Brocade Fabric OS v7.2.0d
Release Notes v1.0

February 28, 2014

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v7.2.0d Release Notes v1.0	Initial Release	February 28, 2014

Contents

Overview

Fabric OS (FOS) v7.2.0d is a patch release based on FOS v7.2.0c. All hardware platforms and features supported in FOS v7.2.0c are also supported in FOS v7.2.0d.

This release is FICON qualified. Please refer to the *Appendix: Additional Considerations for System z (FICON) Environments* section for feature details and notes on deployment in FICON environments.

Due to the impact of defect 491192 and 494570, Brocade recommends all customers planning or using FOS v7.2.0a, v7.2.0b, and v7.2.0c to upgrade to FOS v7.2.0d.

Note: If customers are already running FOS v7.2.0a, v7.2.0b, or v7.2.0c on their switches, and the "Custom.index" on the switches are either 0 or 4, they can choose to continue running the same FOS version because defect 491192 and 494570 do not apply to these switches. To find out the "Custom.index" setting on a switch, users can run CLI command "configShow |grep Custom".

Resolution of Important Defects

- DEFECT000494570 - FOS7.2.0c containing Defect 491192 fix with pre-existing logical switch may still experience fabric wide performance issue or host cannot see target after slot offline event
- DEFECT000492849 - FCIP link became unstable after some runtime.

New Hardware Support

FOS v7.2 does not introduce support for any new hardware platform, while it adds support for the existing embedded switches 5431, 6547 and M6505 on a major FOS release.

Summary of New Software Features

FOS v7.2 includes support for several new software features and enhancements:

- MAPS (Monitoring and Alerting Policy Suite)
- Flow Vision
- FCR enhancements
- FCIP enhancements
- D_Port enhancements
- Access Gateway enhancements
- Encryption platform (BES/FS8-18) enhancements
- FICON enhancements
- Miscellaneous enhancements

New Feature Descriptions

MAPS (Monitoring and Alerting Policy Suite)

FOS v7.2 implements a new easy to use policy based monitoring and alerting suite that proactively monitors the health and performance of the SAN infrastructure to ensure application uptime and availability. Brocade MAPS helps users to uncover potential problems in the SAN fabric quickly, before they cause application performance impacts or costly failures.

MAPS is a key component of Brocade's Fabric Vision technology that is aimed at dramatically reducing the operational complexity in managing the SAN infrastructure and ensuring application uptime and availability.

Note: Usage of MAPS features requires the Fabric Vision license or both the Fabric Watch and Advanced Performance Monitoring (APM) licenses.

MAPS offers the following capabilities:

- Policy Based Monitoring

  The policy based monitoring feature of MAPS offers the following capabilities:

  - Pre-defined monitoring groups and pre-defined monitoring policies with customization capability

  MAPS enables easier monitoring of the switch by providing pre-defined monitoring groups and pre-validated monitoring policies that users can readily enable, while still providing the flexibility to the end users to create their own custom monitoring groups and custom monitoring policies.

  A MAPS monitoring policy is a collection of monitoring rules and actions associated with each rule. Users can define multiple monitoring policies but can activate only one monitoring policy at a time on the switch. This, for example, allows users to use a certain monitoring policy in production and a different monitoring policy during maintenance.

  MAPS provides pre-defined monitoring groups for monitoring switch ports attached to servers, switch ports attached to storage, E_ports, short wavelength SFPs, long wave length SFPs, etc. MAPS also provides pre-defined monitoring policies such as aggressive, moderate and conservative policies, based on different monitoring thresholds and actions. Users can choose one of these pre-defined policies, modify select rules within any of the pre-defined policies, or create their own custom groups and custom policies for monitoring the switch.

  MAPS customization capability allows users to create custom monitoring groups, such as a group of switch ports that are attached to high priority applications, medium priority applications, low priority applications, etc. and monitor these groups using their own unique rules. For example, users may choose to "port-fence" a problematic port connected to a low priority application, while choosing only to notify via RASlog if that port is connected to a high priority application.

  With Brocade Network Advisor 12.1 or later, users can apply a given monitoring policy across multiple switches and multiple fabrics instantly, ensuring consistent monitoring across an entire environment.

  - Flexible monitoring rules

  MAPS provides flexible monitoring rules to monitor a given counter for different threshold values and take different actions when each threshold value is crossed. For example, users can monitor a CRC error counter at a switch port and can generate a RASlog when the error rate is more than two per

minute, send an e-mail notification when the error rate is at five per minute, and fence a port when the error rate exceeds ten per minute.

- Ability to monitor both sudden failures and gradual degradations

MAPS provides the ability to not only detect abnormal conditions but also gradually deteriorating conditions in the switch. For example, if a CRC error counter at a switch port increments suddenly at the rate of five per minute, MAPS can detect and alert the end users about that condition. Similarly, if the CRC error counter is gradually incrementing at the rate of five per day, even that condition can be detected and reported by MAPS as well, with a different action taken for each condition.

- Support for multiple monitoring categories

MAPS supports various monitoring categories such as: Switch status, Port health, FRU (Field Replaceable Unit) health, Security violations, Fabric state changes, Switch resource, Traffic performance and FCIP health.

This essentially enables monitoring of the overall switch status, switch ports, SFPs, port blades, core blades, switch power supplies, fans, temperature sensors, security policy violations such as login failures, fabric reconfigurations, CPU and memory utilization of the switch, traffic performance at port, FCIP circuits health, etc.

- Support for multiple alerting mechanisms and actions

MAPS provides various mechanisms to deliver alerts to the end users via RASlogs, SNMP traps and e-mail notifications when the monitoring thresholds are exceeded. MAPS also allows users to perform port fencing action when errors on a given port exceed a certain threshold. MAPS alerting mechanisms/actions are associated with each monitoring rule. However, users are also given the flexibility to enable or disable these alerting mechanisms/actions for the entire switch. This for example, helps users to suppress all alerts during a maintenance window, or when testing and "tuning" new rules within a policy.

- CLI Dashboard

MAPS provides a CLI based dashboard of health and error statistics to provide an at a glance view of the switch status and various conditions that are contributing to the switch status. This enables users to get instant visibility into any hot spots at a switch level and take corrective actions.

The summary section of the dashboard provides the overall status of the switch health and the status of each monitoring category. If there is any category deemed to be out of "normal" status due to violations of rules, the dashboard shows the rules that were triggered for that category.

The dashboard also provides historical information of the switch status for up to seven days. It provides raw counter information of various error counters such as CRC, Class 3 Transmit Timeout Discard, Link Resets, etc. without requiring users to set any monitoring policy. This historical counter information can also be used to assist the user in fine-tuning their MAPS rules by showing where a particular threshold may be just missing catching a particular behavior on the switch.

Note: Brocade Network Advisor 12.1 or later provides a feature rich dashboard that provides **fabric-wide** visibility of hot spots, deeper historical information and much more. Please refer to Brocade Network Advisor 12.1 documentation for additional details.

- Bottleneck Detection integration with MAPS dashboard

Bottleneck Detection information is integrated with MAPS dashboard. The "Summary" section of the dashboard shows bottleneck events detected by the Bottleneck Monitor. The "History" section of the dashboard shows entries for bottlenecked ports, including transient bottlenecks that are not detected by the Bottleneck Monitor. This enables users to get at an instant view of the bottlenecked ports in the switch and enables rapid problem resolution.

- Proactive Flow Monitoring using MAPS

MAPS can monitor flows created under Flow Vision's "monitor" sub-feature and generate alerts based on user defined rules. To monitor a flow using MAPS, users must first create and activate the flows using Flow Monitor, and then import those flows into MAPS for monitoring. This enables users to monitor and be alerted on various conditions such as, when bandwidth utilization at a port for a given flow exceeds a certain threshold or falls under a certain threshold, when number of SCSI reservation frames at a LUN exceeds a certain threshold, etc.

- Automated Migration of existing Fabric Watch configuration to MAPS

Users who are currently monitoring a switch using Fabric Watch can automatically import all of their Fabric Watch thresholds into a MAPS policy, allowing them to seamlessly migrate from Fabric Watch to MAPS. This allows users to retain monitoring behaviors that have been developed for their unique environment over time, and also take advantage of the powerful new capabilities in MAPS and usability improvements. (Note that the Fabric Watch and MAPS features are mutually exclusive on an individual switch. Only one or the other can be active at one time.)

Flow Vision

Flow Vision is a key component of Brocade's Fabric Vision technology being introduced in FOS v7.2 that provides comprehensive visibility into application flows in the fabric and the ability to non-disruptively create copies of the application flows that can be captured for deeper analysis. Flow Vision also provides test flow generation capability that can be utilized to pre-test a SAN infrastructure for robustness before deploying applications. The test flow generation capability is also useful for testing the internal connections on a switch to ensure ideal performance before deploying the switch into a production environment.

Flow Vision includes the following key features:

- Flow Monitor:
    - Provides comprehensive visibility into application flows in the fabric, including the ability to learn (discover) flows automatically.
    - Enables monitoring of application flows (Example: From a Host to a Target/LUN) within a fabric at a given port.
    - Provides statistics associated with the specified flows to gain insights into application performance. Some of these statistics include:
        - Transmit frame count, receive frame count, transmit throughput, receive throughput, SCSI Read frame count, SCSI Write frame count, number of SCSI Reads and Writes per second (IOPS), etc.
    - When NPIV is used on the host, users can monitor VM (Virtual Machine) to LUN level performance as well.
    - Enables monitoring of various frame types at a switch port to provide deeper insights into storage I/O access pattern at a LUN, reservation conflicts, and I/O errors.
        - Example: SCSI Read, SCSI Write, SCSI Reserve, ABTS, BA_ACC, etc.
    - Integrated with MAPS to enable threshold based monitoring and alerting of flows.

- Flow Generator:
    - Flow generator is a test traffic generator for pre-testing the SAN infrastructure (including internal connections) for robustness before deploying the applications.
    - Allows users to configure a16G FC capable port as a simulated device that can transmit frames at full 16G line rate.
    - Users can emulate a 16G SAN without actually having any 16G hosts or targets or SAN-testers, and pre-test the entire SAN fabric including optics and cables on ISLs, internal connections within a switch, at full line rate.
    - The traffic generator port must be a 16G FC capable port while the traffic destination port can be an 8G or a16G capable FC port on any switch in the fabric (the test traffic is terminated at the destination port and does not leave the switch).
- Flow Mirror:
    - Provides the ability to non-disruptively create copies of application flows that can be captured for deeper analysis. Only mirroring to the CPU of the switch is supported in FOS v7.2.
    - Used for in-depth analysis of flows of interest – SCSI Reservation frames, ABTS frames, flows going to a bottlenecked device, frames during link bring up, etc.
    - Users can select the type of frames to be mirrored.
    - Supported only on 16G FC capable platforms.

Note:
Flow Vision features require the Fabric Vision license or both Fabric Watch and APM licenses.

FCR Enhancements

FOS v7.2 supports the following FCR enhancements:

- EX_Port support on optical ICLs of DCX 8510
    - Provides the ability to configure EX_Ports on the ICL links of DCX 8510 platforms connected to other DCX 8510 platforms.
    - Allows users to build very high performance IFLs (Inter Fabric Links) using ICLs – simplifies cabling as well.
    - Supported only when Virtual Fabrics (VF) is enabled on DCX 8510.
- Increased FCR scalability: FOS v7.2 supports up to 6000 devices per edge fabric (an increase from 2000). Refer to the Brocade SAN Scalability Guidelines document for more information.
- Routing enhancements to select the lowest cost links in the FCR fabric when there are multiple routes available between FCR edge fabrics through an FCR backbone fabric.

FCIP Enhancements

FOS v7.2 adds support for a new FCIP Tunnel failover configuration option that provides the following capabilities:

- Allows a user to define a Failover Group that includes a subset of the circuits in the FCIP Tunnel.
- Provides a more deterministic failover configuration that would allow a mixture of metric 0 and metric 1 circuits to be used in the event of a metric 0 circuit failure.

ClearLink Diagnostics: D_Port Enhancements

FOS v7.2 adds the following D_Port enhancements:

- Enhancement to D_Port test results

  Starting with FOS v7.2 complete results of the D_Port tests will be available on the responder switch as well. Prior to FOS v7.2, D_Port test results on the D_Port responder switch did not include optical and remote loopback test results. Complete results were only available on the D_Port initiator switch.

- D_Port support between Brocade 16G HBA and Brocade 16G Access Gateway.

- Dynamic D_Port support between Brocade 16G HBA and Brocade 16G switch
  - With this enhancement users do not need to explicitly configure D_Port on the switch.
  - A switch port enters D_Port mode upon request from the HBA, D_Port tests then get performed and the switch port reverts back to the normal mode after the D_Port tests are completed.
  - This enhancement significantly reduces the operational overhead by eliminating several manual configuration steps.

Access Gateway Enhancements

FOS v7.2 supports the following Access Gateway enhancements:

- D_Port diagnostics support on the links between Brocade 16G HBA and Brocade 16G Access Gateway to assess SFP and cable health.

- Detect and prevent duplicate PWWN at the time of login.

Encryption Platform (BES/FS8-18) Enhancements

FOS v7.2 introduces the following enhancements for the encryption platforms:

- KMIP Support for TEKA (Thales e-Security Key Authority)
- Thin Provisioning support for IBM XIV and EMC VMAX

FICON Enhancements

FOS v7.2 implements the following FICON enhancements:

- Added the ability for the CUP Diagnostics to determine the firmware version of all the switches in the fabric which allows interoperability with FOS v7.1
- Implemented a new Command Reject Error Code provided by IBM to help define “Fabric Errors”.

Miscellaneous Enhancements

FOS v7.2 supports several useful enhancements across various feature categories:

- FOS v7.2 allows 10G speed configuration on all ports of a 16G FC blade and 16G switch (6510, 6520 only)
  - Provides more flexibility to the end users to enable 10G capability on any port
  - Also provides more flexibility to enable encryption/compression on 10G ports.

    Pre-FOS v7.2 limited 10G FC support to only the first 8 ports of a 16G switch or a 16G blade. This also limited the ability to enable encryption/compression to only two of those first 8 ports due to restrictions on the number of ports supported per ASIC. By removing this restriction, FOS v7.2 allows users to enable more 10G FC ports for encryption and compression by spreading them across multiple ASICs.

- FOS v7.2 allows buffer credit assignment even for “normal distance” (regular) E_ports
    - The portCfgEportCredits CLI introduced in FOS v7.2 allows users to perform fine grained performance tuning on normal E_ports by allowing users to specify buffer credits.
- In FOS v7.2, the portaddess CLI has been enhanced to display an address as user bound when a user has explicitly bound an address to a port.
- FOS v7.2 introduces a new CLI “creditrecovmode” to configure backend link credit loss recovery options
    - Existing credit loss recovery options of the bottleneckmon CLI continue to be supported in FOS v7.2 but will be removed from FOS v7.3.
    - Simplifies the bottleneckmon CLI.
- FOS v7.2 allows users to provide a reason string when disabling a port via portdisable or portcfgpersistentdisable CLIs – helps to track the user intention for disabling a particular port.
- FOS v7.2 introduces new RASlogs (FSPF-1013, FSPF-1014) and new CLI outputs in fabricshow and topologyshow to indicate when the maximum paths (16) to a remote domain are exceeded.

Optionally Licensed Software

Fabric OS v7.2 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 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 offline 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 license is enabled by default on all 16G FC platforms, and on DCX and DCX-4S platforms that are running Fabric OS v7.0.0 or later.

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, or Brocade Encryption Switch to be configured as an Ex_port or VEx_port (on some platforms) supporting Fibre Channel Routing. This eliminates the need to add an FR4-18i blade or use the 7500 for FCR purposes, and also provides double or quadruple the bandwidth for each FCR connection (when connected to another 8Gb or 16Gb-capable port). .

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 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. On the Brocade 6510, Brocade 6520 this license enables 10G FC ports.

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, 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 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.

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 ten DCX 8510 chassis connected in a core-edge topology. Refer to the Brocade SAN Scalability Guidelines document for additional information.

Temporary License Support

The following licenses are available in FOS v7.2 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

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 v7.2 supports the following existing platforms:

- 300, 5100, 5300, 7800, VA-40FC, Brocade Encryption Switch, DCX, DCX-4S
- 6505, 6510, 6520, DCX 8510-8, DCX 8510-4
- FC16-32, FC16-48, FC8-32E, FC8-48E, FX8-24, FS8-18 on DCX 8510-8/DCX 8510-4
- FC8-16, FC8-32, FC8-48, FC8-64, FX8-24, FS8-18, FCOE10-24 on DCX/DCX-4S
- 5410, 5424, 5430, 5450, 5480, 5470, 5460, NC-5480
- Support merged to FOS v7.2: 5431, 6547, M6505

Access Gateway mode is also supported by Fabric OS v7.2, and is supported on the following switches: the Brocade 300, 5100, VA-40FC, 5450, 5430, 5431, 5460, 5470, 5480, NC-5480, M5424, 6547, 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 conform to the following Ethernet standards:

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1s Multiple Spanning Tree
- IEEE 802.1w Rapid reconfiguration of Spanning Tree Protocol
- IEEE 802.3ad Link Aggregation with LACP
- IEEE 802.3ae 10G Ethernet
- IEEE 802.1Q VLAN Tagging
- IEEE 802.1p Class of Service Prioritization and Tagging
- IEEE 802.1v VLAN Classification by Protocol and Port
- IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
- IEEE 802.3x Flow Control (Pause Frames)

The following draft versions of the Converged Enhanced Ethernet (CEE) and Fibre Channel over Ethernet (FCoE) Standards are also supported on the 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 — 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 v7.1 can be non-disruptively upgraded to FOS v7.2.0d. 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.

Note:

To achieve non-disruptive firmware upgrade on 5431, 6547 and M6505 embedded switches to FOS v7.2.0d please follow the instructions given below:

5431:
Upgrade 5431 from FOS v7.0.1_hut to FOS v7.0.1_hut1 before non-disruptively upgrading it to FOS v7.2.0d.

6547:
Upgrade 6547 from FOS v7.0.0_pha3 to FOS v7.0.0_pha4 before non-disruptively upgrading it to FOS v7.2.0d.

M6505:
Upgrade M6505 from FOS v7.0.1_ sh to FOS v7.0.1_sh1 before non-disruptively upgrading it to FOS v7.2.0d.

Disruptive upgrades to Fabric OS v7.2.0d are allowed and supported from FOS v7.0.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 v7.2.0d

Migrating from FOS v7.1

Any 8G or 16G platform running any FOS v7.1. firmware can be non-disruptively upgraded to FOS v7.2.0d.

Migrating from FOS v7.0

Any 8G or 16G platform operating at FOS v7.0.x must be upgraded to FOS v7.1.x before non-disruptively upgrading to FOS v7.2.0d.

Disruptive upgrade to FOS v7.2.0d from FOS v7.0 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 provide 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 12.1.1 is available in

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

For SAN Management, Network Advisor 12.1.1 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 12.1.1 Release Notes, Network Advisor 12.1.1 User Guide, and Network Advisor 12.1.1 Installation, Migration, & Transition Guides.

Note:

Brocade Network Advisor 12.1.1 or later is required to manage switches running FOS 7.2 or later.

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

WebTools Compatibility

FOS v7.2.0, v7.2.0a, and v7.2.0b is qualified and supported only with Oracle JRE 1.7.0 update 25 and update 45. With JRE 1.7.0 update 45, however, users will see a warning message that the application will be blocked in future version of JREs when WebTools is launched through HTTPS. Brocade Network Advisor

users with versions prior to v12.1.4 and Oracle JRE 1.7.0 update 45 will not be able to launch WebTools from Network Advisor.

FOS v7.2.0d is qualified and supported with Oracle JRE 1.7.0 update 25, update 45, and update 51. Users will not see a warning message when WebTools is launched through HTTPS with JRE 1.7.0 update 25 or update 45. Launching WebTools through Brocade Network Advisor is also supported with JRE 1.7.0 update 25 and update 45. Launching WebTools with Oracle JRE 1.7.0 update 51 through Brocade Network Advisor is only supported on version 12.1.5 or later. With JRE 1.7.0 update 51, users could see some browser warning messages that can be ignored.

SMI Compatibility

- It is important to note that host SMI-S agents cannot be used to manage switches running FOS v7.2.

  If users want to manage a switch running FOS v7.2 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[6]
Brocade 5410, 5480, 5424, 5450, 5460, 5470, NC-5480	v6.2.0 or later[6]
Brocade DCX, 300, 5100, 5300	v6.1.0e and later [2 6 8]
VA-40FC	v6.2.1_vfc [6], v6.2.2 or later [6]
Brocade DCX-4S	v6.2.0 or later [6 8]
Brocade DCX with FS8-18 blade(s), Brocade Encryption Switch	v6.1.1_enc or later [6]
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 [6], DCX-4S requires 6.2.x or later[5 6]
Brocade DCX 8510-8/DCX 8510-4	FOS v7.0 or later
Brocade 6510	FOS v7.0 or later
Brocade 6505	FOS v7.0.1 or later

Supported Products and FOS Interoperability	
Brocade 6520	FOS v7.1 or later
5430	FOS v7.1 or later[10]
5431, 6547, M6505	FOS v7.2 or later[10]
48000 with FA4-18 blade(s), Brocade 7600	V6.2.2 or later [6]
Mi10k, M6140 (McDATA Fabric Mode and Open Fabric Mode) [1]	Not Supported

Multi-Protocol Router Interoperability	
Brocade 7500 and FR4-18i blade	V6.2.2 and higher [4 6 8]
McDATA SANRouters 1620 and 2640	Not Supported

NOS (VDX Platform) Interoperability	
Brocade VDX6710, VDX6720, VDX6730	NOS v2.1.1 or later[7]
Brocade VDX8770	NOS 3.0 or later

Table Notes:

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

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

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

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

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

[6] 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.

[7] 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, DCX 8510-4.

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

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

[10] Represents the earliest major FOS version. These embedded platforms running respective dedicated FOS versions can also interoperate with FOS v7.2.

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, 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 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.

Changes in 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

- **SW.mib**
  The following changes have been made to the SW.mib:
  - Added a new counter, swConnUnitUnroutableFrameCounter.
  - Added swFwPowerOnHours in SwFwClassesAreas (supported from v7.0.0).
  - Added swCpuOrMemoryUsage table support for MAPS enabled switches.
  - Added swFCPortDisableReason (SwFCPortEntry) to send a port disable reason as part of the swFCPortScn varbind.
  - Added segmented (incompatible) link remote port/wwn support for connUnitLinkTable/swNBTable.

- **HA.mib**
  Added bpTable (blade processor table) to the MIB (supported from v6.2.0 for blade processor).

- **BRCD-FCIP-EXT.mib**
  Added support for the following MIB objects at tunnel level in the FCIP Extension tunnel. Until and including 7.1.0 release, the following MIB objects were supported only at connection level.
  - fcipExtendedLinkTcpDroppedPackets 1.3.6.1.4.1.1588.4.1.1.3
  - fcipExtendedLinkTcpSmoothedRTT 1.3.6.1.4.1.1588.4.1.1.5
  - fcipExtendedLinkRtxRtxTO 1.3.6.1.4.1.1588.4.1.1.9
  - fcipExtendedLinkRtxDupAck 1.3.6.1.4.1.1588.4.1.1.10
  - fcipExtendedLinkDupAck 1.3.6.1.4.1.1588.4.1.1.11

Deprecated/Obsoleted MIBs

- swFCPortSpeed in SW.mib is obsoleted.
- Customized OID is not supported from 7.1.0 release.

Blade Support

Fabric OS v7.2 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.
Next Generation Distance 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, FC8-32E, FC8-48E	Not supported

Table 1 Blade Support Matrix for DCX and DCX-4S with FOS v7.2

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

Fabric OS v7.2 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.
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	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.
Next Generation Distance Extension Blade (FX8-24)	Up to a max of 4 blades of this type.
FCoE/L2 CEE blade FCOE10-24	**Not supported on DCX 8510 in FOS v7.x**

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

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

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, 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)	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, 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	FC16-32, 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 8Gb ports + QSFP ICLs	FC8-32E, FC8-48E	Port Blade	Not Supported	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	Not Supported	4 Power Supplies	For DCX 8510-8, four (2+2)[1] 220V AC Power Supplies are required when any special purpose blade are installed

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, 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.

Brocade HBA/Adapter Compatibility

- Brocade HBA/Adapter should be using driver version 2.3.0.2 or later when attached to 16G ports on Brocade switches.

D_Port

- FOS v7.0.0a and later support the execution of D_Port tests concurrently on up to eight ports on the switch.
- Support of D_Port is extended to R_RDY flow control mode. The R_RDY mode is useful for active DWDM links that do not work in VC_RDY or EXT_VC_RDY flow control modes.
- A new sub-option "-dwdm" is added to "portcfgdport --enable" CLI to configure D_Port over **active** DWDM links. The "-dwdm" option will not execute the optical loopback test while performing D_Port tests as the **active** DWDM links do not provide necessary support to run optical loopback tests.

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.
- FOS 7.1.0 or later will use SHA256 signatures for the TLS certificates used to connect to the ESKM 3.0 Server using ESKM 2.0 client. Upgrade from FOS v7.0.x to FOS 7.2 and downgrade from FOS 7.2 to FOS v7.0.x would require regeneration and re-registration of CA and signed KAC certificates to restore connectivity to the key vault. Please refer to the Encryption Admin Guide for more details on ESKM/FOS compatibility matrix.
- 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.
- Before upgrading from FOS v7.0.x to FOS7.2, it is required that the RKM server running SW v2.7.1.1 should be upgraded to DPM server running SW v3.2. Please refer to DPM/FOS compatibility matrix in the Encryption Admin Guide for more details.
- 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 v7.1.x to FOS v7.2 or later 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.
- FOS 7.1.0 introduces support for "disk device decommissioning" to the following key vault types: ESKM, TEKA, TKLM and KMIP. To use disk device decommissioning feature for these key vaults, all the nodes in the encryption group must be running FOS v7.1.0 or later. Firmware downgrade will be prevented from FOS v7.2 to a FOS v7.0.x if this feature is in use. Disk Device decommissioning for DPM and LKM key vaults will continue to work as with previous firmware versions.
- FOS7.2 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).

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.

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.

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.

FICON

- For FICON qualified releases, please refer to the *Appendix: Additional Considerations for System z (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, FC8-32E, FC8-48E, Brocade 6510, Brocade 6505 and Brocade 6520.
- 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.
- If users have enabled Virtual Fabrics on a modular chassis platform (DCX, DCX-4S, DCX 8510-8, DCX 8510-4) and created the maximum number of logical switches (eight), and if there are powered off blades or empty slots that are part of any logical switch (including the default switch) for which the flows are defined, then they must delete those flow definitions before performing firmware download or HA failover operations.
- 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.

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.

Port Statistics

- On 16G capable ports, the enc_in (number of encoding errors inside of frames) and enc_out (number of encoding errors outside of frames) counters will not be updated when a port is *operating* at either 10G or 16G speed. This is due to the different encoding scheme used at 10G and 16G speeds when compared to 8G/4G/2G speeds. Because of this, Fabric Watch alerts and Port Fencing based on ITW (Invalid Transmission Word) thresholds will not function as these enc_in and enc_out counters will not be incremented when operating at either 10G or 16G (ITW is computed based on enc_in and enc_out counters). Also any CLI or GUI that displays enc_in and enc_out counters will show no incrementing of these counters when a port is operating at either 10G or 16G.

  Both enc_in and enc_out counters contain valid information when a Condor3-based port is operating at speeds **other than** 10G and 16G.

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

- Please note a documentation correction to the "Table 3 Certified and Tested Platforms" of the Web Tools Administrator's Guide supporting Fabric OS v7.2.0. Unlike what is stated in the table, Web Tools is not supported with the Chrome browser with FOS v7.2.
- 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 certicate 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.
- Launching WebTools with Oracle JRE 1.7.0 update 51 through Brocade Network Advisor is only supported on version 12.1.5 or later. With JRE 1.7.0 update 51, users could see browser warning messages that the WebTools application requires unrestricted access or the certificate signing the application is not recognized. These messages can be ignored. 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.

Zoning

- Support for up to 2MB zone database in a fabric with only DCX/DCX-4S/DCX8510 systems. The presence of any other platform in the fabric will limit the maximum zone database to 1MB. Please note that there is no enforcement by FOS 7.1 or later to restrict users to operate within a zone database limit - it is the responsibility of the user to not exceed this limit.
- 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.
- Beginning with the FOS v6.2.0 release, all WWNs containing upper-case characters are automatically converted to lower-case when associated with a zone alias and stored as part of a saved configuration on a switch. For example, a WWN entered as either "AA.BB.CC.DD.EE.FF.GG.HH" or "aa.bb.cc.dd.ee.ff.gg.hh" when associated with a zone alias will be stored as "aa.bb.cc.dd.ee.ff.gg.hh" on a switch operating with FOS v6.2.0 or later.

  This behavioral change in saved zone alias WWN members will not impact most environments. However, in a scenario where a switch with a zone alias WWN member with upper case characters (saved on the switch with pre-FOS v6.2.0 code) is merged with a switch with the same alias member WWN in lower case characters, the merge will fail, since the switches do not recognize these zoning configurations as being the same.

  For additional details and workaround solutions, please refer to the latest FOS Admin Guide updates or contact Brocade Customer Support.

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.
- POST diagnostics for the Brocade 5100 have been modified beginning with FOS v6.3.1b and v6.4.0 to eliminate an "INIT NOT DONE" error at the end of an ASIC diagnostic port loopback test. This modification addresses BL-1020 Initialization errors encountered during the POST portloopbacktest. (Defect 263200)
- It is important to note that the outputs of slotshow –p and chassishow 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.

Defects

Closed with Code Change in Fabric OS v7.2.0d

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of February 24, 2014 in Fabric OS v7.2.0d.

Defect ID:	DEFECT000494570		
Technical Severity:	High	**Probability:**	Medium
Product:	FOS	**Technology:**	Traffic Management
Reported In Release:	FOS7.2.0	**Technology Area:**	Routing
Closed In Release(s):			
Symptom:	Upgrading to FOS7.2.0c (which contains a fix for defect 491192) with pre-existing user-defined logical switches may lead to fabric wide performance issue or hosts not being able to see targets after a slot offline event		
Condition:	On FOS 7.2.0c, this affects Fabric IDs that do NOT contain a digit of 0, 1, 2, or 5; such as FID 3 or FID 4. FID 35 would not be affected as it contains the digit 5.		
Workaround:	Do not create or modify logical switches, or bounce ports until upgrading to a code revision with fix.		
Recovery:	Use CLI "portcfgdefault" for each port and then cold boot switch to recover, or upgrade to FOS release with the fix - FOS7.2.0d, which will recover and also prevent future occurrence.		

Defect ID:	DEFECT000492849		
Technical Severity:	High	**Probability:**	High
Product:	FOS	**Technology:**	Distance
Reported In Release:	FOS7.2.0	**Technology Area:**	FCIP
Closed In Release(s):			
Symptom:	FCIP link became unstable after some run time and reported the following XTUN messages: 2014/02/03-09:50:40, [XTUN-1008], 12759, CHASSIS, WARNING, , FCIP Control block memory usage slot=0 DP=1 Allocated=5209344 Free=196117248 Total=201326592. 2014/02/03-09:50:41, [XTUN-1001], 12760, FID 128, ERROR, , FCIP Tunnel 16 Memory allocation failed tracker 1/247.		
Condition:	On switch running with FOS 7.2.0b/c and FOS7.2.1, resource is lost when processing periodic vendor unique message ELS-PRLI coming from a disk mirroring application every 5 seconds.		

Defect ID:	DEFECT000487271		
Technical Severity:	High	**Probability:**	Medium
Product:	FOS	**Technology:**	Management
Reported In Release:	FOS7.2.0	**Technology Area:**	Brocade Network Advisor
Closed In Release(s):			
Symptom:	Unable to create flow with Flow Mirror feature through BNA with FOS v7.2.0x		
Condition:	This happens in a race condition when the non-default switch goes to active state prior to the default switch in a VF environment, after a cold boot or hafailover.		
Workaround:	The FOS CLI can be used to successfully create the flow		
Recovery:	User can attempt to restart the flow. If it still fails and user has to use BNA to create flow, upgrade to a FOS code revision with the fix.		

Closed with Code Change in Fabric OS v7.2.0c

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of February 5, 2014 in Fabric OS v72.0c.

Defect ID:	DEFECT000491192		
Technical Severity:	Critical	**Probability:**	Medium
Product:	FOS	**Technology:**	Traffic Management
Reported In Release:	FOS7.2.0	**Technology Area:**	Routing
Closed In Release(s):			
Symptom:	FOSv7.2.0, 7.2.0a, 7.2.0b, 7.2.0c, 7.2.1 with user defined logical switch, hosts may be unable to reach targets due to frames being corrupted or traffic flow may appear to stop.		
Condition:	This happens with customer configuration parameter "Custom.index" of 1,2,3,5, when user creates a logical switch and then moves ports with non-default configuration to it. This can happen for both FOSv7.1.x to FOSv7.2.x upgrade and with freshly installed FOSv7.2.x switches. This does not happen with "Custom.index" of 0 or 4		
Workaround:	Do not create or modify logical switch until upgrade to a code revision with fix.		
Recovery:	Upgrade to a FOS release with the fix (v7.2.0d) will recover and also prevent future occurrence. Downgrading from FOS 7.2.1 to a release with the fix (v7.2.0d) will not correct the problem and v7.2.0d must be downloaded a second time after initial downgrade to v7.2.0d. Upgrade FOS7.2.1 to a future 7.2.1a will address the problem. If a code upgrade is not possible, please use CLI "portcfgdefault" on each port and then cold boot switch to recover		

Defect ID:	DEFECT000481199		
Technical Severity:	Medium	**Probability:**	Medium
Product:	FOS	**Technology:**	Management
Reported In Release:	FOS7.2.0	**Technology Area:**	Web Tools
Closed In Release(s):			
Symptom:	With JRE 1.7.0 update 45, users will see a warning message when WebTools is launched through HTTPS and will not be able to launch WebTools from Network Advisor with prior to v12.1.4 Network advisor revisions		
Condition:	Web Tools will be blocked when it is launched through a version of Network Advisor prior to 12.1.4 on a system running JRE 1.7u45 Web Tools will encounter error messages when it is launched directly through HTTPs on a system running JRE 1.7u45		
Workaround:	Launch Web Tools through Network Advisor running version 12.1.4 or higher		
Recovery:	JRE must be downgraded to 1.7u25.		

Closed with Code Change in Fabric OS v7.2.0b

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of December 2, 2013 in Fabric OS v7.2.0b.

Defect ID: DEFECT000453711	**Technical Severity:** Medium
Summary: Security certificates truncated to zero size causing a continuous reboot	
Symptom: The security certificates truncated to zero size following cert deletion causing a reboot loop	
Probability: Medium	
Feature: FOS Software	**Function:** High Availability
Reported In Release: FOS7.1.0	**Service Request ID:** 1090957

Defect ID: DEFECT000466943	**Technical Severity:** Medium
Summary: FOS switch port does not establish a route	
Symptom: Problematic port will not pass switch traffic	
Probability: Low	
Feature: 8G ASIC Driver	**Function:** Routing
Reported In Release: FOS7.0.2	**Service Request ID:** 1195567

Defect ID: DEFECT000471755	**Technical Severity:** High
Summary: Flow monitor does not work on internal ports on embedded platforms in access gateway mode	
Symptom: Flow monitor is not supported on internal ports of access gateway embedded platforms.	
Probability: High	
Feature: Network Patroller	**Function:** ASIC interfaces
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000471823	**Technical Severity:** High
Summary: FICON Tape Write Emulation control variables go negative causing limited tape performance	
Symptom: Write Emulation Counters go negative causing limited performance. FICON Tape window sizes are never increased from a pipeline of 1 (1 chain).	
Probability: Low	
Feature: FOS Software	**Function:** FCIP
Reported In Release: FOS7.0.0	**Service Request ID:** 1212822

Defect ID: DEFECT000472367	**Technical Severity:** High
Summary: An EX-Port goes into Mod_Invalid state after a switch disable/enable of a core backbone switch	
Symptom: When a user performs a switch disable/enable, one of the EX-Ports can go into the Mod_Invalid state with Speed Mismatch/Incompatible sfp reason	
Probability: Low	
Feature: 16G Platform Services	**Function:** FOS Kernel Drivers
Reported In Release: FOS7.2.0	**Service Request ID:** ,1235215

Defect ID: DEFECT000472649	**Technical Severity:** Medium
Summary: Web Tools launch issue on Embedded FOS switches	
Symptom: When using web tools to connect to admin domains error message "error loading fabric tree. null" displays	
Probability: Low	
Feature: FOS Software	**Function:** Web Management
Reported In Release: FOS7.0.2	**Service Request ID:** 1206388

Defect ID: DEFECT000472858	**Technical Severity:** High
Summary: A learning flow defined with both generator and monitor as feature options and srcdev "*" specified, monitors only a portion of real flows on the egress port	
Symptom: A learning flow, defined on an egress port with both generator and monitor features specified and also has either srcdev or dstdev option as '*' will monitor less number of flows than actual number of flows going through the egress port. This will only happen when the number of real flows exceeds 32.	
Probability: High	
Feature: Network Patroller	**Function:** Flow monitor
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000472886	**Technical Severity:** High
Summary: FCIP FICON Tape Emulation not going into read pipelining due to synchronizing status bit set in 1st command in chain	
Symptom: Slow FICON tape read performance due to long running restore/recall jobs	
Probability: Medium	
Feature: FOS Software	**Function:** FCIP
Reported In Release: FOS7.0.0	**Service Request ID:** 1219501

Defect ID: DEFECT000473053	**Technical Severity:** High
Summary: Configupload after Configdefault retains old simport configuration in uploaded config	
Symptom: Configupload after Configdefault retains old simport configuration in uploaded config. The flow definitions existing in the system before configdefault, will reappear if the uploaded file is down loaded onto a switch.	
Probability: High	
Feature: Network Patroller	**Function:** Other
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000473063	**Technical Severity:** High
Summary: SIM ports stuck as G-port when changing a logical switch to a base switch	
Symptom: Ports that are configured as SIM ports in a logical switch are get stuck in an invalid state when the logical switch is reconfigured as Base switch	
Workaround: Remove configured SIM ports before converting logical switch to base switch	
Probability: High	
Feature: Network Patroller	**Function:** ASIC interfaces
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000473548	**Technical Severity:** High
Summary: When flows are monitored in MAPS, switch disable/enable or port enable/disable could trigger unexpected MAPS RASLOGs	
Symptom: Unexpected MAPS RASLOGs with large values are triggered for the flows affected by port enable/disable or switch enable/disable operations.	
Probability: High	
Feature: Advanced Monitoring Services	**Function:** Flows
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000473948	**Technical Severity:** High
Summary: Creating MAPS policy failed with generic error message 'failed to create policy'	
Symptom: The MAPS policy create failed returning a generic error 'failed to create policy' with no reason why it failed.	
Probability: Medium	
Feature: Mgmt Embedded - CAL	**Function:** Other
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000474234	**Technical Severity:** Medium
Summary: Multiple aborted FICON sequences after processing emulated attention in zOS third party remote mirror	
Symptom: Third party remote mirror does successfully configure but FICN-1062 and FICN-1063 RASLOG messages and associated XTUN-1999 FTRACE messages and zOS IOS000 errors are recorded in SYSLOG	
Probability: Low	
Feature: FCIP	**Function:** FCIP-RAS
Reported In Release: FOS7.1.0	**Service Request ID:** 1226196

Defect ID: DEFECT000474717	**Technical Severity:** High
Summary: DASD warm start processing causes inoperative CHPIDs through an XRC emulation enabled FCIP Tunnel	
Symptom: IOS001E devAddr,INOPERATIVE PATH on CHPID after DASD controller warm start	
Probability: Medium	
Feature: FCIP	**Function:** Emulation
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000475320	**Technical Severity:** Medium
Summary: Reset doesn't work for flow mirror feature when wrap is disabled	
Symptom: Unable to reset a flow mirror when wrap is disabled.	
Probability: Medium	
Feature: Network Patroller	**Function:** Flow Mirroring
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000475599	**Technical Severity:** Medium
Summary: mapssam --show does not show port type of N_port trunks for FOS switch ports attached to access gateway	
Symptom: mapssam --show does not correctly show port type of N_port trunks	
Probability: Medium	
Feature: Advanced Monitoring Services	**Function:** Other
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000476762	**Technical Severity:** Medium
Summary: Web tools to set the "Permissions" attribute in the JAR Manifest	
Symptom: User will see the unwanted warning messages in java console while launching WT	
Probability: Medium	
Feature: WebMgmt	**Function:** Login / Session Management
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000477049	**Technical Severity:** Medium
Summary: Unable to sort columns in name server section of FOS Web Tools	
Symptom: Data is not sorted when toggling column headers of the name server section in Web Tools	
Probability: Medium	
Feature: WebMgmt	**Function:** Name Server
Reported In Release: FOS7.2.0	

Closed with Code Change in Fabric OS v7.2.0a

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of September 9, 2013 in Fabric OS v7.2.0a

Defect ID: DEFECT000433200	**Technical Severity:** Medium
Summary: Switch cannot be managed from WebTools or BNA though management via CLI works.	
Symptom: Under rare condition management process (HTTPD) gets stuck and switch reports as unreachable via BNA and Webtools. This issue has been reported a few times since FOS v7.0.0 and some releases need disruptive way to recover. This release provides a non-disruptive recovery method.	
Probability: Low	
Feature: FOS Software	**Function:** Management Embedded
Reported In Release: FOS7.0.2	**Service Request ID:** 1116227,1157961,1190

Defect ID: DEFECT000435100	**Technical Severity:** Medium
Summary: SNMPCONFIG is inconsistent on ISCSI settings	
Symptom: Disable ISCSI-mibcapability in FOSv6.3 and then upgraded to FOSv6.4, when the new firmware comes up, ISCSI- MIB is in disabled state and ISCSI-TRAPS are in enabled state.	
Probability: Medium	
Feature: FOS Software	**Function:** SNMP
Reported In Release: FOS6.3.0	**Service Request ID:** 1124455

Defect ID: DEFECT000448581	**Technical Severity:** Medium
Summary: Port Rename, F-Port BB Credit & NPIV Max Login dialogs still persist even after the connection is timed out and allows user to configure the values.	
Symptom: User is erroneously allowed to configure the values even after the connection times out.	
Probability: Medium	
Feature: WebMgmt	**Function:** Ports Admin
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000452801	**Technical Severity:** Medium
Summary: Switch unable to process commands	
Symptom: The Switch becomes unmanageable and will not accept FOS commands, including 'Reboot'. The only way to recover is to power cycle the switch.	
Workaround: Avoid querying invalid class from WT.	
Probability: Low	
Feature: FOS Software	**Function:** Management Embedded
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000460453	**Technical Severity:** Medium
Summary: "Can not find platform: 117" and "client: connect: Connection refused" messages occurred during boot up	
Symptom: Error messages are displayed on embedded platform console during boot up and do not affect any functionality.	
Probability: High	
Feature: Embedded Platform Services	**Function:** FOS Kernel Driver
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000465730	**Technical Severity:** Medium
Summary: Enhancement to asic parity error monitoring threshold	
Symptom: Current default configuration for blade faults is not sensitive enough for some ficon environment setup. Customer may experience IFCCs when there are low level asic parity errors. New CLI options will allow blade to be faulted sooner when there are parity errors. Default threshold is maintained the same as Pre-FOS7.1 releases	
Probability: Low	
Feature: FOS Software	**Function:** ASIC Driver
Reported In Release: FOS7.1.0	

Defect ID: DEFECT000465802	**Technical Severity:** Medium
Summary: Webtools does not allow the configuration of the "Signal Loss" area for ports	
Symptom: Customer is unable to see “signal loss” area stats via Webtools while the same can be seen from CLI	
Probability: Medium	
Feature: FOS Software	**Function:** Web Management
Reported In Release: FOS7.1.1	**Service Request ID:** 1190629

Defect ID: DEFECT000465879	**Technical Severity:** High
Summary: 16Gb SFP rules for TXP and SFP Current are violated when a neighbor EPort transitions online.	
Symptom: Invalid reporting of MAPS 16G SFP rules for optice when its neighbor EPort transitions online.	
Probability: High	
Feature: Advanced Monitoring Services	**Function:** Other
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000466750	**Technical Severity:** Medium
Summary: In Switch Events and Switch information tab, the last updated time shows the Host time instead of showing the Switch time.	
Symptom: Misleading last updated time in Switch Events and Switch Information tab.	
Probability: Low	
Feature: WebMgmt	**Function:** Switch Explorer/Switch View
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000467681	**Technical Severity:** High
Summary: Blade server shows incorrect firmware version in IOM module after a switch hotplug	
Symptom: Blade server displays incorrect Firmware Version in IOM module after switch hotplug	
Probability: High	
Feature: Embedded Platform Services	**Function:** Other
Reported In Release: FOS7.2.0	**Service Request ID:** 1001

Defect ID: DEFECT000467760	**Technical Severity:** Medium
Summary: Disabled port is not getting enabled after binding a port address.	
Symptom: Port is disabled after binding a port address.	
Workaround: Enable the port manually	
Probability: Low	
Feature: WebMgmt	**Function:** Ports Admin
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000468007	**Technical Severity:** High
Summary: Host discovery issues via Ex ports on ICL in multi chassis configuration	
Symptom: Host may not see all target LUNs in a topology using multi-chassis EX ports on ICL configuration	
Workaround: Portdisable enable switch ports for affected devices.	
Probability: Medium	
Feature: FC Services	**Function:** Name Server
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000468188	**Technical Severity:** High
Summary: observed MDD kept crashing when a DS was set persistently disabled	
Symptom: user may see MDD hit rolling crashing when the switch is configure VF mode and the DS switch is set disable persistently with MAPS enabled.	
Probability: Low	
Feature: Advanced Monitoring Services	**Function:** Other
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000468413	**Technical Severity:** High
Summary: firmwaredownload -s on standby CP produces protocol failure in circuit setup messages on the console	
Symptom: Firmware download on the standby CP takes a long time to reach Y/N prompt and several "poll: protocol failure in circuit setup" console messages resulted.	
Workaround: Use firmwaredownload without the -s option.	
Probability: Low	
Feature: Striker/Spike Platform Services	**Function:** VEX
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000468455	**Technical Severity:** High
Summary: QoS allowed ASIC buffer pool to become over allocated	
Symptom: Portbuffershow indicated a negative value in the remaining buffers after QoS was enabled on an extended distance link	
Probability: Medium	
Feature: 8G ASIC Driver	**Function:** ASIC Driver
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000468777	**Technical Severity:** Medium
Summary: portcfgpersistentdisable -r does not persist the reason on reboot of a 7800	
Symptom: port reason does not persist across a reboot on a 7800 switch when portcfgpersistentdisable -r is configured	
Probability: Medium	
Feature: 8G Platform Services	**Function:** Other
Reported In Release: FOS7.2.0	

Defect ID: DEFECT000468795	**Technical Severity:** High
Summary: FCIP FICON XRC Emulation Abort after Selective Reset Errors	
Symptom: If FICON XRC Emulation receives a Selective Reset for a device that is currently in Stacked Status State, the Selective Reset is incorrectly responded to by emulation processing leading to an abort sequence from the channel for the Selective Reset Exchange.	
Probability: Low	
Feature: FCIP	**Function:** Emulation
Reported In Release: FOS7.0.0	**Service Request ID:** 1205859

Defect ID: DEFECT000470123	**Technical Severity:** High
Summary: Switch running agshow panics or BNA seed switch panics when polling for AG info in a fabric with AG switches.	
Symptom: After the port connecting AG to switch bounces, before fabric management server and name server data base are stabilized, polling from BNA caused seed switch to panic, similarly run agshow on switch can cause switch to panic. The timing window for triggering the panic is very small.	
Workaround: avoid agshow CLI and managing switch via BNA.	
Probability: Medium	
Feature: FOS Software	**Function:** Fabric Services
Reported In Release: FOS7.0.0	**Service Request ID:** 1206464

Defect ID: DEFECT000470185	**Technical Severity:** High
Summary: portcfgfillword's passive option does not work	
Symptom: The passive option in portCfgFillWord does not work. When issuing: "portcfgfillword <slot/port> 3 passive". The fillword immediately takes effect on the port, regardless of port speed.	
Probability: Medium	
Feature: 8G ASIC Driver	**Function:** C2 ASIC driver
Reported In Release: FOS7.2.0	**Service Request ID:** ,1190443

Defect ID: DEFECT000470487	**Technical Severity:** Medium
Summary: Fabric watch not calculating VEX port packet loss correctly.	
Symptom: Erroneous FW-1190 error messages seen on different VEX tunnels: Event: , VEXport#3/16,Packet Loss, is above high boundary(High=100, Low=0). Current value is 1176 Percentage(%). Severity: Warning	
Feature: FABRIC WATCH	**Function:** Other
Reported In Release: FOS7.2.0	**Service Request ID:** 1197444

Defect ID: DEFECT000471333	**Technical Severity:** Critical
Summary: Incoming corrupted Flogi frame triggered switch to panic in a Loop.	
Symptom: Switch starts rolling reboot. After it stops, type in any command, it will show: "fabos not yet initialized". Further investigation shows device FLogi has certain Vendor Version Level (VVL) bits set unexpectedly	
Workaround: Keep the port connected to the misbehaving device in disabled state	
Probability: Low	
Feature: FOS Software	**Function:** Fabric Services
Reported In Release: FOS7.0.0	**Service Request ID:** 1213514

Appendix: Additional Considerations for System z (FICON) Environments

As noted at the beginning of the release notes, Brocade recommends all customers planning or using previously FICON qualified FOS version 7.2.0b to upgrade to FOS v7.2.0d.

New Features Support

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

FOS v7.2.0d is FICON qualified release with several new features and enhancements for FICON environment including:

- Monitoring and Alerting Policy Suite (MAPS) is a key component of Brocade Fabric Vision technology providing proactive monitoring and alerting capabilities and is fully supported in FICON environments. A description of MAPS functionality can be found at the beginning of this document.
- Flow Vision is another key component of Brocade Fabric Vision technology and is also supported in FICON environments. The Flow Vision tool suite includes Flow Monitoring, Flow Generator, and Flow Mirror capabilities. A description of Flow Vision functionality can be found at the beginning of this document.
- Added the ability for the CUP Diagnostics to determine the firmware version of all the switches in the fabric which allows interoperability with FOS v7.1.0c.
- A new Command Reject Error Code provides more details to the CUP about failures.

Notes on FICON Support

- Multiple 10 Gb/sec ISLs and FCIP links can load-share between cascaded FICON directors/switches but do not load balance in a FICON configuration.
- 10-bit addressing mode is not supported in a FICON environment.
- Please refer to the *Firmware Upgrades and Downgrades* section of this document when planning an upgrade to a fabric that includes the 7800 or has any FX8-24 blades in a DCX, DCX-4S, DCX8510-8, or DCX8510-4 chassis.

Area	Comments
Cascading	There are special configuration considerations for environments with three or more switches (domain IDs) in a FICON fabric. Assistance from service support should be sought to ensure proper configuration.
Cascading	Fiber ICL configurations (with DCX8510-8/DCX8510-4) supported for FICON are the same as the supported configurations for copper ICLs (with DCX/DCX-4S).
Cascading	Encryption and compression is supported on Fibre Channel ISLs in addition to IP links.
FCIP	VEX ports are not supported on the 7800 and FX8-24 blade in a FICON environment

Area	Comments
FCIP	When performing multiple cabling changes to the SAN fabric in a FICON Emulating FCIP Tunnel configuration with the Brocade 7800 or FX8-24 blade, either disable all of the FCIP Tunnels or issue the switch disable command on all FCIP interconnected switches to avoid IFCCs in a mainframe environment. Issuing either a switch disable or an FCIP Tunnel disable command will allow the FCIP FICON Emulation processing state-machine to execute an orderly cleanup process and allow normal activation of the new configuration. When all cabling and Traffic Isolation Zone manipulations have been completed, enable the switches or the FCIP Tunnels.
FCIP	A disabled XGE or GE port will be re-enabled after a code upgrade/downgrade. To prevent XGE/GE ports from being re-enabled after a code load they should be persistently disabled.
Firmware Downloads	Firmware upgrades for FICON are only supported from FOS v7.1.0c or FOS v7.2.0b[i]. When performing non-disruptive upgrade from v7.2.0b to this version, deactivate or delete flow mirrors before starting firmware upgrade. Presence of Flow mirrors with traffic being mirrored might cause IFCCs.
Firmware Downloads	Non-disruptive Hot Code Load is only supported on director class switches (DCX, DCX-4S, DCX8510-8, and DCX8510-4). Comprehensive non-disruptive Hot Code Load is not supported on the 7800 or a DCX, DCX-4S, DCX8510-8, or DCX8510-4 with an FX8-24 blade since the FCIP tunnels will go down for 10-15 seconds and all traffic in the tunnels will be disrupted. IFCCs may result if traffic is not stopped while downloading firmware.
Firmware Downloads	The CUP device must be varied offline to all MVS partitions before starting a code load. The CUP device can be varied back online after the code load completes. Failure to vary off the CUP devices may result in missing interrupt.
Firmware Downloads	When downgrading v7.2.0d to v7.1.0c, ICL ports might go down with port status In_Sync or Port_Flt when FMS mode is turned on and XISLs are configured. Contact device support to get a special version of FOS v7.1.0c for downgrading from v7.2.0d to v7.1.0c in this scenario.
Interoperability	When connecting an 8G or 16G capable port in a Brocade switch to an IBM Virtualization Engine TS7700 with R1.6 or below, the port must be configured to a minimum of 16 buffers to avoid IFCCs at the channel and loss of FICON paths to the control unit. This requires the Extended Fabric license on the Brocade switch. The recommended best practice is to upgrade the TS7700 to R1.7 or higher and leave the BB credits of the switch port at the default setting of 8. Contact TS7700 device support to determine proper settings of your device.

<table>
<tr><th>Area</th><th>Comments</th></tr>
<tr><td>Manageability</td><td>It is suggested that Port Fencing be used to avoid taking ports down for normal fabric events. The recommended fencing criteria and settings are:<table><tr><th>Criteria</th><th>Value</th></tr><tr><td>ITW (Invalid Transmission Words)</td><td>25 per minute</td></tr><tr><td>CRC (Cyclical Redundancy Check)</td><td>3 per hour</td></tr><tr><td>Protocol Errors</td><td>2 per minute</td></tr><tr><td>State Change</td><td>7 per minute</td></tr><tr><td>Link Reset</td><td>3 per minute</td></tr></table>Note: Port fencing should not be set for C3 discards.

While Port fencing is supported in v7.2.0d, it is recommended that all System z customers enable MAPS after upgrading to FOS v7.2.0d using the default aggressive policy, “dflt_aggressive_policy”.</td></tr>
<tr><td>Manageability</td><td>As a "Best Practice" for deploying FOS switches/directors into a FICON environment, verify the FOS version shipped with the most current FOS recommendation. It is recommended to update all FOS switch/directors to the same FOS levels for production.</td></tr>
<tr><td>Manageability</td><td>FMS must be enabled on the local switch for the remote CUP to work.</td></tr>
<tr><td>Manageability</td><td>The FICON merge wizard feature in Network Advisor cannot be used to merge a 48000 with a DCX, DCX-4S, DCX8510-8, or a DCX8510-4.</td></tr>
<tr><td>Manageability</td><td>When setting insistent domain ID on a switch using the FICON Configuration Wizard, the switch will always be taken offline and insistent domain ID set, even if insistent domain ID is already set.</td></tr>
<tr><td>Optics</td><td>When configuring inter-switch links (ISLs) between a 16G platform and an 8G platform, the ISL ports must be configured for E-Port only.</td></tr>
<tr><td>Serviceability</td><td>zDAC may not give reliable results. The SIOCA tool run from HMC on System z performs a similar function and therefore may not give reliable results as well.</td></tr>
<tr><td>Traffic Isolation Zones</td><td>Under certain circumstances, enabling multiple Traffic Isolation Zones with failover disabled may cause some frames to be dropped due to the timing of when paths are re-routed while the zones are being implemented. To avoid this, all Traffic Isolation Zones should be enabled with failover enabled first so that all desired routes are established.</td></tr>
<tr><td>Traffic Isolation Zones</td><td>Assistance from service support should be sought before attempting to configure and enable this feature.</td></tr>
<tr><td>Virtual Fabrics</td><td>Assistance from service support should be sought before attempting to enable Virtual Fabrics or use the XISL (Base Switch ISL) capability.</td></tr>
<tr><td>Virtual Fabrics</td><td>If a port gets assigned a port address of 0xFE in an Open System logical switch, an RSCN will be sent by FOS on behalf of port address 0xFE during CP failover or firmware download. This may result in an IFCC for any FCP channel running traffic to port address 0xFE.</td></tr>
</table>

Maximum CUP Support

This table indicates the maximum supported number of logical switches that can have FMS (CUP) enabled on the specified platform.

Platform	Maximum Number of CUP Instances
8510-8	4
8510-4	4
6510	2 (no base switch)
DCX	4
DCX-4S	4
5300	4
7800	2 (no base switch)

Interoperability

When cascaded to other switches, referred to as a "fabric," all switches in the fabric must be at FOS v7.1.0c or FOS v7.2.0b[i] before upgrading to v7.2.0d. Interoperability between switches at FOS v6.4.2a, FOS v7.0.0c, FOS v7.0.0d, FOS v7.1.0c, FOS v7.2.0b[i] and FOS v7.2.0d is supported; however, the recommended best practice is to have all switches in the same fabric at the same code level.

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

FICON Hardware/Firmware/Software Interoperability with FOS v7.2.0d

Interoperability is supported with FOS v7.2.0d between the following platforms:

- DCX
- DCX-4S
- DCX8510-8
- DCX8510-4
- 6510
- 5300
- 7800

All platforms operating with FOS v7.2.0d must be managed with Brocade Network Advisor v12.1.3 or later. FICON support for FOS v7.2.0d starts with Brocade Network Advisor v12.1.3 – please check Brocade Network Advisor release notes for latest updates.

The following platforms using FOS v6.4.2a, FOS v7.0.0c, FOS v7.0.0d, FOS v7.1.0c or FOS v7.2.0b[i] may also interoperate in a fabric with switches running FOS v7.2.0d:

- DCX
- DCX-4S

- 5300
- 5100
- 7800
- 48000

Platforms operating with FOS v7.1.0c can be managed with Brocade Network Advisor v12.1.3.

The following platforms are NOT supported for interoperability in fabrics with switches using FOS v7.x:

- M6140
- Mi10K
- 7500/7500

[i] Brocade recommends all customers planning or using FICON qualified FOS version 7.2.0b to upgrade to FOS v7.2.0d. Non disruptive firmware upgrade to v7.2.0d for FICON is also supported from FOS v7.1.0c and it is not required to go to FOS v7.2.0b as intermediate step.