Brocade Fabric OS v7.3.1b
Release Notes v2.0

June 25, 2015

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v7.3.1b Release Notes v1.0	Initial Release	June 25, 2015
Brocade Fabric OS v7.3.1b Release Notes v2.0	Correct formatting	June 26, 2015

Contents

Overview

FOS v7.3.1b is a patch release based on FOS v7.3.1a. All hardware platforms and features supported in FOS v7.3.1a are also supported in FOS v7.3.1b. This release also contains fixes for many defects.

Resolution of Important Defects

- DEFECT000520333 - CUP remained quiescent after firmware upgrade.
- DEFECT000531192 - During firmware upgrade, hosts lost paths due to FICON filter that was not properly cleaned up.
- DEFECT000532726 - WebTools will not launch with Java 8 update 40.
- DEFECT000539584 - 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.
- DEFECT000551531 - OpenSSL Security Advisory [19 Mar 2015]: CVE-2015-0286, CVE-2015-0288, CVE-2015-0289, CVE-2015-0292. These vulnerabilities allow various maliciously crafted data could trigger segment fault, memory corruption or DOS attack.

Additional Hardware Platform Support

Brocade Fabric OS v7.3.1 merges in the support for the following embedded platforms, in addition to all hardware platforms supported in FOS v7.3.0.

- Brocade 6545 (embedded switch)
- Brocade 6546 (embedded switch)

New Features & Support

In addition to fixes for defects, FOS v7.3.1 also includes:

- Support for SmartOptics 16G DWDM 40km SFP+
    - Supported only on FC16-32 and FC16-48 blades in DCX8510 and DCX8510-4
    - Supported on 6505, 6510 and 6520 switches
- Enhancement to CLI command “swtichShow -portname" output to display the port WWNs along with the port names.

Planned Deprecation of Legacy FOS Features

Following legacy FOS features will be deprecated beginning with the FOS v7.4.0 release.

- Fabric Watch
- Advanced Performance Monitoring (APM)

For switches that do not have the Brocade Fabric Vision license or the combination of Brocade Fabric Watch license and Brocade APM license that enables the Fabric Vision features, the individual Fabric Watch license and APM license will continue to be available to facilitate the upgrade to Fabric Vision features. Users do not plan to migrate from Fabric Watch or APM to the improved capabilities in MAPS and Flow Vision will continue to be supported at the FOS v7.3.x and earlier firmware levels.

FOS v7.3.0 Feature Descriptions

New Hardware Support

FOS v7.3.1 introduces support for long distance 16G optical cable QSFP that extends the ICL connectivity up to two kilometers (km).

FOS v7.3 introduces support for the following **new** 16G FC hardware platform:

- Brocade 7840 Gen 5 FC extension switch platform that offers the following capabilities:

    - Support 24 16G FC ports, 16 10GE/1GE FCIP ports, and 2 40GE FCIP ports
    - Support maximum 40G WAN throughput with two WAN Rate upgrade licenses.
    - Support maximum 20G bandwidth on a VE port.
    - Support existing FCIP features on Brocade 7800 and FX8-24 blade.
    - Support non-disruptive firmware download.
    - Support Fabric Vision features.
    - Support increased compression performance.
    - Support stream based flow control.
    - Support out of order TCP delivery.
    - Support WAN link test tool.
- Brocade FC16-64 port blade for Brocade 8510 that offers the following capabilities:
    - 16 QSFP ports per blade provide total 64 FC ports supporting 16G, 8G, and 4G speeds.
    - 512 16G FC ports in a fully populated Brocade 8510-8 chassis.

FOS v7.3 introduces the support of the **existing** FCOE10-24 blade in a Brocade **8510-8** chassis.

FOS v7.3 supports all hardware platforms supported by FOS v7.2.x.

New FCIP Features on Brocade 7840

In addition to the existing FCIP features supported on Brocade 7800 and FX8-24, FOS v7.3 supports the following new FCIP features on Brocade 7840.

- Support maximum 40G WAN throughput.
- Support maximum 20G bandwidth on a VE port.
- Non-disruptive firmware download.
- Fabric Vision for Extension.
    - ClearLink Diagnostic Port (D_Port) on all FC ports.
    - Monitoring and Alerting Policy Suites (MAPS) for FCIP QoS, tunnels, and circuits.
    - Full Flow Vision capabilities on all FC ports.
- Ethernet Jumbo Frame
- IPSec enhancement
- Adaptive Rate Limiting (ARL) enhancements
- Increased compression performance
- Path MTU Discovery
- Stream based flow control
- Out of order TCP delivery
- WAN test tool

Support maximum 40G WAN throughput

FOS v7.3 supports maximum 40G WAN throughput on Brocade 7840. The maximum throughput is supported with two WAN Rate Upgrade licenses. The base configuration without either WAN upgrade license supports maximum 5G WAN throughput.

Support maximum 20G bandwidth on a VE port

FOS v7.3 supports on Brocade 7840 10 VE mode with maximum 20G bandwidth on a VE port and 20 VE mode with maximum 10G bandwidth on a VE port. End users can create single FCIP circuit with 20G bandwidth or create multiple circuits to load balance with different bandwidths that sum to 20G.

Non-disruptive Firmware Download

FOS v7.3 supports firmware download on Brocade 7840 without disruption to FCIP links. During a non-disruptive firmware download, throughput of individual FCIP tunnels are maintained, while the total bandwidth is limited to half of the maximum bandwidth supported on the platform.

Fabric Vision for Extension

FOS v7.3 supports and expands Fabric Vision features for Brocade 7840 Extension platform. These include:

- ClearLink Diagnostic Port (D_Port) on all FC ports to diagnose FC link optics and cable problems.
- Monitoring and Alerting Policy Suites (MAPS) enhancements to provide pre-defined threshold and alerting rules for FCIP statistics at QoS level, tunnel level, and circuit level and capture FCIP specific violations in MAPS dashboard.
- Full Flow Vision feature support on all FC ports to provide broad visibility, deep insight, and pre-production validation for traffic between data centers across FCIP links.

Ethernet Jumbo Frame

FOS v7.3 supports a Jumbo IP frame with MTU up to 9216 bytes on Brocade 7840.

IPSec Enhancements

FOS v7.3 increase IPSec performance on Brocade 7840 with near line-rate throughput. FOS v7.3 implements IPSec configuration through a policy applied to a FCIP tunnel. IPSec supports both IPv4 and IPv6 and jumbo frames.

Adaptive Rate Limiting (ARL) Enhancements

FOS v7.3 implements two new ARL algorithms, Modified Multiplicative Decrease and Time-based Decrease, to provide additional performance tailored to network conditions. In addition, ARL ramp up time has been decreased from 10s to 1s comparing to Brocade 7800.

Increased Compression Performance

FOS v7.3 supports increased compression performance on FC data frames on Brocade 7840 before they are sent through FCIP channels. End users can choose None, Aggressive Deflate, Deflate, and Fast Deflate compression algorithm to choose from the highest compression ratio but lowest pre-compression throughput at 10G to lowest compression ratio but highest pre-compression throughput at 40G.

Path MTU Discovery

FOS v7.3 supports path MTU discovery on Brocade 7840 to automatically discover IP MTU settings over the WANs.

Stream Based Flow Control

FOS v7.3 supports stream based flow control on Brocade 7840 to isolate slow devices from affecting performance of other devices for emulated devices sharing the same VE_Port.

Out of Order TCP Delivery

FOS v7.3 supports out of order TCP delivery on Brocade 7840 over WAN connections to minimize retransmission of FC frames in a scenario of TCP packet loss.

WAN Test Tool

FOS v7.3 supports a WAN test tool on Brocade 7840 to generate test traffic over a pair of IP addresses to test a WAN path for any network issue.

Monitoring and Alerting Policy Suite (MAPS) Enhancements

FOS v7.3 has a number of important MAPS feature enhancements. These include:

- Monitor Fabric Performance Impact

- Monitor new FCIP statistics on Brocade 7840
- Monitor fabric scalability limits
- Monitor ClearLink Diagnostic ports
- Monitor Ethernet management ports
- Monitor Flow Vision learning flows
- Support Port Decommissioning as an action
- Support dynamic groups
- Support port group augmentation
- Usability enhancements

Monitor Fabric Performance Impact

FOS v7.3 supports automatic monitoring and alerting of latency bottleneck conditions through pre-defined thresholds and alerts in all pre-defined policies in MAPS. The advanced monitoring capabilities identify ports in two latency severity levels and provide intuitive reporting in MAPS dashboard under a new Fabric Performance Impact category.

Monitor FCIP statistics

FOS v7.3 supports new monitoring elements (RTT, Jitter) in the FCIP circuit group, adds a FCIP tunnel group to monitor tunnel state change and throughput, adds 4 FCIP tunnel QoS groups to monitor throughput and packet loss for each QoS priority. These new monitoring elements and groups are included in MAPS pre-defined policies and supported only on Brocade 7840.

Monitor fabric scalability limit

FOS v7.3 supports new monitoring elements in the switch group to monitor them against the fabric scalability limits supported by Brocade. These elements include number of device connections in a layer2 fabric, number of imported devices in a metaSAN, number of FCRs in a backbone fabric, and zoning database size. These new monitoring elements are included in MAPS pre-defined policies.

Monitor ClearLink Diagnostic (D_Port) ports

FOS v7.3 supports new monitoring elements for port error statistics (CRC, ITW, PE, LF, and LOSS_SYNC) in a new D_Port logical group to monitor D_Port tests so that the test results can be determined by thresholds in the MAPS rules. These new monitoring elements and groups are included in MAPS pre-defined policies.

Monitor Ethernet management port

FOS v7.3 supports monitoring Ethernet management port state in a new Ethernet port group to generate alerts if states for Ethernet management ports are changed. These new monitoring elements and group are included in MAPS pre-defined policies.

Monitor Flow Vision learning flows

FOS v7.3 supports importing and monitoring of learning flows created through Flow Vision in MAPS. Administrators can use this capability to configure thresholds and alerts for application flows without knowing the source or destination device identities in advance.

Support Port Decommissioning as an action

FOS v7.3 supports port decommissioning as an action that can be triggered by MAPS rules. With port decommissioning, ports can be gracefully shutdown in the event of violations without I/O interruption. FOS v7.3 supports port decommissioning on E_Port natively through MAPS. For port decommissioning on F_Port, Brocade Network Advisor 12.3 is required.

Support dynamic group based on user defined pattern

FOS v7.3 introduces dynamic group to enhance logic group definition for port objects. Administrators can create custom groups whose membership dynamically changes based on user defined port identity traits.

Support port group augmentation

FOS v7.3 implements port group augmentation to pre-defined groups and dynamic groups so that administrators can make small adjustments to group memberships without having to create a new group.

Usability enhancements

FOS v7.3 has a number of usability enhancements to MAPS. These include:

- Change *mapssam* CLI to display system CPU, memory, and flash usage.
- Change *mapsrule* and *logicalgroup* CLIs to make deletion of rules and groups easier.
- Add a new option to *mapsConfig* CLI to send test emails to validate email configuration.

Flow Vision Enhancements

FOS v7.3 has a number of important Flow Vision enhancements to the Flow Monitor, Flow Generator, and Flow Mirror functionalities.

Flow Monitor enhancements

FOS v7.3 extends the learning capability to Flow Monitor on E_Port and Ex_Port. FOS v7.3 also supports Flow Monitor for static and learning flows on XISL ports and backbone E_Port. These enhancements allow administrators to apply Flow Monitor function at all point of interests in most supported SAN topologies.

Flow Mirror enhancements

FOS v7.3 introduces Local Flow Mirror to mirror application flows to a mirror port on the same local switch where the flows are defined. This feature enables administrators to attach external analyzers to the mirror port to capture all frames belonging to the flows for deep analysis. FOS v7.3 enhance Flow Mirror to mirror flows originated from switch CPU and egress on a port, to mirror flows on either ingress or egress on F_Port and F_Port trunks. FOS v7.3 adds the support of combination of *-frametype* and *-ingrport* keywords and combination of *-frametype* and *-bidir* keywords in flow definition for Flow Mirror.

Flow Generator enhancements

FOS v7.3 introduces a system pre-defined flow *sys_gen_all_simports* for Flow Generator to generate test traffic from every SIM port in a switch to all the other SIM ports. This allows administrators to fully stress test a switch before deployment.

Miscellaneous Flow Vision enhancements

FOS v7.3 supports duplicated flow definition to be created but not activated in a switch. Administrators can create flows with the same parameters but for different Flow Vision functions. FOS v7.3 increases the maximum number of flows on fixed port switches to 128 user-defined flows and 128 sub flows and on backbone switches to 512 user-defined flows and 512 sub flows.

ClearLink Diagnostic (D_Port) Enhancements

FOS v7.3 implements following important D_Port feature enhancements.

D_Port and MAPS Integration

FOS v7.3 integrate D_Port test with MAPS threshold based monitoring. Administrators can use this ability to automatically monitor D_Port tests and determine D_Port test success or failure base on threshold settings within MAPS.

Dynamic D_Port and On-demand D_Port

FOS v7.3 implements dynamic D_Port and on-demand D_Port modes on ISLs. With these modes, administrators can configure D_Port test to be run automatically on ISLs after switch enable, slot enable, or port persistent enable.

D_Port Provision

FOS v7.3 implements D_Port provision list to be configured by CLI command portcfgdport (via --provision option). Ports on the pre-provisioned list do not need to be disabled before being configured as D_Port.

portCfgDport Show Result

FOS v7.3 enhances the D_Port test result displayed by portCfgDport command (via --show option) to clearly identify loopback connection type or remote port index.

Port LED Display D_Port Result

FOS v7.3 implements visually display D_Port test failure by flashing yellow on the port LED.

D_Port on FC16-64 Blade QSFPs

FOS v7.3 implements D_Port test on the FC compliant QSFPs for FC16-64 blade. Electrical loopback and optical loopback tests are not supported on these QSFPs. Only link saturation test and link distance and latency measurements are performed.

Read Diagnostics Parameters

FOS v7.3 introduces the Read Diagnostics Parameters feature to support reporting diagnostics parameters associated with optics and media for any link between Nx_port and Fx_port from any point within a fabric. Administrators can use this ability to discover and diagnose link related errors or degrading conditions from a single point anywhere within a fabric.

Link Cable Beacon (Port Peer Beacon)

FOS v7.3 introduces the support of Link Cable Beacon feature, with which administrators can run the *portpeerbeacon* command to turn on port LED beacon on both end of a link cable connection. Administrators can use this feature to quickly identify peer ports of a connection without physically tracing the cables in a data center.

E_Port Balance Priority Routing

FOS v7.3 enhances routing policy with the E_Port Balance Priority option. 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.

FCR enhancements

FOS v7.3 adds a number of enhancements to FCR.

lsanZoneShow Change

FOS v7.3 enhances CLI lsanZoneShow (via -d option) to display the fabric IDs for devices exist in a fabric and devices imported to a fabric.

lsCfg Change

FOS v7.3 enhances CLI lsCfg (via --show -n option) to display additional information for a logical switch.

Fabric Alias Name

FOS v7.3 supports assigning alias names to each edge fabric IDs. Administrator can use the fabric alias name to represent each edge fabric.

Security Enhancements

FOS v7.3 has a number of important security enhancements.

FCAP and DH-CHAP Enhancements

FOS v7.3 supports SHA-256 hashing algorithm for FCAP and DH-CHAP in both FIPS mode and non-FIPS mode to provide stronger security.

In-flight Encryption Enhancements

FOS v7.3 supports in-flight encryption with session keys derived from FCAP. With this enhancement, administrators can use FCAP and in-flight encryption features at the same time.

Fabric-wide Consistency Policy Enhancements

FOS v7.3 supports FCRs to be present in a fabric with strict fabric-wide consistency policy configuration. Administrators can turn on strict fabric-wide consistency policy even when an FCR is connected to the fabric via an Ex_Port.

Open Source Software Packages

FOS v7.3 upgrades a number of important open source software packages (openSSH, openSSL, Apache) to provide stronger security.

Access Gateway Enhancements

FOS v7.3 implements following Access Gateway (AG) enhancements.

ClearLink Diagnostics (D_Port) Support on AG

FOS v7.3 supports dynamic D_Port on connections between an AG and an HBA to allow automatically start D_Port test requested by an HBA.

User Account and Password Distribution to AG

FOS v7.3 supports user account and password database distribution from a native switch to an AG so that user accounts and passwords can be managed the same way as native switches in a fabric.

Fabric Device Management Interface (FDMI) Data Access on AG

FOS v7.3 adds the support of accessing device information for devices that are registered with FDMI and connected through AGs.

Zoning Enhancements

FOS v7.3 enhances zoning to disallow two fabrics with empty zoning configuration to merge if one fabric has All Access as default zone access mode and the other has No Access as default zone access mode. This enhancement prevents the fabric with All Access default zone access mode from losing all device connections due to converting to No Access default zone access mode after fabrics merging.

High Integrity Fabric

FOS v7.3 introduces support of High Integrity Fabric mode to ensure strict and consistent fabric configurations required by a FICON fabric, which include Insistent Domain ID and strict fabric-wide Switch Connection Control policy. Administrators can use the High Integrity Fabric mode to enforce these configurations for a FICON fabric.

RAS Enhancements

FOS v7.3 implements the following RAS enhancements.

Frame Viewer (Class 3 Discard Log) Enhancements

FOS v7.3 enhances Frame Viewer to capture two new types of class 3 discard frames. The new discard types captured include destination unreachable frames and unroutable frames.

Audit Log for Class 3 Discard Frames

FOS v7.3 adds to audit log message for each class 3 discard frame. This ability to allow administrator to configure audit log to send class 3 discard frame messages to a centralized syslog server, which does not have size limitation of a switch Frame Viewer log.

Forward Error Correction (FEC) Enhancements

FOS v7.3 adds the ability to allow FEC capability negotiation during speed negotiation in Transmitter Training Signal. This ability can be configured by existing CLI command portCfgFec.

Firmware Download Enhancement

FOS v7.3 introduces firmware sync ability for the firmware on an active CP to be automatically synced to a standby CP after the standby CP is hot-plugged into a backbone switch chassis. Administrator can configure this ability on their chassis to enable quick operational replacement of a standby CP.

Rolling Reboot Detection Enhancements

FOS v7.3 enhances the rolling reboot detection feature to detect and stop a rolling reboot in disabled FOS switch state as a first attempt. This would enable an administrator to capture more diagnostic information.

New external RASLOG for Link Reset

FOS v7.3 adds a new external RASLOG (Cx-1014) for Link Reset due to credit loss for both front-end and back-end ports.

supportInfoClear Command

FOS v7.3 introduces a new CLI command supportInfoClear to clear a number of statistics counters and logs. This command can help administrators to quickly reset the counters and logs on behalf of switch vendors in support scenarios.

Brocade 8510 ICL Scalability Enhancement

FOS v7.3 increases the supported number 8510 chassis connected via ICL in a core-edge topology to twelve switches.

Miscellaneous Enhancements

trunkShow CLI Enhancement

FOS v7.3 adds to CLI trunkShow (via -swname option) to display the switch name of the neighboring switch connected on the other end of trunked ports.

fabricShow CLI Enhancement

FOS v7.3 adds to CLI fabricShow (via -version option) to display the firmware version of each switch listed in the fabricShow output.

portShow and portName CLI Enhancement

FOS v7.3 enhances the CLI portShow and portName to display as port name the host name registered with FDMI for the host system attached to that port. Administrators must enable the “Display FDMI Host Name” configuration via the configure CLI.

fspfShow and lsdbShow CLI Enhancement

FOS v7.3 changes fspfShow and lsdbShow CLI output to omit all zero value to be listed in port bitmap values.

Device Probing and Update on ALPA 0xC0 and 0x40

FOS v7.3 enhances FCP probing for devices connected to a port with ALPA 0xC0 and 0x40 to obtain the device information for NS entry.

For base devices that logged in with ALPA 0xC0 and 0x40, FOS v7.3 provides the ability to update NS entries when these base devices perform logout. Administrators can turn on this update mode to ensure NS and login database consistency with "F-port Device Update Mode" option under the "Fabric parameters" section of the configure CLI. This option can only be changed when a switch is disabled.

NPIV Base Device Logout Enhancements

FOS v7.3 enhances NPIV by allowing NPIV devices remain logged in on a port to a fabric when the base device on the same port performs a logout. Administrator can configure this feature via the portCfgFlogiLogout CLI.

fosExec Remote Execution

FOS v7.3 adds the ability to execute a FOS CLI command via fosExec CLI on a remote domain in the fabric. Administrators can enable this capability to execute CLI commands on multiple switches from a single switch in a fabric.

CS_CTL QoS Enhancements

FOS v7.3 enhances CS_CTL based QoS feature by reporting the CS_CTL auto mode in responses to device FLOGI, FDISC, and PLOGI requests.

bottleneckMon CLI Change

FOS v7.3 deprecates the back-end credit recovery options in the bottleneckMon CLI. These options are supported via the existing creditRecovMode CLI.

Maximum Auto Speed Negotiation

FOS v7.3 allows configuring a maximum speed for port auto speed negotiation with CLI portcfgspeed (via -m option). Administrators can use this to control the maximum speed a device is allowed to join a fabric but still allow port speed to be auto negotiated.

Back-end credit recovery on FX8-24 blade

FOS v7.3 enhances back-end credit loss detection and recovery to back-end links on FX8-24 with the existing CLI command creditRecovMode.

aptPolicy change

FOS v7.3 deprecates AP policy related configuration from the CLI command aptPolicy. AP policy is used only by FR4-18i blade, which is not supported since FOS 7.1.

slotPowerOn and slotPowerOff enhancement

FOS v7.3 supports slotPowerOn and slotPowerOff command on core blades in a DCX/DCX-4 or DCX 8510/DCX 8510-4 chassis. Administrators can use this command to power on or off a core blade without physical presence.

Port Transition from Persistent Disabled to Disabled

FOS v7.3 supports directly transition a persistently disabled port to the disabled state without having to persistently enable the port first. Administrator can configure this option via the new portCfgPersistence command

portBeacon Change

FOS v7.3 enhances the portBeacon command to list all beaconing ports in a switch (via -all option).

ethif Command

FOS v7.3 introduces a new CLI command ethif to manage the switch Ethernet management interfaces. With this command, administrator can configure and show the state Ethernet management interfaces.

haRedundancy Command

FOS v7.3 introduces a new CLI command haRedundancy to display switch uptime and HA redundancy settings for a backbone switch.

Optionally Licensed Software

Fabric OS v7.3 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—Enables performance monitoring of networked storage resources. This license includes the Top Talkers feature.

Brocade Fabric Watch — Monitors mission-critical switch operations. Fabric Watch includes Port Fencing 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. (Functionality requires support by attached device, availability TBD).

Fabric Vision license also enables Fabric Watch and Advanced Performance Monitoring functionalities without requiring Brocade Fabric Watch or Brocade Advanced Performance Monitoring license (with FOS v7.2 and later only).

Note:

> If installed on a switch operating with FOS v7.1.x, the Fabric Vision license will be displayed as "Fabric Insight". If installed on a switch operating with FOS v7.0.x or earlier, the Fabric Vision license will be displayed as "Unknown". Fabric Vision features are not supported under FOS v7.1.x or earlier.

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—Adaptive Networking provides a rich framework of capability allowing a user to ensure high priority connections obtain the bandwidth necessary for optimum performance, even in congested environments. The QoS SID/DID Prioritization and Ingress Rate Limiting features are the first components of this license option, and are fully available on all 8Gb and 16Gb platforms.

Note :

With FOS v7.2, the Adaptive Networking license has become part of the base FOS firmware, and features under this license no longer require the license to be installed. Customers that wish to have these capabilities without purchasing the license are required to upgrade to FOS v7.2 or later.

Brocade 6520 does not require the Adaptive Networking with QoS license to enable the capabilities associated with this license. These capabilities are included by default on the Brocade 6520.

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

Note :

With FOS v7.2, Server Application Optimization license has become part of the base FOS firmware, and features under this license no longer require the license to be installed. Customers that wish to have these capabilities without purchasing the license are required to upgrade to FOS v7.2 or later.

Brocade 6520 does not require the SAO license to enable the capabilities associated with this license. These capabilities are included by default on the Brocade 6520.

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.

Note that 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 v7.3 as Universal Temporary or regular temporary licenses:

- Fabric (E_Port) license
- Extended Fabric license
- Trunking license
- High Performance Extension license
- Advanced Performance Monitoring license
- Fabric Watch license
- 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 v7.3.1 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 v7.3, 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.

The Brocade 8000 is not supported with FOS v7.2.0 and later.

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 DCB Capability Exchange Protocol (Proposed under the DCB Task Group of IEEE 802.1 Working Group)
- FC-BB-5 FCoE (Rev 2.0)

Technical Support

Contact your switch supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information immediately available:

1. General Information
    - Technical Support contract number, if applicable
    - Switch model

- Switch operating system version
- Error numbers and messages received
- **supportSave** command output and associated files
  - 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.

1. **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 units running any FOS v7.2.x can be non-disruptively upgraded to FOS v7.3.1b. This upgrade is non-disruptive to both FC and FCoE traffic (when using FCOE10-24 blades).

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.

Disruptive upgrades to Fabric OS v7.3.1b are allowed and supported from FOS v7.1.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 v7.3.1b

Migrating from FOS v7.2

Any 8G or 16G platform running any FOS v7.2.x firmware can be non-disruptively upgraded to FOS v7.3.1b.

Migrating from FOS v7.1

Any 8G or 16G platform operating at FOS v7.1.x must be upgraded to FOS v7.2.x before non-disruptively upgrading to FOS v7.3.1b.

Disruptive upgrade to FOS v7.3.1b from FOS v7.1 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 12.3.0 is available in

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

For SAN Management, Network Advisor 12.3.0 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 one FOS fabric at a time and up to 1,000 switch ports. It provides support for Brocade FC switches, Brocade HBAs / CNAs, and Fibre Channel over Ethernet (FCoE) 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 thirty-six physical or virtual fabrics and up to 9,000 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 12.3.0 Release Notes, Network Advisor 12.3.0 User Guide, and Network Advisor 12.3.0 Installation, Migration, & Transition Guides.

Note:

Brocade Network Advisor 12.3.0 or later is required to manage switches running FOS 7.3.0 or later.

The Brocade Network Advisor seed switch should always have the highest FOS version used in the fabric.

WebTools Compatibility

FOS v7.3.1b is qualified and supported with Oracle Java version 7 update 80 and Java version 8 update 45. Please refer to 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 v7.3.

  If users want to manage a switch running FOS v7.3 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_CEE1 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]

Supported Products and FOS Interoperability	
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

Table 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

Starting with FOS v7.2.0, the *Fabric OS MIB Reference* document is not updated. You can obtain the latest MIBs from the downloads area of MyBrocade site after logging in.

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.

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.

FOS v7.3.0a Changes in SNMP MIBs and Objects

This release introduces the following changes in MIBs and objects.

New MIBs

There are no new MIBs introduced in this patch release.

Modified MIBs

The "swIODState" MIB object is newly added to the **SW.mib** to display the In-Order delivery (IOD) state.

MIB Object and OID	Description
swIODState 1.3.6.1.4.1.1588.2.1.1.1.1.38	The MIB object represents the IOD feature state. Possible values are: • 1 – enabled • 2 – disabled • 3 – unknown

FOS v7.3.0 Changes in SNMP MIBs and Objects

This release introduces the following changes in MIBs and objects:

New MIBs

There are no new MIBs introduced in this release.

Updated MIBs

The following existing MIBs are supported for Brocade 7840 platform.

- **BRCD-FCIP-EXT-MIB**

Table Name	Is Supported	Description
fcipExtendedLinkTable	Yes	This table contains statistical information about FCIP tunnel compression, retransmission, packet loss, and latency details. The information stored in this table is returned in response to **portshow fciptunnel** commands.
fcipConnStatsTable	Yes	The table contains statistical information about FCIP tunnel compression, retransmission, packet loss, and latency details. **Note:** This table shows circuits and TCP connections stats. However, for Brocade 7840 platform this table shows only circuit stats.

- **IF-MIB**

Table Name	Is Supported	Description
ifTable	Yes	This table contains the statistics of switch interfaces including FCIP tunnels.
ifXTable	Yes	This table is enhanced version of ifTable.
ifTestTable	No	Not supported.
ifStackTable	No	Not supported.
ifRcvAddressTable	No	Not supported.

- **FCIP-MGMT-MIB**

Table Name	Is Supported	Description
fcipEntityInstanceTable	Yes	This table contains the information related to FCIP entities.
fcipLinkErrorsTable	No	Not supported.
fcipLinkTable	Yes	This table contains the information about link of FCIP entities.
fcipTcpConnTable	No	Not supported.

ifRcvAddressTable	No	Not supported.

MIB Objects

fcipExtendedLinkTable

This table contains statistical information about FCIP tunnel compression, retransmission, packet loss, and latency details.

MIB Object and OID	Description
fcipExtendedLinkIfIndex 1.3.6.1.4.1.1588.4.1.1.1	The ifIndex value of the virtual interface corresponding to the FCIP tunnels running over TCP/IP.
fcipExtendedLinkTcpRetransmits 1.3.6.1.4.1.1588.4.1.1.2	The number of retransmitted packets.
fcipExtendedLinkTcpDroppedPackets 1.3.6.1.4.1.1588.4.1.1.3	The number of dropped packets.
fcipExtendedLinkTcpSmoothedRTT 1.3.6.1.4.1.1588.4.1.1.4	The round trip time (latency) in milliseconds for a transfer over an FCIP tunnel.
fcipExtendedLinkCompressionRatio 1.3.6.1.4.1.1588.4.1.1.5	The ratio between compressed bytes and raw bytes over an FCIP tunnel.
fcipExtendedLinkRawBytes 1.3.6.1.4.1.1588.4.1.1.6	The total number of raw bytes sent or received.
fcipExtendedLinkCompressedBytes 1.3.6.1.4.1.1588.4.1.1.7	The total number of compressed bytes received over an FCIP tunnel.
fcipExtendedLinkConnectedCount 1.3.6.1.4.1.1588.4.1.1.8	The total number of TCP session connections.
fcipExtendedLinkRtxRtxTO 1.3.6.1.4.1.1588.4.1.1.9	A counter containing retransmit packets due to timeout.
fcipExtendedLinkRtxDupAck 1.3.6.1.4.1.1588.4.1.1.10	A counter containing retransmit packets due to duplicate acknowledgement.
fcipExtendedLinkDupAck 1.3.6.1.4.1.1588.4.1.1.11	A counter containing duplicate acknowledgement packets.
fcipExtendedLinkRtt 1.3.6.1.4.1.1588.4.1.1.12	The round trip time in milliseconds.
fcipExtendedLinkOoo 1.3.6.1.4.1.1588.4.1.1.13	A counter containing TCP out-of-order.
fcipExtendedLinkSlowStarts 1.3.6.1.4.1.1588.4.1.1.14	A counter containing slow starts.

fcipConnStatsTable

This table contains statistical information about FCIP circuit and connection compression, retransmission, packet loss, and latency details. For Brocade 7840 platform this table shows only circuit stats.

MIB Object and OID	Description
xfcipEntityId 1.3.6.1.4.1.1588.4.2.1.1	The FCIP entity identifier.
xfcipLinkIfIndex 1.3.6.1.4.1.1588.4.2.1.2	The ifIndex value of the virtual interface corresponding to the FCIP Link running over TCP/IP.
xfcipLinkIndex 1.3.6.1.4.1.1588.4.2.1.3	An arbitrary integer that uniquely identifies one FCIP link within an FCIP entity.
xfcipExtendedLinkTcpRetransmits 1.3.6.1.4.1.1588.4.2.1.4	The number of retransmitted packets.
xfcipExtendedLinkTcpDroppedPackets 1.3.6.1.4.1.1588.4.2.1.5	The number of dropped packets.
xfcipExtendedLinkTcpSmoothedRTT 1.3.6.1.4.1.1588.4.2.1.7	The round trip time (latency) in milliseconds.
xfcipExtendedLinkCompressionRatio 1.3.6.1.4.1.1588.4.2.1.6	The compression ratio of the link.
xfcipExtendedLinkRawBytes 1.3.6.1.4.1.1588.4.2.1.8	The total number of raw bytes sent or received.
xfcipExtendedLinkCompressedBytes 1.3.6.1.4.1.1588.4.2.1.9	The total number of compressed bytes sent or received.

ifTable

This table contains the statistics of switch interfaces including FCIP tunnels.

MIB Object and OID	Description
ifIndex .1.3.6.1.2.1.2.2.1.1	The interface index.
ifDesc .1.3.6.1.2.1.2.2.1.2	The description of the interface.
ifType .1.3.6.1.2.1.2.2.1.3	The media type.
ifMtu .1.3.6.1.2.1.2.2.1.4	The largest size packet that can be transmitted.
ifSpeed .1.3.6.1.2.1.2.2.1.5	The interface speed in Mbps.

MIB Object and OID	Description
ifPhysAddress .1.3.6.1.2.1.2.2.1.6	The physical address of the interface.
ifAdminStatus .1.3.6.1.2.1.2.2.1.7	The admin status of the interface
ifOperStatus .1.3.6.1.2.1.2.2.1.8	The operational status of the interface.
ifLastChange .1.3.6.1.2.1.2.2.1.9	The operational state time.
ifInOctets .1.3.6.1.2.1.2.2.1.10	The number of received bytes.
ifInUcastPkts .1.3.6.1.2.1.2.2.1.11	The number of received unicast packets.
ifInNUcastPkts .1.3.6.1.2.1.2.2.1.12	This object is deprecated in favour of ifInMulticastPkts and ifInBroadcastPkts.
ifInDiscards .1.3.6.1.2.1.2.2.1.13	The number of discarded packets.
lfInErrors .1.3.6.1.2.1.2.2.1.14	The number of received packets having errors.
ifInUnknownProtos .1.3.6.1.2.1.2.2.1.15	The number of received packets having unknown or unsupported protocols.
ifOutOctets .1.3.6.1.2.1.2.2.1.16	The number of transmitted bytes.
ifOutUcastPkts .1.3.6.1.2.1.2.2.1.17	The number of transmitted unicast packets.
ifOutNUcastPkts .1.3.6.1.2.1.2.2.1.18	This object is deprecated in favour of ifOutMulticastPkts and ifOutBroadcastPkts.
ifOutDiscards .1.3.6.1.2.1.2.2.1.19	The number of discarded outgoing packets.
ifOutErrors .1.3.6.1.2.1.2.2.1.20	The number of outgoing packets not transmitted because packet has error.
ifOutQLen .1.3.6.1.2.1.2.2.1.21	The length of outgoing packets.
ifSpecific .1.3.6.1.2.1.2.2.1.22	This object is deprecated.

ifXTable

This table is enhance version of ifTable.

MIB Object and OID	Description
ifName .1.3.6.1.2.1.31.1.1.1.1	The interface name.
ifInMulticastPkts .1.3.6.1.2.1.31.1.1.1.2	The number of received multicast packets.
ifInBroadcastPkts .1.3.6.1.2.1.31.1.1.1.3	The number of received broadcast packets.
ifOutMulticastPkts .1.3.6.1.2.1.31.1.1.1.4	The number of transmitted multicast packets.
fOutBroadcastPkts .1.3.6.1.2.1.31.1.1.1.5	The number of transmitted broadcast packets.
ifHCInOctets .1.3.6.1.2.1.31.1.1.1.6	The number of received bytes in 64 bits format.
ifHCInUcastPkts .1.3.6.1.2.1.31.1.1.1.7	The number of received unicast packets in 64 bits format.
ifHCInMulticastPkts .1.3.6.1.2.1.31.1.1.1.8	The number of received multicast packets in 64 bits format.
fHCInBroadcastPkts .1.3.6.1.2.1.31.1.1.1.9	The number of received broadcast packets in 64 bits format.
ifHCOutOctets .1.3.6.1.2.1.31.1.1.1.10	The number of transmitted bytes in 64 bits format.
ifHCOutUcastPkts .1.3.6.1.2.1.31.1.1.1.11	The number of transmitted unicast packets in 64 bits format.
ifHCOutMulticastPkts .1.3.6.1.2.1.31.1.1.1.12	The number of transmitted multicast packets in 64 bits format.
ifHCOutBroadcastPkts .1.3.6.1.2.1.31.1.1.1.13	The number of transmitted broadcast packets in 64 bits format.
ifLinkUpDownTrapEnable .1.3.6.1.2.1.31.1.1.1.14	Indicates if linkUp/linkDown traps must be generated for this interface.
ifHighSpeed .1.3.6.1.2.1.31.1.1.1.15	The interface speed in Mbps.
ifPromiscuousMode .1.3.6.1.2.1.31.1.1.1.16	Indicates if it accepts all the packets on the media. Value must be 2.

MIB Object and OID	Description
ifConnectorPresent .1.3.6.1.2.1.31.1.1.1.17	This object has the value 'true(1)' if the interface sublayer has a physical connector and the value false(2)' otherwise.

fcipEntityInstanceTable

This table contains information related to FCIP entities.

MIB Object and OID	Description
fcipEntityId 1.3.6.1.2.1.224.1.1.4.1.1	The entity identifier.
fcipEntityName 1.3.6.1.2.1.224.1.1.4.1.2	The entity name.
fcipEntityAddressType 1.3.6.1.2.1.224.1.1.4.1.3	The address type and it can be ipv4, ipv6, etc.,
fcipEntityAddress 1.3.6.1.2.1.224.1.1.4.1.4	The address of the entity.
fcipEntityTcpConnPort 1.3.6.1.2.1.224.1.1.4.1.5	The connection port number.
fcipEntitySeqNumWrap 1.3.6.1.2.1.224.1.1.4.1.6	The sequence number.
fcipEntityPHBSupport 1.3.6.1.2.1.224.1.1.4.1.7	Not supported.
fcipEntityStatus 1.3.6.1.2.1.224.1.1.4.1.8	The entity status and it is always active.

fcipLinkTable

This table contains information about link of FCIP entities.

MIB Object and OID	Description
fcipLinkIndex 1.3.6.1.2.1.224.1.1.5.1.1	The ifIndex of ifTable.
fcipLinkIfIndex 1.3.6.1.2.1.224.1.1.5.1.2	The ifIndex value of the virtual interface corresponding to the FCIP Link running over TCP/IP.
fcipLinkCost 1.3.6.1.2.1.224.1.1.5.1.3	The link cost.
fcipLinkLocalFcipEntityMode 1.3.6.1.2.1.224.1.1.5.1.4	The entity mode and it is always eport.

MIB Object and OID	Description
fcipLinkLocalFcipEntityAddressType 1.3.6.1.2.1.224.1.1.5.1.5	The address type.
fcipLinkLocalFcipEntityAddress 1.3.6.1.2.1.224.1.1.5.1.6	The entity address.
fcipLinkRemFcipEntityId 1.3.6.1.2.1.224.1.1.5.1.7	The remote entity identifier.
fcipLinkRemFcipEntityAddressType 1.3.6.1.2.1.224.1.1.5.1.8	The remote entity address type.
fcipLinkRemFcipEntityAddress 1.3.6.1.2.1.224.1.1.5.1.9	The remote entity address.
fcipLinkStatus 1.3.6.1.2.1.224.1.1.5.1.10	The link status and it is always active.
fcipLinkCreateTime 1.3.6.1.2.1.224.1.1.5.1.11	Not supported.

fcipTcpConnTable

This table contains TCP connection information about the link.

MIB Object and OID	Description
fcipTcpConnLocalPort 1.3.6.1.2.1.224.1.1.6.1.1	The TCP connection local port.
fcipTcpConnRemPort 1.3.6.1.2.1.224.1.1.6.1.2	The TCP connection remote port.
fcipTcpConnRWSize 1.3.6.1.2.1.224.1.1.6.1.3	The windows size.
fcipTcpConnMSS 1.3.6.1.2.1.224.1.1.6.1.4	The segment size.

Modified MIBs

The following changes have been made to the **SW.mib:**

- The "swBrcdBitObjVal" MIB object is newly added.

MIB Object and OID	Description
swBrcdBitObjVal 1.3.6.1.4.1.1588.2.1.1.1.1.37	The MIB object will have object value for each change mentioned in swBrcdGenericTrap. It will be empty for the events which do not have any values.

- The "swFCPortPrevType" MIB object is updated to include D_Port option.

Updated Traps

The following BD traps are updated to include a new variable “slotPort” to display port number in slot/port format:

- bdTrap
- bdClearTrap

Deprecated/Obsoleted MIBs

The following MIB objects/traps in **SW.mib** are deprecated:

- swTrackChangesInfo
- swTelnetShellAdmStatus
- swTrackChangesTrap

Blade Support

Fabric OS v7.3 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 max of 4 blades of this type.
FCoE/L2 CEE blade FCOE10-24	Up to a max 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 v7.3

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

Fabric OS v7.3 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.
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, FC8-48E[1]	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 max 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 v7.3

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 restrictions:
    - E-port connections between two FC16-64 blades are not supported.
    - Connecting a QSFP port between a FC16-64 blade and an ICL QSFP port on a core blade is not supported.
    - E-port connections between a FC16-64 and other port blades (via break-out) are 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	
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) 220VAC Power Supplies are required for redundancy. • For DCX with one or two FS8-18 Blades, (2) 220VAC Power Supplies are required for redundancy. • For DCX-4S, (2) 220VAC Power Supplies provide redundant configuration with any supported number of FS8-18 Blades. • For both DCX and DCX-4S with FX8-24 blades, (1+1) 220VAC Power Supplies are required for redundancy.

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

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

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	200-240VAC: 1+1 Power Supplies 110VAC: 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	200-240VAC: 1+1 Power Supplies 110VAC: 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	200-240VAC: 1+1 Power Supplies 110VAC: 2+2[1] Power Supplies Max 8 FC8-32E port blades
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	200-240VAC: 1+1 Power Supplies 110VAC: 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	200-240VAC: 1+1 Power Supplies 110VAC: 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	200-240VAC: 1+1 Power Supplies 110VAC: 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	200-240VAC: 1+1 Power Supplies 110VAC: 2+2[1] Power Supplies Max 7 FC8-48E 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**
384 16Gb ports + QSFP ICLs	FC16-48	Port Blade	Not Supported	4 Power Supplies	200-240VAC: For DCX 8510-8, four (2+2)[1] 220V AC Power Supplies are required
384 16Gb ports + QSFP ICLs	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200-240VAC: 1+1 Power Supplies 110VAC: 2+2[1] Power Supplies
384 8Gb ports + QSFP ICLs	FC8-48E	Port Blade	4 Power Supplies	4 Power Supplies	200-240VAC: For DCX 8510-8, four (2+2)[1] 220V AC 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] 220V AC Power Supplies are required when any special purpose blade are installed
512 16Gb ports	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200-240VAC: 1+1 Power Supplies 110VAC: 2+2[1] Power Supplies
512 16Gb ports + QSFP ICLs	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200-240VAC: 1+1 Power Supplies 110VAC: 2+2[1] Power Supplies

Table 4 Power Supply Requirements for DCX 8510-8

Notes:

1. When 2+2 power supply combination is used, the users are advised to configure the Fabric Watch setting for switch marginal state to be two power supplies. Users can use the CLI switchstatuspolicyset to configure this value if the current value is set to zero. In FOS v7.0.x, the default setting for the marginal state due to missing power supplies is incorrectly set to zero, which will prevent Fabric Watch from generating notifications when the switch enters the marginal state due to missing power supplies

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 Specifications in the 8510-4 Backbone Hardware Reference Manual)

Configured Number 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	200-240VAC: 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 net installed), 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:
  - Log in to http://my.brocade.com
  - Go to Documentation > Tech Notes.
  - Look for the Tech Note on Access Gateway Device-Based Mapping in VMware ESX Server.

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. 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 v7.2.x to FOS v7.3 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.
- FOS7.2 and later supports KMIP key vault type for Thales e-Security Key Authority SW v4.0.0 KMIP servers. Please refer to the KMIP Encryption Admin Guide for more details.
    - Replication feature from Thales e-Security Key Authority KMIP server is not supported with BES/FS8-18.

- In FOS 7.1.0 or later the encryption FPGA has been upgraded to include parity protection of lookup memory (ROM) within the AES engine. This change enhances parity error detection capability of the FPGA.
- 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).

FCIP (Brocade 7840)

- Brocade 7840 does not support FCIP connection to Brocade 7800 or FX8-24.
- FOS v7.3- does not support concurrent non-disruptive firmware download.
- FOS v7.3- does not support 10G speed on the 24 16G FC ports on Brocade 7840.
- FOS v7.3- does not support VEX port on Brocade 7840.
- FOS v7.3- does not support base switch on Brocade 7840.
- FOS v7.3- does not support credit recovery on BI ports 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

- FCIP non-disruptive firmware download can fail in configurations with large FCIP object counts. This can occur in FICON or FCP emulation enabled configurations. FCIP non-disruptive

firmware download may fail if there are greater than 20,000 FCP or FICON device objects. This problem can be avoided by performing a disruptive firmware download. (This issue is also noted as defect 528010.)

- 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.

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.

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.

Native Connectivity (M-EOS interoperability)

- A switch running FOS v7.0 or later cannot form E-port connectivity with any M-EOS platform.
- Platform running FOS v7.1 or later does not support EX port configuration in Interopmode 2 or Interopmode 3.
- Device sharing between a switch running FOS v7.1 or later and McDATA fabrics is allowed via Integrated Routing platforms using FOS v7.0.x (or earlier) firmware.

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 specifics 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.
- 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.
- FOS v7.3.1b is qualified and supported with Oracle Java version 7 update 80 and Java version 8 update 45. When launching WebTools using a browser with FOS 7.3.1b, ensure that Oracle JRE update 1.7u80 (or) JRE update 1.8u45 is installed on that computer. WebTools can be launched from the local client of Brocade Network Advisor installed on Windows OS. Launching WebTools from local client of Brocade Network Advisor installed on Linux OS will fail due to the expiration check with JRE 1.7 update 51. As a workaround for this issue on Linux, please do the following changes in the Brocade Network Advisor installed computer.

  1. Add following lines in <User Home>/.java/deployment/deployment.properties file
     deployment.expiration.check.enabled=false

     For example, if the user is root then the absolute path of this file is as below

     /root/.java/deployment/deployment.properties

  2. Launch the java control panel using below command and click on Ok button
     <Network Advisor Home>\jre\bin\jcontrol

  Please refer to Brocade Network Advisor release notes for more details.

  In addition, users must check the "Enable Java content in the browser" box under the Security tab of Java Control Console to allow launching WebTools from BNA server clients.
- Due to Java signing certificate expiration, launching WebTools from Network Advisor 12.3.2 remote client will not work with JRE 8 starting from 2/13/2015. An attempt to launch the WebTools will be blocked and "Failed to validate certificate. The application will not be executed" message will be shown. Network Advisor 12.3.4 resolves this issue. To work around this issue in Network Advisor 12.3.2, please uninstall JRE 8, install JRE 1.7U80 and set the security level to Medium.

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

- FOS v7.3 only supports the Read Diagnostics Parameters (RDP) feature between Brocade switches both running FOS v7.3. RDP is not supported with any other vendor devices nor supported with switches running other FOS versions.

Link Cable Beaconing

- The Link Cable Beaconing (LCB) feature on FOS v7.3 is only supported on ISLs between two Brocade switches both running FOS v7.3.0 – FOS v7.3.1a. Support with third party vendor devices is only available with FOS v7.3.1b or above with fix for defect 540720.

16G 2km ICL QSFP

- For existing DCX8510 switches with 16G 2km ICL QSFP installed to fix defect 539584, in addition to upgrade to FOS v7.3.1b, it is required to port decommission or disable the affected ICLs, pull out and insert the 2km QSFP, followed by persistently disable then persistenly enable the ICL ports.
- 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.
- 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.

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 rules of default active policy will restore access to the switch.
- Firmware downgrade from FOS v7.3.0 with one or more ports enabled with the Flow Generator feature as a SIM port will be blocked. The SIM ports configuration must first be disabled.
- Firmware upgrade to FOS v7.3.0 with one or more ports enabled with the Flow Generator feature as a SIM port will be blocked. The SIM ports configuration must first be disabled.
- FOS v7.3.0 includes a fix for defect 492340 where users may see frame drops on the back-end edge and core ports with FS8-18 and FX8-24 blades in DCX 8510 chassis. This fix will only take effect after the affected blades are powered off and on. After the fix takes effect, a new credit allocation model leads to fewer credits available for long distance ports. If there are long distance port configurations that have used up all the credits prior to applying this fix, some long distance ports may experience degraded performance.
- Firmware downgrade from FOS v7.3.0 will be blocked when any logical switch is configured with in-flight encryption with FCAP protocol or SHA-256 hashing algorithm is used with FCAP or DH-CHAP protocol. These configurations must be removed from all logical switches for downgrade.
- 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.

Defects

Closed with Code Change in Fabric OS v7.3.1.b

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of July 25, 2015 in Fabric OS v7.3.1b

Defect ID: DEFECT000494952	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0_fuj	**Technology Area:** Web Tools
Symptom: In Webtools fabric watch explorer, F/FL copper Port class is missing.	
Condition: On embedded switch where internal ports 1 - 16 are copper ports.	

Defect ID: DEFECT000520333	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.2.0	**Technology Area:** FICON CUP
Symptom: CUP remained quiescent after firmware upgrade.	
Condition: It happens in a timing condition when the firmware download completion notification is missed by CUP.	

Defect ID: DEFECT000521204	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS6.4.3	**Technology Area:** Component
Symptom: During hafailover, customer encountered a switch panic.	
Condition: This was encountered during a rare PCI write failure to an ASIC chip. An invalid DMA descriptor was accessed without validation check.	
Recovery: Replace the faulty port blade.	

Defect ID: DEFECT000525413	
Technical Severity: Low	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: The 'portcfgge <port> --show' command and 'portshow autoneg <port>' command do not show the valid output for 7800/FX8-24. It will report 'No GE configuration entries found' instead of reporting the actual data.	
Condition: This will occur every time the 'portcfgge <port> --show' and 'portshow autoneg <port>' commands are issued.	

Defect ID: DEFECT000531192	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.2.0	**Technology Area:** FICON CUP
Symptom: During firmware upgrade, hosts lost paths due to FICON filter that was not properly cleaned up.	
Condition: On a FMS CUP enabled switch, if trunk master goes offline first, after hafailover FICON CUP filter is not properly removed.	
Recovery: Bounce trunk ports	

Defect ID: DEFECT000532726	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.4.0	**Technology Area:** Web Tools
Symptom: WebTools will not launch with Java 8 update 40.	
Condition: When Admin Domain is enabled in the switch.	
Workaround: If supported, enable virtual fabric.	

Defect ID: DEFECT000534141	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.3.0_HUR	**Technology Area:** Port Bring-up
Symptom: BR6543 switch takes very long time for the internal link to come online.	
Condition: This problem can be observed by disabling/enabling the port using portdisable/portenable CLI.	

Defect ID: DEFECT000537108	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS6.4.3	**Technology Area:** Credit Loss
Symptom: Standby CP reboots due to software assert during a hafailover.	
Condition: If back-end credit recovery is enabled with Link Reset only option via CLI, creditrecovmode and credit recovery algorithms kick in. During that window if either core or edge blade goes offline, this can sometimes cause the standby CP to panic during a subsequent hafailover.	

Defect ID: DEFECT000537311	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** FCIP
Symptom: Switchshow shows no ports found in the system.	
Condition: Run switchshow command.	

Defect ID: DEFECT000538046	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS7.1.1	**Technology Area:** Component
Symptom: Fabric Watch terminates in a busy system causing switch reboot.	
Condition: This is a very rare occurrence that may be encountered on systems that are very busy.	

Defect ID: DEFECT000538917	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.4.0	**Technology Area:** Management Server
Symptom: The Fibre Channel specification (FC-FS-3) pertaining to Read Diagnostic Parameters (RDP) has been updated with new descriptor codes and descriptor flags. This renders current implementation incompatible. Device will not get properly formatted RDP response.	
Condition: This happens in a fabric with device capable of RDP and running FOS v7.3.0 or above.	
Workaround: Disable device port capable of RDP	

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: DEFECT000540720	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** Equipment Status
Symptom: Even though the portpeerbeacon CLI does succeed and correctly lights up the LED on both end ports, a trace shows the 'Beacon on" sub-command is in the wrong format.	
Condition: When user executes portpeerbeacon CLI.	

Defect ID: DEFECT000540971	
Technical Severity: Low	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: In extreme conditions MAPS generates false alert for port errors such as LR etc.	
Condition: This false alert could be generated during state change of port and this happen in extreme conditions.	

Defect ID: DEFECT000542388	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.1.1	**Technology Area:** Access Gateway
Symptom: Even though there are no mappings being shown in ag -mapshow for some ports, available F-ports cannot be mapped to existing N-ports. All F-ports are reported to be mapped to a non-existent N-port, and do not show up in ag -mapshow.	
Condition: Inconsistent config file is downloaded to the switch with configdownload. The inconsistency entails one of the following: - F-to-N-port mapping for F-Ports, or - No port config, but F-to-N-port mapping exists.	
Recovery: Configure all non-used ports (ports that are not N-port and not F-port) as N-port and then remove that configuration. In rare cases, even the F-ports may need to be temporarily configured as N-ports and then remove the configuration.	

Defect ID: DEFECT000542770	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.4.0	**Technology Area:** Port Bring-up
Symptom: Port 60 on BR6520 cannot come online.	
Condition: This seems to happen with FOSv7.3.1 and later code.	
Workaround: Use a different port.	

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: DEFECT000543734	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.1	**Technology Area:** Name Server
Symptom: DCX CP reboots after a port blade going to faulty state.	
Condition: This happened when NPIV devices falsely detected duplicate PWWN as a result of path failover upon detect faulty blade. It could also happen if a device connected to a port blade which goes faulty and moving the device to other port blades in chassis without powering down the faulty blade.	

Defect ID: DEFECT000544160	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.2.1	**Technology Area:** Encryption
Symptom: After FS8-18 or BES was powered up, several LUNs were inaccessible. The LUN state was "LUN setup".	
Condition: After firmware download or power event, BES re-establish nexus for each Container-Host pair. It's not properly clean up and retry timed-out internal request.	
Recovery: Bounce affected port.	

Defect ID: DEFECT000545217	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Web Tools
Symptom: End to End (EE) monitor is not supported in base switch, yet, when configuring it, improper message pops up such as: 1). "The SID is not associated with any devices. Do you still want to use this SID?" 2). "The DID is not associated with any devices. Do you still want to use this DID?" Rather than just error out with : "EE monitor not supported on base switch".	
Condition: It occurs when configuring EE monitor(SID/DID performance graph through WEBTools in base switch.	
Workaround: Use CLI.	

Defect ID: DEFECT000546941	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.2.0	**Technology Area:** FCIP Fastwrite
Symptom: XTUN-1001 and XTUN-1008 RASLOG messages generated and failed FCIP Fast Write or Tape Pipelined I/O operations.	
Condition: When there are multiple logical switches each with an emulation feature enabled FCIP Tunnel (Fast Write and/or OSTP). If one of the Fast Write or OSTP configurations include a large number of discovered FCIP objects (ITNs and ITLs), the FCIP emulation memory manager may incorrectly allocate and cache too many I/O structures leading to out of memory conditions in any one of the different FCIP Tunnel logical switch configurations.	

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: DEFECT000548713	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.2.0	**Technology Area:** FCIP
Symptom: Disk to disk mirroring application failures with associated XTUN-1001 RASLOG messages.	
Condition: When a specific Disk to Disk mirroring application encounters IO errors over a 7800 or FX8-24 FCIP Tunnel, it will issue an odd sequence of Extended Link Services commands (concurrent LOGO/LOGO and PLOGI sequences). The problem can be encountered if the FCIP Tunnel has OSTP and/or Fast Write enabled and there are still active FCP commands flowing when the ELS sequences are processed.	
Recovery: Reboot 7800 platform or slotpoweroff/slotpoweron the FX8-24 blade.	

Defect ID: DEFECT000548721	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS6.4.3	**Technology Area:** Fabric Watch
Symptom: E-port is fenced even after port fencing has been disabled.	
Condition: This issue would only happen if E-port and port classes are configured with the same thresholds for ST area. Disabling port fencing does not handle properly E-ports that have been fenced earlier under this condition.	
Workaround: Use the E-Port only threshold to monitor the State change of ISLs, or to monitor all the ports in general, choose different threshold values for E-port thresholds and port class thresholds (probably E-Port threshold + 5).	
Recovery: Bounce the port.	

Defect ID: DEFECT000550167	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.1	**Technology Area:** Fabric Watch
Symptom: portthconfig --show CLI doesnt show ST area configuration (either default or custom) for port class.	
Condition: All platforms exbhit this behavior with FOS 7.3.1 version and above	

Defect ID: DEFECT000550514	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** System
Reported In Release: FOS7.2.1	**Technology Area:** CLI
Symptom: Creditrecovmode --check fails between core blade and FX8-24 blade creditrecovmode --check 5/108,30 Error: Not Supported on this link.	
Condition: Error: Not Supported on this link is seen if an AP blade has ever had a VE port enabled without a reboot, manual credit recovery CLI "creditrecovmode" occurring. This is seen even if the VE port is currently disabled.	
Recovery: After rebooting the switch, the "creditrecovmode --check" will work on non-VE port AP blade.	

Defect ID: DEFECT000550684	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.4.0	**Technology Area:** Platform Services
Symptom: When an embedded switch configured in Access Gateway mode is connected to a 3rd party fibre channel switch, the Brocade embedded switch has a software assert error and reboots. [KSWD-1002], 18/14, FFDC | CHASSIS, WARNING, 5, Detected termination of process fdmid0:1226., hasm_swd.c.	
Condition: Error occurs during FDMI request response process with following embedded platforms: BR6547, 6548, M5424, M6505 running FOSv7.3.0 and higher. The error does not occur with v7.2.x.	

Defect ID: DEFECT000551520	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.2.0	**Technology Area:** WAN Performance Analysis Tools
Symptom: Brocade NMS monitoring services are unable to do snmpwalk of fcipExtendedLinkTable to collect statistical data.	
Condition: When a 7800 or FX8-24 blade is configure with Virtual Fabrics and have the GE ports in the default switch and the VE port in a separate VF the fcipExtendedLinkTable fails. If the GE ports and VE port are in the same VF the snmpwalk will work without problems.	

Defect ID: DEFECT000551531	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.4.0	**Technology Area:** Security Vulnerability
Symptom: OpenSSL Security Advisory [19 Mar 2015]: CVE-2015-0286, CVE-2015-0288, CVE-2015-0289, CVE-2015-0292. These vulnerabilities allow various maliciously crafted data could trigger segment fault, memory corruption or DOS attack.	
Condition: To exploit these vulnerabilities in FOS requires access to switch after user authentication through console, Telnet, and SSH connections.	
Workaround: Place switch and other data center critical infrastructure behind firewall to disallow access from the Internet; Change all default account passwords; Delete guest accounts and temporary accounts created for one-time usage needs; Utilize FOS password policy management to strengthen the complexity, age, and history requirements of switch account passwords. Upgrading to a FOS version including this fix prevents exposures to the four CVEs noted in the defect Symptom.	
Recovery:	

Defect ID: DEFECT000551787	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.4.0	**Technology Area:** Routing
Symptom: FCR devices not imported for up to 10 minutes following hafailover, resulting in IO disruption.	
Condition: This may be encountered in an FCR setup, when ports(E/ExVex/Fport) are bounced in edge fabric during hafailover. This only impacts FOS7.3.x and FOS7.4.0 with staged port matching feature.	
Workaround: If there is VEx port in a FCR fabric, upgrade to a FOS version with this fix. If already running a version of FOS without this fix, contact tech support to disable staged port matching feature on backbone fabric to reduce future risk until able to upgrade to a version with fix.	
Recovery: Wait approximately 10 minutes for FCR to re-import the devices after an HaFailover or toggle end device to recover	

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.	

Defect ID: DEFECT000553197	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.1	**Technology Area:** OSTP - Open Systems Tape Pipelining
Symptom: I/O errors to BR7840 FCIP Open Systems Tape Pipelining connected FCP SID/DID pairs and XTUN-1000 Missed data frame RASLOG.	
Condition: This may occur when OSTP is currently in read pipelining when a FCP Inquiry command is received using the same OXID that is currently active for an OSTP read-ahead read command sequence.	
Workaround: Disable OSTP Read Pipelining on the BR7840 FCIP Tunnel.	

Defect ID: DEFECT000553920	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.2.1	**Technology Area:** Virtual Fabrics
Symptom: Ports in logical switch may bounce following firmwaredownload or hareboot.	
Condition: In a VF environment with XISL on and base switch not defined, FMS is enabled on one logical switch, other logical switches without FMS mode enabled, will have FICON filters installed on ports by mistake and cause traffic disruption.	

Defect ID: DEFECT000554238	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.4.0	**Technology Area:** Firmware upload/download
Symptom: After swap QSFP with 2km SFP on core blade ICL ports, cannot code downgrade to FOS v7.3.x.	
Condition: Customer swapped QSFP with 2km SFP, and wants to perform code downgrade.	
Recovery: Remove all 2km optics, finding an old standard QSFP optic and inserting it into the empty port previously occupied by the 2km optic, then perform firmware downgrade.	

Defect ID: DEFECT000554414	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** System
Reported In Release: FOS7.3.0	**Technology Area:** Component
Symptom: Link issues are seen when fcippathtest runs for a longer duration on BR7800.	
Condition: Running systemverification test in a loop of about 10+ iterations results in this issue.	

Defect ID: DEFECT000554530	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.1	**Technology Area:** Zoning
Symptom: Zone enforcement changes on an NPIV port may not be properly enforced in time to prevent frame loss or observe a timeout. The frame loss or timeout can be seen on any of the NPIV devices on the same switch port where the zoning config change was made.	
Condition: Performing a zoning change to any member of the NPIV port can cause any device on that port to be impacted. This can be seen in FOS v7.2.1d, v7.2.1e, v7.3.1, v7.3.1a, v7.4.0, v7.4.0a	

Defect ID: DEFECT000554744	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.1	**Technology Area:** Web Tools
Symptom: The alias member revert back to an old offline WWPN as one switched from the "Alias" tab to the "Config" tab in Webtools.	
Condition: Name server dialog is opened with “Auto refresh” on, such that name server info, zoning info and switch details will be polled from switch and refreshed in webtools. As the zone information is refreshed, user changed zone alias will be overwritten.	
Workaround: Disable the auto refresh before doing any zoning changes in webtools	

Defect ID: DEFECT000555286	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.1.1	**Technology Area:** OSTP - Open Systems Tape Pipelining
Symptom: FCIP OSTP (Open Systems Tape Pipelining) Read I/O Job failures (block count mismatch or other errors).	
Condition: After tape server or tape server HBA code upgrade, SSC-2/3 (T10 standard) commands can be issued to an FCIP OSTP enabled tunnel to a tape device. FCIP currently does not have the SSC-2 command set implemented and therefore unknown errors can occur.	
Workaround: Disable OSTP Read Pipelining on the FCIP Tunnel between the server and the tape device.	

Defect ID: DEFECT000556108	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.1	**Technology Area:** Web Tools
Symptom: Zone Administration display is painted complete white and fails to display the buttons.	
Condition: When trying to fetch the vendor name using the OUI which doesn't exist in WebTools repository.	

Defect ID: DEFECT000556188	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.4.0	**Technology Area:** Buffer Credit Recovery
Symptom: On 16G director, while credit recovery feature is not turned on, if there is unstable back-end link, blade could be faulted.	
Condition: A blade could be faulted on 16G director when following conditions are meet: 1. Credit recovery feature is off 2. There is credit loss caused by link level error on back-end ports. 3. The link cannot be recovery by an automatic Link Reset. This can happen with FOS7.2.1e and 7.3.1a and FOS7.4.0; With earlier releases, the credit loss will result no further action until user manually link reset if credit recovery feature is off.	
Workaround: Turn on credit recovery "creditrecovmode --cfg onLrOnly" to limit the fault to a back-end port only under error condition.	
Recovery: Turn on credit recovery "creditrecovmode --cfg onLrOnly" to limit the fault to a back-end port only under error condition.	

Defect ID: DEFECT000557254	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.4.0	**Technology Area:** FICON CUP
Symptom: CUP goes offline when CSCTL priority is enabled on CUP port.	
Condition: Plogi response frame has priority bit set and CSCTL priority to the CUP is not supported.	

Defect ID: DEFECT000558511	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** System
Reported In Release: FOS7.4.0	**Technology Area:** Component
Symptom: Loss of CUP connectivity in a cascaded FICON environment, following the disruption of all ISL paths to a given CUP.	
Condition: Following disruption of all ISL paths to a given cascaded CUP, subsequent exchanges destined to the cascaded CUP cannot be delivered until a new PLOGI session is established.	
Recovery: Vary channel online to recover.	

Defect ID: DEFECT000558820	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** System
Reported In Release: FOS7.3.1	**Technology Area:** CLI
Symptom: Response time out happens with higher nframes value specified for fcippathtest.	
Condition: Issue happens when nfrmaes value as high as 70 is specified for fcippathtest.	

Defect ID: DEFECT000558936	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** System
Reported In Release: FOS7.3.1	**Technology Area:** CLI
Symptom: HIF mode value is not always being displayed in switchshow output .	
Condition: This is encountered when HIF mode is disabled. HIF mode value is displayed only when HIF mode is enabled.	

Defect ID: DEFECT000559709	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.1	**Technology Area:** Web Tools
Symptom: Switch Health Report does not reflect accurate state of the ports: WebTools shows the Error Ports Monitor as DOWN - but displays "All ports are healthy"	
Condition: Error Ports Monitor does not correctly reflect the status through Web tools when there are ports with errors.	
Workaround: CLI command works properly and can be used as a workaround.	

Defect ID: DEFECT000559947	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.1	**Technology Area:** End-to-end Performance Monitoring
Symptom: Switch goes into rolling reboot following the execution of these sequence of commands: fmmonitor, configdefault, configupload/download.	
Condition: This may be encountered if configuration download and upload is performed when there are user defined frame monitors.	
Workaround: Avoid downloading configuration file with user defined frame monitors.	

Closed with Code Change in Fabric OS v7.3.1a

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of March 13, 2015 in Fabric OS v7.3.1a

Defect ID: DEFECT000431369	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.2	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: Mib browser displays ascii-hex of populated fcportflag value. For example it displays "30" for 0, "31" for 1, where expected display is "0", "1".	
Condition: This is seen only for the MIB display of fcportflag.	

Defect ID: DEFECT000472607	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS7.2.0	**Technology Area:** CLI
Symptom: Brocade 6510 switch may become inaccessible via SSH and/or Telnet when a firmware upgrade of the switch initiated through Brocade Network Advisor results with “failed to enforce new iptable rules” error message,.	
Condition: It's a race condition caused by an existing ineffective file locking mechanism.	
Workaround: Activating (from console) a new policy with rules of default active policy will restore access to the switch. such as: Ipfilter –clone new_rules –from default_ipv4 Ipfilter –activate new_rules	

Defect ID: DEFECT000513544	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.1	**Technology Area:** Management Server
Symptom: During code upgrade, standby CP may run into repeated msd panics and may not come online to standby ready mode.	
Condition: This occurs when AG node name is missing on active CP during execution of the FC-GS-3 Register Platform (RPL) command.	

Defect ID: DEFECT000523845	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS6.3.2	**Technology Area:** Access Gateway
Symptom: appearance of the configuration parameter "ag.fporttrunking" differs depending on reboot/hareboot	
Condition: After non-disruptive firmware upgrade from FOS v6.2 to FOS v6.3, configuration key ag.fporttruking(introduced in FOS v6.3) created at boot stage is getting removed. And the issue persists when user performs non-disruptive firmware upgrade to higher firmware versions without reboot..	
Recovery: No other functional impact	

Defect ID: DEFECT000527025	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** APM - Advanced Performance Monitoring
Symptom: CLI command fmmonitor --delmonitor <fmtype> -port 2/2 returns with "Specified Frame type doesn't exist on the specified port" even though a new fm-type was created and added to port 2/2.	
Condition: This may be seen when user moves the frame monitor installed port from one logical switch to another and then moves back the same port to the original logical switch	

Defect ID: DEFECT000527506	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** System
Reported In Release: FOS7.1.0	**Technology Area:** Component
Symptom: I2C access failures leading to various symptoms such as: 1. slotshow command output may flag some components with an "*", indicating no i2c access to that component. 2. switchshow command output may indicate “Speed Mismatch / Incompatible SFP” 3. tempshow command output may display "unknown" 4. Console log (dmesg) may include: pcf954x_select_mux: Failed to select the I2C mux (addr=76, val=08, err=-1 id=0)!	
Condition: Brocade 6520 with the current version of software fails to properly reset or clear transient i2c faults. Consequently, Temporary or Transient errors on the I2C bus can result in what appears to be a permanent HW failure on a Brocade 6520.	
Recovery: Cold boot switch	

Defect ID: DEFECT000527862	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Web Tools
Symptom: Name server table column position is not persistent across relaunch	
Condition: This name server table column display issue is seen when the switch is in non AG mode.	

Defect ID: DEFECT000528010	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: FCIP HCL failure encountered due to a large number of FCIP objects in the configuration	
Condition: This is encountered when a large number of FCIP Objects (>> 20K FICON or FCP objects) are present.	
Workaround: Schedule a maintenance window for a disruptive FOS code load.	
Recovery: Recover environment after disruptive code load completes.	

Defect ID: DEFECT000528657	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.0	**Technology Area:** Name Server / Zoning
Symptom: FCPD termination encountered when device sends malformed response with incorrect R_CTL information during FCP probing	
Condition: This occurs only when the device reponds with malformed frames during FCP probing	

Defect ID: DEFECT000532816	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.0	**Technology Area:** Trunking
Symptom: Traffic disruption in normal traffic encountered following an HA-failover during firmware upgrade.	
Condition: This may happen when an E-port trunk port with FEC active bounces during HA-failover phase of the firmware upgrade process.	

Defect ID: DEFECT000533925	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.1.0	**Technology Area:** FICON emulation
Symptom: FCIP FICON Emulated Tape device failures with FICN-1062 in RASLOG and LastStates=0x0000423F443F	
Condition: When attempting to complete read processing and the device presents Device Busy then Device End, FICON emulation logic incorrectly generated a No-Op command with chaining instead of accepting the Device End Status.	
Workaround: Disable FICON Read Pipelining	

Defect ID: DEFECT000534413	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: "logicalgroup --show" command will show more ports than switch has under "ALL_PORTS" group. MAP-1003 RASLOG messages on non-existent ports.	
Condition: This issue happens if the customer has MAPS enabled and performs hafailover or migrate firmware to MAPS supported versions with online F_Port trunk.	
Workaround: Bring up the F_port trunk ports after hafailover,	

Defect ID: DEFECT000534507	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** FCIP
Symptom: Severe FICON workload disruption during 7840 HCL	
Condition: This is encountered when FCIP HCL is attempted on a single 7840 switch in a 7840 pair with HA and active FICON data flow,	
Workaround: Plan a disruptive firmware download.	

Defect ID: DEFECT000536455	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Platform Services
Symptom: Both Active and Standy CPs panic in a director while processing Read Diagnostic Parameters (RDP) Extended Link Service (ELS) request from local device.	
Condition: This is triggered by a race condition when a local device repeatedly sends unsolicited RDP ELS request and the switch is running FOS7.3.0 or above.	
Workaround: Disable device port capable of RDP	

Defect ID: DEFECT000536632	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.4.0	**Technology Area:** POST - Power-on Self-Test
Symptom: Diagnostic test "systemverification" failed with "NON_DIAG errors detected during run"	
Condition: This is encountered when running systemverification test on BR7840	

Defect ID: DEFECT000536832	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.4.0	**Technology Area:** In-flight Compression
Symptom: Port does not come online and raslog is flooded with the following message: "Brocade6520, S0,P51(114): Port is offline due to Encryption Compression Block error."	
Condition: This is seen when Inflight Encryption is enabled on an Ex-Port.	

Defect ID: DEFECT000537093	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.1.1	**Technology Area:** OSTP - Open Systems Tape Pipelining
Symptom: Timeouts after Reservation Conflict Status with tape devices when Fastwrite and Tape-pipelining are enabled	
Condition: This occurs when multiple servers attempt to reserve the same tape device over OSTP enabled tunnel.	
Workaround: Disable OSTP on the FCIP Tunnel	

Defect ID: DEFECT000537848	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.4.0	**Technology Area:** FC-FC routing
Symptom: Host unable to discover target devices in an Edge-to-Edge FCR topology.	
Condition: When some of the edge fabric switches having trunked IFLs are rebooted, resulting in Fabric ID conflicts in any of the backbone fabric FCRs, few hosts may not be able to discover targets.	

Defect ID: DEFECT000538051	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.3.0	**Technology Area:** FICON emulation
Symptom: BR7840 FICON Emulation OXID usage overlap causes Interface Control Check error messages on the mainframe console.	
Condition: The issue can occur anytime when two or more devices are active in FICON emulation over an FCIP tunnel.	
Workaround: Disable FICON emulation features on the FCIP Tunnel.	

Defect ID: DEFECT000538092	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.2.1	**Technology Area:** Access Gateway
Symptom: Following a FOS firmware upgrade or hareboot, traffic to and from the Access Gateway stops after the N-Port trunk master is disabled.	
Condition: This issue will occur when the following conditions occur: - hareboot for any reason, including firmwaredownload. - N-port trunk with at least two trunk members. - Trunk master of the N-port trunk is disabled.	
Workaround: Never disable the N-port trunk master when other trunk members are online. Instead, always disable all trunk members. Trunk slaves can be disabled with no issue.	
Recovery: To recover, do one of two things: 1. Bounce a host F_port on the Access Gateway. Or, 2. Disable all trunk members and then enable all trunk members.	

Defect ID: DEFECT000538492	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** OSTP - Open Systems Tape Pipelining
Symptom: Error recovery issue when the last write in a small write block is dropped.	
Condition: Data Integrity Error can be exposed when the Last Write Data Frame in a small write (8k) Across 7840 FCIP Tunnel when TP is on.	

Defect ID: DEFECT000539167	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.1	**Technology Area:** Web Tools
Symptom: Weblinker termination when the TACACS+ server is unreachable	
Condition: Happens only when user tries to login to switch which has unreachable TACACS+ server for authentication.	
Workaround: Use local or other remote authentication(LDAP/RADIUS) for login	

Defect ID: DEFECT000539290	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.1	**Technology Area:** Buffer Credit Recovery
Symptom: On internal back end (BE) link with 16G core blade to 8G edge blade, credit is not automatically recovered.	
Condition: In the case of 16G core blade to 8G edge blade direction, if there is credit loss on VC and the "creditrecovmod --cfg onLROnly" command is not enabled in an early release, then once the 16G credit leak interrupt is triggered, the credit leak interrupt enabled bits will not be enabled again.	
Workaround: Run creditrecovmod --cfg onLROnly before credit is depleted.	
Recovery: Slotpoweroff /on core blade to recover the BE link	

Defect ID: DEFECT000540035	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.1	**Technology Area:** Licensing
Symptom: There is a new business requirement to offer a 20 port version of the Brocade 5432 switch plus 4 "port on demand" licensed ports.	
Condition: POD was not supported before.	
Recovery: Upgrade to the new FOS version to limit the switch to 20 licensed ports. To enable the additional 4 ports, the customer would need to purchase and install the POD license.	

Defect ID: DEFECT000540245	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.1.0	**Technology Area:** FCIP
Symptom: Tunnels bounce caused FFDC event.	
Condition: This may occur if a FICON frame sequence is received with FC type of 0x1B or 0x1C, with one SOFi3 frame followed by more than 13 SOFn3 frames in sequence on an FCIP Tunnel. This is probably caused by a failed FICON adapter in a connected device.	

Defect ID: DEFECT000540469	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.1.0	**Technology Area:** FICON emulation
Symptom: Channel Detected Error message after a tape job failure.	
Condition: When running a tape write job that experiences a timeout (due to FC CRC errors occurring during the IO), the job will normally detect an MIH failure and go through error recovery and the error recovery could encounter the invalid token CDE.	
Workaround: Disable FICON Tape Pipelining or correct the cause of the FC CRC errors.	

Defect ID: DEFECT000540585	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** supportShow
Symptom: Support Save output does not include VE or GE port information	
Condition: This is seen after multiple logical switches have been created and one or more of the logical switches have been deleted and the VE ports reside in a logical switch that was created after one that was deleted.	
Workaround: Recreate empty logical switches up to the limit of logical switches in that chassis.	

Defect ID: DEFECT000540694	
Technical Severity: Critical	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** Top Talker Monitors
Symptom: Switch repeatedly logs the following raslog message: "[PS-1009], 16386, SLOT 7 | FID 128, WARNING, , Failed to add the device updates in condb database." This can mislead the customer on the number of devices supported by name server, zoning and device connectivity.	
Condition: This happens when there are large number of devices zoned together and with "Performance Monitor license". There is no impact to device connectivity, but Top talkers may not be able to display the top talking flows	

Defect ID: DEFECT000541322	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.4.0	**Technology Area:** FICON emulation
Symptom: IOS050I CHANNEL DETECTED ERROR message on mainframe console after 0x70 Status from XRC primary controller.	
Condition: This is seen during FCIP FICON XRC emulated tunnel processing of 0x70 Status from the connected DASD controller.	
Workaround: Disable FICON XRC Emulation on the FCIP Tunnel.	

Defect ID: DEFECT000541661	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.2.1	**Technology Area:** Virtual Fabrics
Symptom: Active CP Panic may occur while running Brocade SAN Health report.	
Condition: This may be encountered in a large virtual fabric environment when running back to back CLI commands "lfcfg --showall -xxxx"	

Defect ID: DEFECT000542559	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.4.0	**Technology Area:** FCIP
Symptom: Tunnel bounce with an associated BLS-5024 FFDC event.	
Condition: This issue can occur after FCIP tunnel bounces due to WAN outage or other network issue.	

Defect ID: DEFECT000543727	
Technical Severity: Low	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Logging
Symptom: The CP flash drive can run low on space due to the /var/log/esmd_lib.log file growing too large.	
Condition: The problem may occur on any switch other than the Brocade 7840 switch, when running with FOS7.3.0x and FOS7.3.1. The problem will not occur on the Brocade 7840 switch.	
Recovery: Manually delete the /var/log/esmd_lib.log file.	

Defect ID: DEFECT000547042	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.1	**Technology Area:** Firmware upload/download
Symptom: When BufOpMode is enabled for core blades, Firmware upgrade/downgrade to FOS versions not supporting BufOpMode on core blades is not being blocked (as should be the case).	
Condition: This is encountered when BufOpMode is enabled and firmware upgrade/downgrade to FOS version not supporting this feature is being attempted.	
Workaround: Check to see if BufOpMode is enabled and clear/reset it before attempting a firmwaredownload of FOS versions that do not support this feature.	

Open in Fabric OS v7.3.1

This section lists the open defects with Critical, High and Medium Technical Severity as of December 12, 2014 in Fabric OS v7.3.1

Defect ID: DEFECT000497810	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.1	**Technology Area:** Diagnostic Port (D_Port)
Symptom: Core blade faults when dport tests are being run on ICL ports and ports are disabled.	
Condition: Disable port under testing	
Workaround: Don't disable ports when dport tests are in progress.	

Defect ID: DEFECT000529293	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.1	**Technology Area:** Ethernet Interface
Symptom: IFMODESET command does not change the mode of the interface.	
Condition: This is seen when the CLI command "ifmodeset" is run in non-interactive mode	
Workaround: Use interactive mode of this CLI command to set AN or Speed	

Defect ID: DEFECT000529395	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** System
Reported In Release: FOS7.3.1	**Technology Area:** CLI
Symptom: ipfilter --show command lists all ports as "permit".	
Condition: BR543x does not deny access to TCP/IP port 23 and 80 by default	
Workaround: Manual block ports	

Defect ID: DEFECT000529904	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.3.1	**Technology Area:** Port Bring-up
Symptom: Bounced ISL links may not come back to full speed setting when port speed is set to AN.	
Condition: This can only happen during hafailover with a fabric rebuild. This results from all ISL's going down at the same time.	
Recovery: Bounce ports to recover from this situation.	

Defect ID: DEFECT000531269	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.3.1	**Technology Area:** Access Gateway
Symptom: Static mapped F-ports do not come back online after reboot, while all the non-static mapped ports come back online after the reboot.	
Condition: This is encountered when F-ports are statically mapped.	
Workaround: Toggle the F-port manually.	
Recovery: Disable and then enable the N-ports that the F-ports are static mapped to.	

Open in Fabric OS v7.3.1

Defect ID: DEFECT000535664	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.1	**Technology Area:** FCIP
Symptom: BR7840 switch may go down as a result of DP crash from ECC errors in memory controller DIMMs.	
Condition: This may occur on BR7840 under rare situation, as a result of ECC errors.	

Closed with Code Change in Fabric OS v7.3.1

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of December 12, 2014 in Fabric OS v7.3.1

Defect ID: DEFECT000436921	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS6.3.1_dcb	**Technology Area:** CLI
Symptom: Console may hang, leading to switch Panic from unexpected termination of daemons from Out of Memory condition.	
Condition: This may be observed while performing supportsave or other CLI management operations	

Defect ID: DEFECT000457373	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.0.2	**Technology Area:** Access Gateway
Symptom: BR5480 embedded switch displays invalid message without functional impact.	
Condition: Invalid message "Request F-N Port Mappings for Access Gateway Change from SW" is observed while running in native switch mode.	
Recovery: No impact to switch functionality.	

Defect ID: DEFECT000470918	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.0	**Technology Area:** POST - Power-on Self-Test
Symptom: POST tests do not run when standard and extended levels of testing are chosen from CMM.	
Condition: Issue happens when post test is triggered from CMM on embedded switch.	

Defect ID: DEFECT000473541	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS6.4.3	**Technology Area:** CLI
Symptom: Large number of threads in environmental daemon (emd) cause system to run out of memory and panic.	
Condition: Over 100 portshow CLIs are concurrently running on a director.	
Workaround: Limit the number of concurrent CLIs to under 50 at a time.	

Defect ID: DEFECT000484261	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** Frame Monitoring
Symptom: CLI command "sloterrshow" reports timeout frame. However, “framelog –show” does not capture the timed out frame.	
Condition: This discrepancy with respect to timeout frames maybe noted when comparing outputs of CLI commands "sloterrshow" and “framelog –show”	

Closed with code in Fabric OS v7.3.1

Defect ID: DEFECT000484537	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** System
Reported In Release: FOS7.1.1	**Technology Area:** Component
Symptom: Switch CP experienced rolling kernel panic at "indirect_read_config" during blade initalization	
Condition: When a not properly seating blade or failed blade hang the PCI bus.	
Recovery: Remove the problem blade.	

Defect ID: DEFECT000488832	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.1.1	**Technology Area:** Virtual Fabrics
Symptom: During testing, embedded switch intermittently fails after reboot.	
Condition: After high reboot count, with less than 127 targets, switch will occasionally not respond to name server queries.	

Defect ID: DEFECT000489311	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS6.4.1	**Technology Area:** User Accounts
Symptom: Running "ifconfig eth0 down" on the console may lead to a panic and reboot of the switch.	
Condition: This may occur when the switch becomes unaccessible via the management port and the CLI command "ifconfig eth0 down" is executed from the serial console	

Defect ID: DEFECT000491910	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** Logging
Symptom: SNMP query connUnitPortStatCountBBCreditZero or CLI portstats64show could display an unexpected large value for tim64_txcrd_z counter in a very brief time	
Condition: This issue will be seen when there is a FC traffic slowness in fabric and statistic counter wraps.	
Workaround: Customer could use portstatsshow command to get the correct counter value.	

Defect ID: DEFECT000494270	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.1.0	**Technology Area:** Fabric Authentication
Symptom: Customer might see devices reported as unauthorized when they try to login to a switch even when DCC policy is configured properly. Sometimes when the DCC policy is activated, some of the ports might bounce.	
Condition: The WWN that starts with "80" has the most possibility to hit this issue. The issue might also be seen when the device WWNs starts with "C0", "50", "20", or "10".	
Workaround: Avoiding the device WWN that starts with "80" or greater from DCC policy would resolve the issue.	

Defect ID: DEFECT000499012	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Platform Services
Symptom: Unable to stop the autoboot using the ESC key to get into command shell.	
Condition: This is encountered during boot up, where the escape sequence key is not functioning properly.	

Closed with code in Fabric OS v7.3.1

Defect ID: DEFECT000499177	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.3.0	**Technology Area:** Other
Symptom: Some hosts from an edge fabric may fail to discover the LUNs in another edge fabric.	
Condition: After doing a switchdisable of all the switches in the edge fabric and doing simultaneous switchenable of the disabled switches.	
Recovery: Toggle the port, host and target. If condition persists, switchdisable/enable the switch.	

Defect ID: DEFECT000499356	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: CLI command "snmptraps --block/unblock -port [slot]port | ALL" appears to permit configuration for portsbeyond the valid range for a switch, without flagging any errors.	
Condition: This issue is seen when attempting to configure snmptraps for ports beyond the valid range for a given switch. No Error messages are shown to the user. However the problem itself is benign, with no functionality impact.	

Defect ID: DEFECT000501658	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.1	**Technology Area:** NTP - Network Time Protocol
Symptom: Switch panics after time server daemon failed to sync time with server.	
Condition: This may occur from an Ethernet network issue in the fabric resulting in a failure to resolve DNS names into IP addresses.	
Workaround: Use IP address instead of DNS server name in clock server configuration. Alternately do not configure DNSconfiguration in switch.	

Defect ID: DEFECT000503827	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** Extended Fabrics
Symptom: VE port comes up as G-port when concurrent firmwaredownload is initiated on two BR7840.	
Condition: Concurrent firmwaredownload is not supported on 7840, but if performed, this issue can be hit.	

Defect ID: DEFECT000503942	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** EZSS Switch Manager
Symptom: Unable to configure 7840 using EZ Setup	
Condition: In some cases the EZ Setup for 7840 may fail with ambigous error message and display issues.	
Recovery: Relaunch EZ Manager to restart EZ Setup	

Closed with code in Fabric OS v7.3.1

Defect ID: DEFECT000504254	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.1.1	**Technology Area:** Other
Symptom: Intermittent systemverification failures may be encountered when the number of test runs are increased to 50 or more.	
Condition: This problem is encountered only when the parameters for systemverification test are modified to a different value which the system does not support. This works as expected under normal circumstance, with supported values.	

Defect ID: DEFECT000505389	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.3.0	**Technology Area:** Other
Symptom: Switch may be Disabled due to internal ports not being Online	
Condition: This may be encountered in rare circumstance on a Brocade 7840 switch	

Defect ID: DEFECT000507532	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: This is a display issue of dashboard. DB shows wrong or NULL flow name if user does slotpoweroff/on	
Condition: This is a cosmetic display issue seen on dashboard only when user performs slotpoweroff/on.	

Defect ID: DEFECT000511542	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** supportShow
Symptom: Running supportsave on a director switch with faulted FC8-48E blades may lead to panic and cold recovery.	
Condition: This may occur when supportsave is run with blades in faulted state with reason code of PCI timeout (90) or power issues (28)	

Defect ID: DEFECT000512347	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.1.1	**Technology Area:** Access Gateway
Symptom: Logical port WWN displayed by the "portshow" CLI may change after hot code load or haReboot on a switch running in AG mode, followed by any subsequent offline/online event to the F_Port trunk ports.	
Condition: This may occur under the following conditions: - Upgrade or downgrade to firmware versions v6.1.2d, v6.2.2, or v6.3.0 and above. - Hareboot on firmware versions v6.1.2d, v6.2.2, or v6.3.0 and above. - Then disable / enable all ports of F-port trunk.	
Workaround: Cold boot of the switch in AG mode.	

Closed with code in Fabric OS v7.3.1

Defect ID: DEFECT000512726	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.0.2	**Technology Area:** Fabric Watch
Symptom: Multiple FW-1038 and FW-1042 messages reported, indicating that the SFP RX and TX power are below boundary - current value 0 uwatts.	
Condition: This may occur only when a switch CPU is very busy.	

Defect ID: DEFECT000513806	
Technical Severity: Low	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.2.0	**Technology Area:** Other
Symptom: Sorting switch events by date does not function properly in webtools	
Condition: This issue is seen in webtools, only when sorting events on the Time column, following an upgrade to Fabric OS version v7.2.0d. This sorting operation on the Time column does not function properly.	

Defect ID: DEFECT000515187	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** System
Reported In Release: FOS7.1.2	**Technology Area:** CLI
Symptom: While performing CLI command “seccertutil delkey”, the certificates/keys are truncated to zero but the "Certificate File" does not become "none". This may cause the switch to panic due to configuration inconsistencies.	
Condition: This may occur when executing the CLI command "seccertutil delkey".	

Defect ID: DEFECT000515313	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Fabric Watch
Symptom: While performing a supportsave, user may see benign display messages, interspersed with the supportsave output.	
Condition: This may be seen when the user attempts a supportsave operation after deleting frame monitoring.	

Defect ID: DEFECT000515403	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.2	**Technology Area:** supportShow
Symptom: Some command names are missing in SSHOW files of supportsave.	
Condition: This issue occurs in Director class platforms.	

Defect ID: DEFECT000516108	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: QSFPs having serial number starting with "HUA" are being monitored using ALL_OTHER_SFP group. These should instead be monitored under ALL_QSFP or some other special QSFP group. All other QSFPs are correctly monitored under ALL_QSFP.	
Condition: This is encountered only with QSFPs having serial number starting with "HUA" .	

Closed with code in Fabric OS v7.3.1

Defect ID: DEFECT000516196	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** System
Reported In Release: FOS7.3.0	**Technology Area:** CLI
Symptom: BNA users may witness failure in moving ports across LS's on Brocade 7840 switch.	
Condition: This may be encountered following the CLI command 'portCfgDefault' on GE ports of Brocade 7840 Switch.	

Defect ID: DEFECT000516309	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.0.0_pha	**Technology Area:** Access Gateway
Symptom: Hosts have problems logging into the fabric through an Access Gateway.	
Condition: This may be encountered under the following conditions: - Hosts are connected to an Access Gateway. - F-ports on Access Gateway have NPIV logins. - Different hosts login and logout of the same Access Gateway F-port, and - Access Gateway Persistent AL_PA feature is enabled.	
Recovery: Identify all affected F-ports with duplicate ALPA entries ag --printalpamap <port#> Disable _all_ the affected F-ports with duplicate ALPA entries portdisable <port#> ag --clearalpamap <port#> portenable <port#>	

Defect ID: DEFECT000516632	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** CLI
Symptom: Userspace daemon mdd may crash after an extended period. This incident is benign since the daemon is automatically restarted	
Condition: This is a rare occurrence resulting from a very slow memory leak in L2 device monitoring. With the default polling rate of once per day the incident may occur about once a year. Accelerated polling will increase the frequency but the daemon is automatically restarted and the incident is rendered benign.	

Defect ID: DEFECT000517927	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.2.1	**Technology Area:** Access Gateway
Symptom: Following an upgrade, BES panics when user attempts to enable access gateway.	
Condition: This is encountered on FOS v7.2.x and v7.3.x code streams; However, FOSv7.3 no longer support access gateway mode on BES switch, and FOS7.3.1 now enforces the no support.	
Workaround: Avoid enabling access gateway mode on encryption switches.	

Defect ID: DEFECT000519313	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.0.2	**Technology Area:** Other
Symptom: Internal ports may not be properly enabled or disabled after boot-up.	
Condition: This may be encountered on a very busy system, where expansion commands from SVP may not get processed in time.	
Recovery: The problem is intermittent. The expansion command can be re-triggered if any of the server blades is moved.	

Defect ID: DEFECT000519965	
Technical Severity: Critical	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.1.1	**Technology Area:** Other
Symptom: FCoE AP blades may be faulted following a firmware upgrade.	
Condition: This may occur due to ethernet connectivity issues on FCOE blades that have been up for a long period of time.	

Defect ID: DEFECT000520219	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: customer cannot achieve Port Decom even though that action is configured in the rule	
Condition: This is encountered if Port Fence and Port Decom are the only actions configured in the rule	

Defect ID: DEFECT000520550	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.3.0	**Technology Area:** Routing
Symptom: SW7840 Hot Code Load encountered an ESM fatal error during Failback which resulted in cold recovery.	
Condition: This may occur when a pair of SW7840s are tunnel-linked in all 4 Logical Partitions, and an HCL is performed on just one of the two SW7840s.	
Recovery: No recovery is necessary, after the HCL completes a cold reboot, the switch and tunnel(s) are stable again.	

Defect ID: DEFECT000521166	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS6.4.3	**Technology Area:** Name Server
Symptom: Corrupted frames cause nsd to panic and result in multiple switches in the fabric to cold boot.	
Condition: This may occur upon a rare hardware failure on a neighboring switch, resulting in corrupted nsd query response frames arriving at the other switches in the fabric.	
Recovery: Remove the failed blade or switch to eliminate the cause of these corrupted frames.	

Defect ID: DEFECT000521195	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.2.0	**Technology Area:** FICON
Symptom: Add ability to enable insistent domain ID (IDID) while the switch is online to permit non-disruptive upgrade v7.2.x to v7.3.	
Condition: As per design, upgrade to from FOS7.2.x to FOS v7.3 is blocked if customer has single switch fabric in FMS mode with SCC policy configured but IDID OFF. It requires a "switchdisable" in FOS v7.2.x to set IDID ON.	

Closed with code in Fabric OS v7.3.1

Defect ID: DEFECT000521209	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** POST - Power-on Self-Test
Symptom: POST tests do not run as expected using CMM.	
Condition: Issue happens when POST tests are verified through CMM on embedded switches.	

Defect ID: DEFECT000521218	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** Extended Fabrics
Symptom: Host discovery issues after upgrade to FOS7.2.x in FC Routed configuration over VE/VEX ports	
Condition: These host discovery issues may be encountered following upgrade to any FOS7.2.x release from a FOS version prior to FOS7.2.0, in FC Routed configuration over VE/VEX ports	
Workaround: Downgrade to a FOS release prior to FOS7.2.0.	

Defect ID: DEFECT000521272	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.1	**Technology Area:** Fabric Watch
Symptom: FW-1430 raslog messages logged to indicate possible faulty temperature sensor, but with no subsequent FW-1003 messages to indicate which sensor is triggering the alarms.	
Condition: This may be encountered if the sensor issue is transient in nature and problem recovers before triggering subsequent faults.	

Defect ID: DEFECT000521398	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.1.1	**Technology Area:** Other
Symptom: Before shutdown switch due to a high temperature alert, emd encountered an assert and caused switch to panic.	
Condition: This may happen during switch shutdown following a high temperature warning "Unit will be shut down in 2 minutes if temperature remains high"	

Defect ID: DEFECT000522602	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** System
Reported In Release: FOS7.3.0	**Technology Area:** CLI
Symptom: 'fabricshow -v' does not display FOS revision patch id under "Version" column.	
Condition: Display content overrun the declared array size.	

Defect ID: DEFECT000522807	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: User space daemon mdd might auto restart due to memory corruption.	
Condition: This happen when more than 5 rules get trigger for more than 2-3 hours.	

Closed with code in Fabric OS v7.3.1

Defect ID: DEFECT000523092	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** System
Reported In Release: FOS7.3.0	**Technology Area:** CLI
Symptom: Unable to collect supportsave on BR5460 with error msg: "The switch does not have enough disk space to run full supportSave. Available Free disk space is 27 MB."	
Condition: This is encountered when Compact Flash available free space is low	

Defect ID: DEFECT000523193	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.1.0	**Technology Area:** FICON emulation
Symptom: IFCC during tape reads - Emulation Error Code=86 during REPOSITION_PENDING_STATE	
Condition: When FICON tape read pipelining is active and the device presents Short Busy status	
Workaround: Disable FICON Read Pipelining	
Recovery: The I/O recovers on its own - no further action is required.	

Defect ID: DEFECT000523451	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.2.0	**Technology Area:** Other
Symptom: Customer may experience a cold boot on the DCX after bouncing FCoE port	
Condition: This may occur during a small timing window, when an external FCoE interface goes down, the corresponding internal FI ports is moved to temporary internal state and ELS frames arrive at the same time, triggerring a CPU busy condition.	
Recovery: Switch cold boots and recovers on its own. No further recovery action is necessary.	

Defect ID: DEFECT000523507	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.2	**Technology Area:** Fabric Watch
Symptom: Fabric Watch ST area of SFP class does not change to "pause" when executing CLI " thconfig --pause sfp -area all -port all" or gives any error to indicate that it's not supported.	
Condition: The issue is seen only when the ST area option is used with SFP class. ST is already deprecated in FOS v7.0.0 and no longer supported.	

Defect ID: DEFECT000523796	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.0	**Technology Area:** BB Credits
Symptom: Increased latency and negative performance impact may be encountered in an edge/core configured fabric.	
Condition: This may be observed when hosts exhibiting mild latency behavior are present, along with over-subscribed devices leading to congestion within the fabric.	
Workaround: Remove or Isolate latency devices into QoS zone to avoid impact to others in fabric	

Defect ID: DEFECT000524168	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Diagnostic Port (D_Port)
Symptom: AG ports get disabled, instead of coming up as N-ports.	
Condition: It happens when connecting AG to switch with On-Demand D_Port's ports.	

Defect ID: DEFECT000524328	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.3.0	**Technology Area:** Monitoring and Alerting Policy Suite (MAPS)
Symptom: User will not see rules triggered for utilization statistic.	
Condition: This only applies to FOS7.3.0 and later	

Defect ID: DEFECT000525285	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** System
Reported In Release: FOS7.3.0	**Technology Area:** CLI
Symptom: CLI command "firmwaredwonload" may fail with SULB-1011 raslog message “Firmwaredownload command failed. Unexpected reboot occurred during firmware download. The command is aborted.” but with no apparent unexpected actual reboot.	
Condition: This may occur in a rare situation from a failure in setting an internal state variable. The resulting unexpected state leads firmwaredownload to infer there has been an unexpected reboot.	
Recovery: Rerun the firmwaredownload command.	

Defect ID: DEFECT000525347	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.2	**Technology Area:** FC-FC routing
Symptom: Customer may observe performance issues between multiple servers and storage with EX-port connected to VDX	
Condition: This may occur when there are link level errors that trigger credit loss on 16G EX port and there was prior HA warm recovery that disabled credit leak detection.	
Recovery: Bounce the port to recover	

Defect ID: DEFECT000525834	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Web Tools
Symptom: Invalid IP Address/Domain is populated in the "Please Login" WEB Tools dialog display, disregarding the configured details.	
Condition: When both ipv4/ipv6 are configured: 1. ipv4 address is shown when attempting to login via ipv6 2. ipv4 address is shown when attemping to login with domain name	

Defect ID: DEFECT000526158	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Other
Reported In Release: FOS7.0.2	**Technology Area:** Other
Symptom: Customer may observe increasing er_crc_good_eof and er_enc_in errors on backend ports, leading to performance problems.	
Condition: This may be be seen in a DCX 8510-8 system with FC8-64 port blades in slots 1, 2, 11, 12;	
Recovery: Additional tuning on DCX-4s with FC8-16, FC8-32, FC8-48 and FC8-64.	

Closed with code in Fabric OS v7.3.1

Defect ID: DEFECT000526777	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0_hit	**Technology Area:** Platform Services
Symptom: When SVP sends the expansion commands, the BR6546 doesn't respond to the requests intermittantly. The result is that some of the internal ports may not be properly enabled/disabled.	
Condition: The issue happens when BR6546 is busy processing the previous request and can't respond to the new ones. And the additional polling period is larger than the SVP's retry interval so it can't catch the retry requests from SVP.	
Workaround: The issue has been fixed by optimizing the polling mechanism and the request response routines so that it won't miss the retries from SVP.	
Recovery: Combined with the fix on IOSW, the issue can be recovered if SVP sents retry request at proper intervals.	

Defect ID: DEFECT000526934	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** FCIP
Symptom: CLI "portcfg ipif ge2.dp0 delete 2102:211:31:dead::2:7" returns "IP Address configuration on BCM failed" message	
Condition: Run a scrip to perform tunnel deletion/creation in a loop, issue was seen during second deletion	

Defect ID: DEFECT000527848	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.2.0	**Technology Area:** FICON emulation
Symptom: FCIP FICON emulated Tape VM SPOOL DUMP jobs fail after FOS upgrade	
Condition: This may be seen upon upgrade to FOS v7.2.0d, when using FICON Tape Emulation for VM tape operations	
Workaround: Disable FCIP FICON Tape emulation or downgrade to a FOS version without fix for TR 414719	

Defect ID: DEFECT000527997	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Management
Reported In Release: FOS7.3.0	**Technology Area:** Licensing
Symptom: FOS7.3.0 LicenseShow no longer shows capacity values for capacity based licenses on switches.	
Condition: Customer using "licenseshow" with FOS7.3.0 or later. Director products are not impacted.	

Defect ID: DEFECT000528085	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.1	**Technology Area:** Name Server / Zoning
Symptom: Devices are unable to discover their targets due to failure of login (PLOGI) to the Name Server because the PLOGI never receives a response.	
Condition: This may be encountered when running FOS versions v7.2.1a or higher and back-to-back FLOGIs are sent from a device such that the second FLOGI is sent before the device receives an ACC for the first FLOGI.	

Closed with code in Fabric OS v7.3.1

Defect ID: DEFECT000528207	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.1.0	**Technology Area:** Bottleneck Detection
Symptom: Inconsistent slot/port display format in Bottleneck Detection related RASLOG messages make it hard to read, track, and program to monitor these messages.	
Condition: This may occur when there is congestion or slow drain devices in a fabric.	

Defect ID: DEFECT000528631	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS6.4.2	**Technology Area:** Name Server / Zoning
Symptom: Fibre Channel Common Transport (FC_CT) response to GPL query exceeds maximum allowed size and causes 3rd party HBA in a non-responsible state.	
Condition: This happens when HBA makes the GPL query to remote switch. Query to directly connected switch is not impacted.	

Defect ID: DEFECT000531265	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.3.0	**Technology Area:** Extended Fabrics
Symptom: During an upgrade of BR7800 from FOS v7.1.0 or later to FOS v7.1.2a, FOSv7.1.2b, FOSv7.3.0, v7.3.0a, v7.3.0b, v7.3.0c, the switch may go into a rolling reboot.	
Condition: This is encountered only if the switch was shipped with FOS7.1.0GA or later.	

Defect ID: DEFECT000531517	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.2	**Technology Area:** Port Bring-up
Symptom: Link to host failed to come up when configured at 'Fixed 4 Gbps'. Trace dump shows that the host issued NOS/OLS/LIP primitives after speed negotiation, but the switch did not respond.	
Condition: Switch port configured with "Fixed 4G" mode may get its RX incorrect when connected to 8G HBA in Auto Negotiate (AN) mode.	

Defect ID: DEFECT000531571	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.0	**Technology Area:** Port Bring-up
Symptom: Port blade remained faulted after a power event.	
Condition: This may occur in a rare scenario, when CP is up for a while and memory is utilized to cache file system buffers and a blade is power cycled. In this small timing window, this may lead to free memory not being readily available for blade initialization.	
Recovery: slotpoweroff/on the blade to recovery	

Closed with code in Fabric OS v7.3.1

Defect ID: DEFECT000532851	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.3.0	**Technology Area:** Security Vulnerability
Symptom: Security vulnerability CVE-2009-1895 makes it easier for local users to leverage the details of memory usage.	
Condition: The personality subsystem in the Linux kernel before 2.6.31-rc3 has a PER_CLEAR_ON_SETID setting does not clear the security-relevant compatibility flags when executing a setuid or setgid by a program, which makes it easier for local users to leverage the details of memory usage to (1) conduct NULL pointer dereference attacks,(2)bypass the mmap_min_addr protection mechanism, or(3)defeat address space layout randomization	

Defect ID: DEFECT000532888	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.1.0	**Technology Area:** FICON emulation
Symptom: I/O Errors to FICON extended device over an FCIP Tunnel with FICON Emulation features enabled.	
Condition: When running FICON channel programs to an extended device that includes Repeat Execution CCW commands (typically used in Disk I/O channel programs).	
Workaround: Disable the FCIP FICON emulation Idle Status Accept feature. The feature can be disabled via the following command: portcfg fciptunnel <slot/>vePort modify --ficon-debug NewFlags Where NewFlags includes the 0x1000 bit.	

Closed without Code Change in Fabric OS v7.3.1

This section lists the defects with Critical, High and Medium Technical Severity closed without a code change as of December 12, 2014 in Fabric OS v7.3.1

Defect ID: DEFECT000533422	**Technical Severity:** High
Reason Code: Already Fixed in Release	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.1	**Technology Area:** FC-FC routing
Symptom: Fabric router switch may observe panic upon receiving invalid frame from edge switch.	
Condition: This happens when fabric router running FOS7.2.x or earlier receives unknown Fibre Channel Common Transport (FC_CT) request from edge switch with zero sized payload. This does not apply to FOS v7.3.x or later.	
Recovery: Disable edge switch port and upgrade.	