layer2 Ethernet traffic is not supported.
  - If an FCoE10-24 blade is inserted into a DCX 8510-8 chassis, it is required to reboot the chassis or slot poweroff/poweron core blades. A chassis reboot or slot poweroff/poweron core blades must also be performed if the FCoE10-24 blade is removed and replaced with another blade type.

FCR and Integrated Routing

- With routing and dual backbone fabrics, the backbone fabric ID must be changed to keep the IDs unique.
- VEX edge to VEX edge device sharing will not be supported.
- The man page and help display of *fcrlsanmatrix --display* and *fcrlsan --show* command syntax should be corrected as below:

  fcrlsanmatrix --display -lsan | -fcr | -all

  fcrlsan --show -enforce | -speed | -all

Forward Error Correction (FEC)

- Though FEC capability is generally supported on Condor3 (16G capable FC) ports when operating at either 10G or 16G speed, it is not supported with all DWDM links. Hence FEC may need to be disabled on Condor3 ports when using DWDM links with some vendors by using portCfgFec command. Failure to disable FEC on these DWDM links may result in link failure during port bring up. Refer to the Brocade Fabric OS 7.x Compatibility Matrix for supported DWDM equipment and restrictions on FEC use.
- To connect between a switch and an HBA at 16 Gbps, both sides must be in the same mode (fixed speed, and FEC on or off) for them to communicate at that rate. If only one port has FEC enabled, neither port will be able to see the other. If the ports are in dynamic mode, then they may connect, but not at 16 Gbps.

FICON

- For FICON qualified releases, please refer to the *Appendix: Additional Considerations for FICON Environments* section for details and notes on deployment in FICON environments. (This appendix is only included for releases that have completed FICON qualification).

FL_Port (Loop) Support

- FL_Port is not supported on FC16-32, FC16-48, FC16-64, FC8-32E, FC8-48E, Brocade 6510, Brocade 6505, Brocade 6520, or Brocade 7840.
- The FC8-48 and FC8-64 blade support attachment of loop devices.
- 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 with no new restrictions.

Flow Vision

- Users must not specify well known FC addresses, domain controller addresses or CUP Port ID (in FMS mode) for either the source or the destination device field while defining flows.
- Flow Vision does not support port swap. Users must not create flows on ports that are already swapped and users must not swap the ports on which the flows are currently defined.
- After a HA reboot, a flow generator flow can be created if the source or the destination port is F-Port. But traffic will not be initiated. Toggling the port will enforce the restriction again to simulated ports.
- Flow Monitor does not support flows with defined LUN parameters on ingress ports on 8G platforms.
- Flow Generator traffic over VE port is supported only if no other traffic is running on any of the VE ports on that blade or switch platform. If Flow Generator traffic is run over a VE port and production traffic is run over another VE port, then the production traffic may be effected..
- The all F-Port learning flow *sys_mon_all_fport* does not support fabric mode. In a chassis with virtual fabric enabled, this flow can only be activated for a logical switch at a time.

ICLs on DCX/DCX-4S

- 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.

Port Initialization

Users may observe that a port is in "Port Throttled" state when an F_Port is being initialized. This is mostly an informational message that is shown in switchshow output indicating systematic initialization of F_Ports.

However, a port may remain in "Port Throttled" state for an extended period of time and may never come online if it fails to negotiate speed successfully with the neighboring port. Users are advised to check the speed setting of the neighboring switch port to determine the cause of the speed negotiation failure.

Example Output:

```
74    9   10   36ed40   id    N8      In_Sync   FC  Disabled (Port Throttled)
```

Port Mirroring

- Port Mirroring is not supported on the Brocade 7800.

Virtual Fabrics

- 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.
- ISL R_RDY mode is not supported in a base switch with FOS version 7.0 or higher.

WebTools

- WebTools since FOS v7.1.0 has a "SupportSave" interface. It only collects, however, information specific to WebTools. It does not contain the same information as collected by supportSave initiated through CLI or Brocade Network Advisor.
- When launching WebTools on a computer without Internet access, it could take up to 5 minutes to complete because the certificate revocation check performed for the WebTools application takes time to timeout. Users can turn off the certification revocation check on the Java control panel as a workaround.
- FOS v7.4.0 is qualified and supported with Oracle Java version 7 update 76 and Java version 8 update 40. Oracle enforces the latest JRE update to be used to launch WebTools. After JRE expiration date users will see the message "Your Java version is out of date" when launching WebTools. Users can either ignore the message by selecting the later option to proceed with launching WebTools, or install the latest JRE release and then launch WebTools. For JRE 8 users, launching WebTools with Java version 8 updates earlier than 40 is not supported.

Zoning

- There are limitations to zoning operations that can be performed from a FOS v6.x switch that is in the same fabric as a FOS v7.0 or later switch if the FOS v6.x switch is not running the recommended firmware version. Please see Fabric OS Interoperability section for details.

Read Diagnostics Parameters

- RDP on FOS v7.4 is not compatible with RDP on FOS v7.3 switches. FOS v7.3 only supports the Read Diagnostics Parameters (RDP) feature between Brocade switches both running FOS v7.3.

Link Cable Beaconing

- The Link Cable Beaconing (LCB) feature on FOS v7.4 is not compatible with the implementation in FOS v7.3.0 – FOS v7.3.0c. LCB is only supported on ISLs between two Brocade switches both running FOS v7.3.0 – FOS v7.3.0c, or both running FOS v7.3.1 or above.Support with third party vendor devices is only available with FOS v7.3.1 or above with fix for defect 540720.

Miscellaneous

- Users must also keep the RADIUS accounting port (Authentication Port+1) open in the firewall to ensure proper working of the RADIUS authentication.
- Using a Windows anonymous FTP server for supportsave collection:
- When using anonymous ftp, to avoid long delays or failure of simultaneous supportsave collections when AP blades are present in a director chassis, the number of unlimited anonymous users for a Windows FTP server should be configured as follows:
- Number of anonymous FTP connections = (Number of director chassis) + (Number of installed Application Blades x 3)
- RASlog message AN-1010 may be seen occasionally indicating "Severe latency bottleneck detected". Even though it is a "Warning" message, it is likely to be a false alarm and can be ignored.

- It is important to note that the outputs of *slotshow –p* and *chassisShow* commands also display the maximum allowed power consumption per slot. These are absolute maximum values and should not be confused with the real-time power consumption on 16G blades. The chassisshow command has a "Power Usage (Watts):" field that shows the actual power consumed in real-time on 16G blades.
- Class 3 frames that have been trapped to CPU will be discarded in the following scenarios on DCX/DCX-4S/DCX 8510 during the following conditions:
- HA failover on DCX/DCX-4S/DCX 8510 platforms while running FOS v7.0 or later firmware
- Firmware upgrade from v7.0 to a later release on Brocade 300, 5100, VA-40FC, 5300, 6510
- Firmware upgrade from v7.0.1 to a later release on Brocade 6505
- Firmware upgrade from v7.1.0 to a later release on Brocade 6520
- The QSFP information in the *sfpShow* output will indicate the ID field as all zeros. This is as designed.

  ras080:FID128:root> sfpshow 5/32
  QSFP No: 8 Channel No:0
  Identifier: 13 QSFP+
  Connector: 12 MPO Parallel Optic
  Transceiver: 0000000000000000 16_Gbps id
- 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 Brocade Network Advisor seed switch should always have the highest FOS version used in the fabric.
- For login authentication through RADIUS, Brocade switch should be able to reach RADIUS servers through TCP authentication port (default 1812) and accounting port (default 1813). Both of these ports must be kept open in any firewall settings.
- When a firmware upgrade on a Brocade 6510 switch initiated through Brocade Network Advisor results with "failed to enforce new iptable rules" error message, the switch could be inaccessible via SSH and/or Telnet. Activating (from console) a new policy with the rules of the default active policy will restore access to the switch.
- The Location ID parameter under the *configure* CLI affects routing calculations, and should remain set to the default value of 0 for normal use. Do not change the value unless explicitly instructed to do so by a Brocade Support engineer.
- Fabric OS Command Reference contains an error for the command *creditRecovMode*. The *creditRecovMode –fe_crdloss* configures time-out based credit loss detection of Condor-2 front-end ISL links. However, this feature is NOT enabled by default.
- Support for the 16G 2km ICL QSFP optics has the following notes:
  - The maximum number of ICL ports with the 2km ICL QSFP can be supported in an 8510 backbone switch with the two kilometer distance is 10, which requires 16 credits configured per Virtual Channel. More ports can be supported with less distance and fewer credits. Full 16 ICL ports can be supported with 11 credits configured per Virtual Channel for upto 1,375 meters.
  - Before the ICL ports with the 2km ICL QSFP come online, switchShow CLI command may display the port states as in-sync or shifting in and out of port fault.
  - The sfpShow CLI command displays the 16G 2km ICL QSFP incorrectly as "Length Cu: 3 (units m)" instead of the correct value 0.
  - Firmware downgrade from FOS v7.3.1 to a prior version is blocked if ICL ports with 2km ICL QSFP optics are present in the switch.
- The maximum number of ports supported for slow drain device quarantine in the same zone with a slow-draining device port is 32. If the 32-port zone limit is exceeded, the quarantine action will not be taken. Once the 32-port zone limit is reached, any new zoned device or port coming online will not be quarantined.

Defects

Closed with Code Change in Fabric OS v7.4.0a

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change.

Defect ID: DEFECT000554782	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.4.0	**Technology Area:** Firmware upload/download
Symptom: Unable to download v7.4.0 firmware with unsupported performance monitor configurations on base switch.	
Condition: Moving a default switch with TopTalker on as a base switch leads to unsupported TopTalker configurations on the base switch. Firmware download to v7.4 is blocked at this point and there is not a command to clear the toptalker as well.	
Workaround: Donot make a logical switch configured with TopTalker as base switch.	

Defect ID: DEFECT000539584	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS7.4.0	**Technology Area:** Optics
Symptom: 2KM QSFP ICL ports may see link errors such as CRC and FEC errors. The link errors may result in credit or frame loss and trigger link reset.	
Condition: Errors may be seen after any conditions that causes the port to be toggled, such as a portdisable or switchdisable.	
Recovery: Clear the stats. Toggle the port and check for link errors.	

Defect ID: DEFECT000542995	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.2.1	**Technology Area:** Access Gateway
Symptom: Customer encounters a panic when enabling access gateway through webtools and then running commands through the CLI subsequently.	
Condition: Enable AG mode in the switch through webtools.	
Recovery: Auto-recovery after panic dump.	

Defect ID: DEFECT000546724	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.4.0	**Technology Area:** FICON CUP
Symptom: Observed " -- FICU_DGB_MSG_001(D) -- Function - ficu_api_deliver_msg_from_remote_CUP() FICU Error RC(-14)" on the console.	
Condition: Normal switch operation, the message is seen when the IPC system is unable to deliver an IPC message to FICUD.	
Recovery: No recovery necessary. No loss of functionality, it is an informational non-essential message	

Defect ID: DEFECT000547349	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS7.4.0	**Technology Area:** CLI
Symptom: Powering on a slot which had quarantined port doesn't result in the port getting moved to quarantined state, until an hafailover is done	
Condition: Powering on the slot which has quarantined port	
Workaround: Remove ports from quarantined list before slotpoweroff using "sddquarantine --clear <slot/port>"	

Defect ID: DEFECT000547765	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.2	**Technology Area:** BB Credits
Symptom: Link reset events encountered on internal back-end (BE) port trunks while there are no link errors or credits lost.	
Condition: Under conditions of heavy congestion that cause frames to be dropped at internal Back-End ports and Front-End E-ports at the same time. If multiple overlapping frame drops are detected, then a Link Reset may be observed on a link even though no credits were actually lost. This defect only affects 8G Platforms.	
Workaround: Disable Front-End E-ports credit recovery.	
Recovery: Remove the source of congestion that is causing frame drops.	

Defect ID: DEFECT000547921	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.3.1	**Technology Area:** Access Gateway
Symptom: In an AG fabric or NPIV environment, device is not found or HBA detects SCSI command timeout and fabric switch stops routing AG switch/NPIV device traffic.	
Condition: This may occur when fabric switch is configured for session based zoning and a device connected to AG switch or an NPIV device that is not in any zone database, is enabled. This causes all traffic going through the same fabric switch F-port to be disrupted. This issue only impacts 16G fabric switch running FOSv7.4.0, FOSv7.3.1 and FOSv7.2.1d	
Workaround: Use hard zoning on fabric switch, or add the device into zoning database first before bringing it online.	
Recovery: Upon hitting this issue, the user may bring up ANY zoned member on AG switch or NPIV,that is using the fabric switch F-Port, to recover.	

Defect ID: DEFECT000548463	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.1.1	**Technology Area:** Port Bring-up
Symptom: Kernel panic encountered on a CP while taking over the Active Role, due to heartbeat loss, causing a cold recovery of the system.	
Condition: This may be encountered only when processing FDISC with duplicate PWWNs.	

Defect ID: DEFECT000548978	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Monitoring and Alerting Policy Suite
Symptom: During the firmware upgrade from v7.3.0 to v7.4.0, the MAPS Back-End port BAD_OS rule violations are reported for every port in the AP blades (FX8-24). The errors happen and are reported at the end of the firmware upgrade on both CP's.	
Condition: Topology: If there are any AP blades in the chassis, the BAD_OS errors may be seen after the firmware upgrade completes and the MAPS rules monitoring these counters will get triggered.	
Recovery: None of the blades in the switch, or VE ports in the AP blades get affected. So no recovery procedure is needed when the problem is seen.	

Defect ID: DEFECT000549030	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Diagnostic Port (D_Port)
Symptom: Dport test between two FC16-64 blades fail.	
Condition: If Dport on demand, or dynamic Dport or static Dport is in effect, the Dport test between two FC 16-64 blades may fail.	
Workaround: Disable Dport configuration and do not allow dynamic or on demand Dport to run.	
Recovery: Use "portdporttest --exit" to exit failed Dport test. Disable Dport configuration and do not allow dynamic or on demand Dport to run. Toggle the port.	

Defect ID: DEFECT000549168	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** Extended Fabrics
Symptom: If any VE ports are disabled non-persistently before a non-disruptive firmaredownload is performed on 7840 then, those VE ports will come up as online after the non-disruptive firmwaredownload	
Condition: Non-disruptive firmwaredownload on 7840 to FOS 7.4.0 where VE ports have been disabled non-persistently.	
Workaround: Persistently disable any disabled VE ports prior to a non-disruptive firmwaredownload.	
Recovery: Disable the VE port(s) after the non-disruptive firmwaredownload. Persistently disabled VE ports are not affected.	

Defect ID: DEFECT000549278	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** FCIP
Symptom: The 'portshow lan-stats --per-flow --tcp' command incorrectly reports 0 for the TCP TX bytes field even when LAN traffic is active.	
Condition: Issuing the 'portshow lan-stats --per-flow --tcp' command.	

Defect ID: DEFECT000549477	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Monitoring and Alerting Policy Suite (M
Symptom: MAPS might generate a transient MAPS-1021 RASLOG message to indicate switch in Critical state due to faulty port rule/thresholds has violated during CEC testing. Effect of this RASLOG does not stay very long (less than few minutes) and MAPS generates a healthy message.	
Condition: This happens during CEC IML test.	

Defect ID: DEFECT000551522	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** Tunnel Management
Symptom: At the start of non-disruptive firmware download[HCL] on VE ports if there is a Tunnel outage and the tunnel comes online later, it can result in DP-Recovery and all VEs on that DP will be disrupted.	
Condition: Tunnel outage at the start of HCL	

Defect ID: DEFECT000551787	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.4.0	**Technology Area:** Routing
Symptom: IO is disrupted after HA Failover for FCR imported devices that are configured for Staged Pair	
Condition: In an FCR setup with Staged Pair Matching configured	
Recovery: Wait approximately 6 minutes for FCR to re-import the devices after the HA Failover	

Defect ID: DEFECT000552474	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.2.1	**Technology Area:** FICON emulation
Symptom: Unable to run Teradata with Teradata FICON emulation enabled on the FCIP tunnel.	
Condition: When Teradata emulation is enabled on an FCIP tunnel and a read operation presents early ending status for a short read. This leads to an error in the FICON Teradata emulation logic and subsequent IOs fail.	
Workaround: Disable Teradata emulation on the FCIP Tunnel.	

Appendix: Additonal Considerations for z Systems (FICON) Environments

New Features Support

Not all possible combinations of features and hardware configurations are included in the FICON qualification process. Features and hardware configurations not supported for FICON may be supported for open systems environments. This appendix articulates those features and configurations tested for FICON environments and include supplemental information for users deploying FOS-based platforms in FICON environments.

FOS v7.4.0a is IBM z Systems qualified release with several new features and enhancements for FICON environments. The new supported features and functions in this release are:

- 2KM QSFP for ICLs
- Base Switch support on the 7840
- MAPS – FMS as a MAPS action (FMS CUP)
- Dynamic Load Sharing – E_port balancing
- Forward Error Correction (FEC) for FICON Express16S
- High Integrity Fabric (HIF), required feature for FICON

Notes on New Features Supported

2 KM QSFP for ICLs

Prior to Fabric OS 7.3.0, all the FE ports and ICL ports used the same buffer credit model. In Fabric OS 7.4.0a and later, in FICON environments ICL ports support a 2 km distance. To support this distance, you must use specific QSFPs and allocate a greater number of buffer credits per port.

The following points should be considered if you are attempting to support 2 km links on ICL ports:

• Only the QSFPs that have the version number "57-1000310-01" and the serial number

"HME114323P00044" support 2 km on ICLs. The second character ('M') in this serial number indicates that the QSFP supports 2 km distance. You can also use the **sfpShow** command to identify the QSFPs that support 2 km on ICL ports.

• The new credit model does not affect the HA configuration.

• You cannot downgrade from Fabric OS 7.3.0 to any earlier version if either of the following conditions is true:

- When you have plugged in the QSFPs that support 2 km on one ore more ICL ports.

- When you have configured buffer credits using the **EportCredit** command on one or more ICL

ports.

• The **portCfgEportCredits** configuration cannot have less than 5 buffer credits or more than 16 buffer credits per VC. If there are insufficient buffer credits available, the default configuration is retained and the message *Failed: already exceeds Buffer credits allowed* is displayed.

• Only a maximum of 10 ICL ports can be configured with 2 km QSFPs with 16 buffer credits per VC.

• Only a maximum of 14 ICL ports can be configured with 2 km QSFPs with 13 buffer credits per VC.

When you configure the 15th port using **portCfgEportCredit**, the message *Failed: already exceeds Buffer credits allowed* is displayed. The remaining two ports can have only 34 buffer credits. To remedy this, disable some ports and configure the remaining ports using 13 buffer credits per VC.

• If you are using the **portCfgEportCredit** command, a maximum of 16 buffer credits can be configured on all the ICL ports when all the 16 ICL ports are in the disabled state. After enabling all the ports, until the buffer credits are available, the ports will come up with the configured buffer credits. The remaining ports will come up in degraded mode. In case of remaining QoS-enabled ports, the ports will come up without QoS enabled. If all the ICL ports are QoS enabled, there will only be 448 buffer credits available for 2 km distance support.

• Due to the 2 km QSFP module limitation, the link failure counter is not reliable during module or cable removal or insertion.

Base Switch support on the 7840

FOS v7.4 enhances Virtual Fabric support on 7840 switches to include the base switch, i.e., to support XISL. FICON users can configure E_port (ISL over FC), and VE_port (ISL over GE) in base switch. The maximum number of logical switches supported — including the base switch — remains four. Two of the logical switches can support CUP.

MAPS-FMS as a MAPS action (FMS CUP)

The Monitoring and Alerting Policy Suite (MAPS) is an optional storage area network (SAN) health monitor supported on all switches running Fabric OS 7.2.0 or later. MAPS allows you to enable each switch to constantly monitor itself for potential faults and automatically alerts you to problems before they become costly failures.

MAPS tracks a variety of SAN fabric metrics and events. Monitoring fabric-wide events, ports, and environmental parameters enables early fault detection and isolation as well as performance measurements.

MAPS provides the following set of predefined monitoring policies that allow you to immediately use MAPS on activation:

• dflt_conservative_policy

• dflt_moderate_policy

• dflt_aggressive_policy

It is recommended that all IBM z Systems customers enable MAPS after upgrading to Fabric OS version supporting MAPS and use the default aggressive policy (dflt_aggressive_policy). This policy contains rules with very strict thresholds.

FOS v7.4 introduces FICON notification as a new action that enables MAPS events to be sent to FMS with detailed event information upon rule violations. FMS CUP can translate these MAPS events into FICON-specific Health Summary Check reports via the z/OS I/O Health Checker. In order to send the MAPS triggered events notification, MAPS supports the new action configurable at rule and maps global action level.

The rules with FICON notification action are part of all three default policies such as *dflt_aggressive_policy, dflt_moderate_policy and dflt_conservative_policy*. In the active policy, if FICON notification action is configured for any triggered events, then MAPS sends the notification to FMS with event information. The following information are send to FMS:

- Triggered event rule name
- Object and its type on which the event was triggered
- Severity of the event
- Condition on which the event was triggered
- Monitoring service details and the measured value

Dynamic Load Sharing-E_Port balancing

With this enhancement, when multiple paths to a domain exist, routing policy would assign routes so that the bandwidth demands from source ports are evenly distributed among all E_Ports.

E_port balance priority allows you to balance the E_port load. You can enable the E_port balance priority feature from Web Tools. When you enable the E_port balance priority feature, the E_Port load will be even across all the E_Ports of same domain during the topology change. You can select **Rebalance** or **Rebalance**

ALL to re-balance the E_Port load on a particular logical switch or on all the logical switches, without waiting for a topology change to occur.

When the **Dynamic Load Sharing (DLS)** is disabled, **Lossless Dynamic Load Sharing (DLS)** is not supported and the **E_port Balance Priority** feature also gets disabled; but the **E_port Balance Priority** can be enabled even if the DLS is in **Off** state.

The E_port balance priority is supported on the following z Systems qualified platforms at FOS 7.4.0a:

- Brocade DCX Backbone
- Brocade DCX-4S Backbone
- Brocade DCX 8510-4 Backbone
- Brocade DCX 8510-8 Backbone
- Brocade 7800
- Brocade 7840

To enable or disable E_port balance priority , perform the following steps.

1. Open the **Switch Administration** window.

2. Select the **Routing** tab.

3. Select **On** in the **E-port Balance Priority** area to enable E_Port load balance, or select **Off** to disable E_Port load balance.

- Clicking the **Rebalance** button will perform E_Port balancing on the current logical switch only and clicking the **Rebalance All** button will perform E_Port balancing on all the logical switches available.

4. Click **Apply**, and then click **OK.**

Forward Error Correction (FEC) for FICON Express16S

With the FICON Express16S generation of features, IBM z Systems added Forward Error Correction (FEC) capabilities to the Fibre Channel link protocol. FEC allows FICON channels to operate at higher speeds, over longer distances, with reduced power and higher throughput, while retaining the same reliability and robustness that FICON has traditionally been known for.

FEC is a technique used for controlling errors in data transmission over unreliable or noisy communication channels. The technique has the sender encode messages in a redundant way by using an error-correcting code (ECC). The redundancy allows the receiver to detect a limited number of errors that might occur anywhere in the message and often corrects these errors without retransmission. FEC gives the receiver the ability to correct errors without needing a reverse channel to request retransmission of data, but at the cost of a fixed, higher forward channel bandwidth.

With FEC enabled, errors that might have started to show up with the new faster link speeds can likely be corrected by the error correction technology in the optical transmit/receive ports. End users should see fewer I/O errors, thus easing the transition to the new link technologies, reducing the potential impact to any production workloads by I/O errors. For latency reduction, the entire path (end-to-end) needs to run at 16 Gbps link speed. Likewise, each link, the entire path from the channel through the switch ports to the storage subsystem, should be protected by an FEC-capable link to minimize the risk of I/O errors.

- Though FEC capability is generally supported on Condor3 (16G capable FC) ports when operating at either 10G or 16G speed, it is not supported with all DWDM links. Hence FEC may need to be disabled on Condor3 ports when using DWDM links with some vendors by using portCfgFec command. Failure to disable FEC on these DWDM links may result in link failure during port bring up. Refer to the Brocade Fabric OS 7.x Compatibility Matrix for supported DWDM equipment and restrictions on FEC use.

- To connect between a switch and an HBA at 16 Gbps, both sides must be in the same mode (fixed speed, and FEC on or off) for them to communicate at that rate. If only one port has FEC enabled, neither port will be able to see the other. If the ports are in dynamic mode, then they may connect, but not at 16 Gbps.

  NOTE: Enabling/disabling FEC is a disruptive operation

portCfgFec

Use this FOS CLI command to enable or disable Forward Error Correction (FEC) or Transmitter Training Signal (TTS) on a specified port or on a range of ports, or to display the configuration.

FEC provides a mechanism for reducing error rates during data transmissions over 16 Gbps Fibre Channel links. When FEC is enabled on a port, the sender adds systematically generated error-correcting code (ECC) to its data transmission. This mechanism allows the receiver to detect and correct errors without needing to get additional information from the sender.

By default, TTS is disabled switch-wide on all 16 Gbps platforms. If the TTS mode is enabled, the port negotiates FEC through TTS. The 16 Gbps TTS is not compatible with the more commonly used 16 Gbps 64B/66B. Thus, the TTS mode should only be enabled if a similarly TTS-capable and enabled device is connected to the port.

The Brocade implementation of FEC is supported on 16 Gbps platforms and enables the switch to recover bit errors in 16 Gbps and 10 Gbps data streams. The FEC encoding can correct one burst of up to 11 error bits in every 2,112-bit transmission. The error correction covers both frames and primitives. There is no loss of bandwidth or added transmission data rate overhead to the 16 Gbps FC link.

By default, FEC is enabled switch-wide on all 16 Gbps platforms. If FEC is already enabled on the ports, enabling FEC has no effect. If a range of ports is specified, some of which are already in the requested configuration, a notification is generated, and no action is taken for those ports only. All other ports in the specified range are updated. **Enabling or disabling FEC is disruptive to traffic.**

When used with the **–show** option, the command displays the following information for the specified ports:

Port
: The port index number

FEC Capable
: Displays YES if the port supports FEC. Displays NO if the port does not support FEC.

FEC Configured
: Displays ON if FEC is enabled on the port (default). Displays OFF if the feature is disabled.

FEC via TTS Configured
: Displays OFF if TTS is disabled on the port (default). Displays ON if the FEC negotiation via TTS feature is enabled.

FEC State
: The FEC state can be active or inactive. An active FEC state indicates that FEC is enabled and actually running. An inactive state can indicate two conditions: FEC is enabled, but not running due to some error condition (for example, FEC may not be enabled on both ends of the link). Or FEC is disabled and therefore inactive.

Use the **portCfgShow** command to display the FEC configuration along with other port parameters. Use the **islShow** command to view interswitch link-level FEC configurations. Use the **portErrshow** and **portStatShowhow** commands to monitor data transmission errors. You should see a significant reduction in CRC errors on FEC-enabled links.

FEC is supported the following links:

- Between E_Ports on all 16 Gbps platforms running Fabric OS v7.0.0 or later. Both sides of the link must be configured with port speeds of 10 Gbps and 16 Gbps.
- Between F_Ports and N_Ports in Access Gateway mode (requires Fabric OS v7.1.0 and later on the AG and the switch.

- Between Brocade 16 Gbps capable HBAs (Catapult2) Host Bus Adapters and an F_Port. The HBA must be running v3.2 or later and the switch must be running Fabric OS v7.1.0.
  FEC is compatible with QoS, Credit Recovery, and Fabric-Assigned Port WWM (FA-PWWN).
  FEC is not supported on D_Ports configured with Dense Wavelength Division Multiplexing (DWDM). The TTS mode is supported only for F_Ports. If a port initializes as an E_Port, it is disabled with a warning message and its peer port will be in "No_Light". status.

  For additional details, including examples please see the Fabric OS 7.4 Command Reference Manual.

High Integrity Fabric (HIF)

The High Integrity Fabric Feature (HIF) is required for proper operation with FICON channels. Therefore, it is recommended that customers verify HIF is enabled upon upgrade to FOS 7.3.0b or higher. If HIF is not enabled, FICON channels will go into an invalid attach state after a channel or port event occurs that requires the channels to log in to the FICON fabric.

Meeting high-integrity fabric (HIF) requirements

In a cascaded switch configuration, FICON channels use an Extended Link Service Query Security Attributes (ELS QSA) function to determine whether they are connected to a high-integrity fabric. Each switch in a high integrity fabric must have the following attributes configured:

- An insistent domain ID (IDID)
- A valid SCC policy (configured and activated)
- A fabric-wide consistency policy greater to or equal than switch connection control - strict mode (SCC:S)

NOTE

You enable the fabric-wide consistency policy on the fabric once the switch joins the fabric.

NOTE

If FMS mode is enabled before upgrading to v7.3.0, IDID, SCC_Policy, and SCC:S will be validated and the firmware attempt failed if either are incorrect. If validation is successful, HIF mode will automatically enable when the firmware installs. If a FICON channel tries to connect to a fabric switch without these features configured, the channel segments from the fabric.

Once these features are configured, you must enable the switch in High-Integrity Fabric (HIF) mode using the Fabric OS configure command. This verifies the required features are set and locks the configuration to ensure connection with the FICON channel. Once the HIF mode is set, you cannot change the IDID, fabric-wide consistency policy, and SCC policy without disabling HIF mode.

Following are considerations for using HIF mode:

- You must enable HIF mode to enable FMS mode.
- Before a Fabric OS downgrade, you must disable HIF mode. Note that this operation is not recommended for FICON and should only be used when downgrading firmware. You will receive a warning to this effect if FMS mode is enabled. If HIF is disabled, any new channel initialization would fail as the Query Security Attribute (QSA) reply from the switch to the channel will fail. The existing channel will continue to operate, however.
- Before a Fabric OS upgrade, be sure the switch has appropriate IDID, fabric-wide consistency policy, SCC policy settings are enabled so that HIF mode can enable when the firmware installs.

The following instructions are provided in the remainder of this section to configure a switch as part of a high-integrity fabric:

- Enabling insistent domain ID
- Creating and activating the SCC policy
- Enabling the fabric-wide consistency policy
- Enabling High-Integrity Fabric mode

Enabling the insistent domain ID

To enable the insistent domain ID, complete the following steps for each switch in the fabric:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the configure command and step through the interactive prompts.

a. At the "Fabric parameters" prompt, type y.

b. At the "Insistent Domain ID Mode" prompt, type y.

Creating and activating the SCC policy

Creating a switch connection control (SCC) policy defines switches allowed in the fabric.

To configure and activate an SCC policy, use the following steps:

1. Connect to the switch and log in.

2. Perform one of the following steps:

•Enter the secpolicycreate command to add all switches in the fabric, if they are connected. secpolicycreate "SCC_POLICY","*"

•Enter the secpolicyadd command to add one or more members to an existing policy. The following command is an example of adding a member using device WWNs. secpolicyadd "SCC_POLICY","wwn1;wwn2"

3. Enter the secpolicyactivate command to activate the currently defined SCC policy. This activates the policy set on the local switch or all switches in the fabric, depending on the configured fabric-wide consistency policy.

Enabling the fabric-wide consistency policy

Enable the fabric-wide consistency policy after all the switches have joined the merged fabric. If there are fabric-wide data distribution (FDD) conflicts on any of the ISLs, disable the fabric-wide consistency policy on each switch in the fabric. Once the fabric has merged successfully (use fabricShow to verify), enter the following command:

fddcfg --fabwideset "SCC:S"

Following are considerations for enabling the fabric-wide security policy:

• SCC:S enforces strict mode, which is required for FICON.

• Fabric-wide consistency policy cannot be set to strict mode on an edge fabric if the fabric connects to a FCR, although FCR front and translate domains can exist in the fabric.

Enabling High-Integrity Fabric mode

Setting High-Integrity Fabric (HIF) mode on a switch verifies that the switch meets high-integrity fabric requirements through the channel's Extended Link Services Exchange Query Security Attributes (ELS QSA) function.

Setting HIF mode locks the IDID, fabric-wide consistency policy, and SCC policy settings to ensure that the fabric is of high integrity so that it can connect with the FICON channel. You cannot change these settings without disabling HIF mode.

NOTE

HIF mode must be enabled to enable FMS mode.

To enable HIF mode, use the following steps:

1. Connect to the switch and log in using an account assigned to the admin role.

2. Enter the configure command and step through the interactive prompts.

a. At the "Fabric parameters" prompt, type y.

b. At the "High Integrity Fabric Mode" prompt, type y.

If HIF configuration requirements have not been met, an error message describes what you must configure for the command to succeed. For example, the following message states that an IDID, SCC policy or fabric-wide consistency policy have not been configured for the switch. Perform additional configuration if required, then enable HIF mode.

Error: Unable to set HIF Mode. No valid IDID settings, SCC policy and/or Fabric wide(SCC:S) configuration.