BROCADE

Brocade Fabric OS v6.2.0g
Release Notes v3.0

July 28, 2009

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v6.2.0g Release Notes v1.0	Initial release	May 14, 2009
Brocade Fabric OS v6.2.0g Release Notes v2.0	Second release - Update Important Notes with QOS information and added new appendix for FICON support information	July 6, 2009
Brocade Fabric OS v6.2.0g Release Notes v3.0	Third release - Updated Important Notes with clarified QOS information	July 28, 2009

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

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

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

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

Contents

Document History 1

Quick Look **5**

Overview **5**

New Feature Descriptions **6**

Virtual Fabrics 6

FCR and FCIP Enhancements 6

Enhanced Native Connectivity with McDATA Products 7

Security Enhancements 7

Encryption Enhancements 7

Optionally Licensed Software **8**

Temporary License Support 9

Previously Licensed Software Now Part of Base FOS 9

Supported Switches **10**

Standards Compliance **10**

Technical Support **10**

Important Notes **11**

DCFM Compatibility 11

EFCM Compatibility 12

Fabric OS Compatibility 12

Firmware Upgrades and Downgrades 18

SAS Version Requirements for FA4-18 and Brocade 7600: 19

Scalability 19

FICON Support 19

Other Important Notes and Recommendations 19

Documentation Updates **28**

Brocade Fabric OS Administrator's Guide (Publication Number 53-1001185-01) 28

Brocade Fabric OS Command Reference (Publication Number 53-1001186-01) 33

Fabric OS Troubleshooting and Diagnostics Guide (Publication Number 53-1001187-01) 34

Brocade Fabric Watch Administrator's Guide (Publication Number 53-1001188-01) 35

Fabric OS MIB Reference (Publication Number 53-1001156-01) 36

Access Gateway Administrator's Guide (Publication Number 53-1001189-01) 36

Brocade Encryption Administrator's Guide (Publication Number 53-1001201-02) 36

Generating and exporting the master key 37

Brocade DCX Backbone Hardware Reference Manual (Publication Numbers 53-1000685-01 through -05) 37

Brocade DCX-4S Hardware Reference Manual (Publication Number 53-1001191-01) 39

Brocade 5100 Hardware Reference Manual (Publication Number 53-1000854-02) 39

Brocade 7500 Extension Switches Hardware Reference Manual (Publication Number 53-1000026-04) 39

Brocade 48000 Hardware Reference Manual (Publication Number 53-0000645-05) 40

Brocade SilkWorm 200E Hardware Reference Manual (Publication Number 53-0000633-03) 40

Brocade SilkWorm Multiprotocol Router Model AP7420 Hardware Reference Manual (Publication Number 53-1000179-01) 41

Brocade Mi10K Director Installation and Service Manual (Publication Number 53-1000711-01) 42

Brocade Fabric OS Message Reference (Publication Number 53-1001157-01) 42

Defects 43

Closed with Code Change Defects in Fabric OS v6.2.0g 43

Closed with Code Change Defects in Fabric OS v6.2.0f 46

Closed with Code Change Defects in Fabric OS v6.2.0e 47

Closed with Code Change Defects in Fabric OS v6.2.0d 50

Closed with Code Change Defects in Fabric OS v6.2.0c 56

Closed with Code Change Defects in Fabric OS v6.2.0b 60

Closed with Code Change Defects in Fabric OS v6.2.0a 62

Appendix: Additional Considerations for FICON Environments... 65

Quick Look

If you are already using the most recent version of the Fabric OS v6.2.0f Release Notes, here are the changes between that version and this version.

The table at the end of these notes contains a list of the defects closed since the release of the Fabric OS v6.2.0f release notes.

Additional information for FICON environments is included in the *Additional Considerations for FICON Environments* appendix.

Overview

Brocade Fabric OS v6.2.0 supports the following new hardware platforms:

- **Brocade DCX-4S: 192 port backbone**
  - 192 ports, 8 Gbit/sec technology in a 8Uchassis with horizontal slots
  - Supports FC8-16, FC8-32 and FC8-48 Fibre Channel port blades.
  - Supports all special purpose blades available for DCX
  - Supports ICL connectivity to other DCX-4S or DCX chassis

In addition to support for the new hardware platforms and blades, there are numerous new features in Fabric OS v6.2.0, including:

- **Virtual Fabrics**
  - Full VF feature support on DCX, DCX-4S, 5300, 5100
  - Single physical chassis can be subdivided into two or more logical switches creating a logical fabric with other switches
  - Per-port assignment of ports to logical switches
  - Shared ISLs provide connectivity for multiple logical fabrics
- **FCR and FCIP Enhancements**
  - FCIP (SCSI) Read Tape Pipelining
  - Enhancements to SoTCP
  - LSAN Tagging
  - Support Pathinfo over MetaSAN
  - Use FSPF cost in FCR backbone fabric to find shortest path to edge fabric
  - In-band management link over FCIP connections for the Brocade 7500
  - TCP Byte Streaming for FCIP connections used with WAN optimization hardware
  - Improved FCIP statistics support including TCP connection history, high water mark information and connection snapshot capability
- **Support temporary licenses** for Adaptive Networking, Integrated Routing, and Fabric Watch
- **Security Enhancements**
  - IPv6 Auto-configuration
  - IPSec with IPv6 (for management port)
  - Configurable switch-wide policy requiring authentication of all HBAs
  - RADIUS enhancements allowing password expiration and source IP address information
  - LDAP enhancement allowing for alternate domain UPN
  - IPv6 certified for JITC Approved Product List
- **FICON Enhancements**

    - RNID support for CUP
    - New FC addressing modes for support with Virtual Fabrics
    - Support for FC8-48 blade with VF-enabled DCX/DCX-4S for FICON environments
- **Access Gateway Enhancements**
    - AG mode supported on Brocade 5100
- **Encryption Enhancements**
    - Data Encryption support in Virtual Fabrics environments
    - Support for Tape encryption and compression.
    - Key Management support for HP's SKM
    - Support for up to four FS8-18 Encryption blades in a single DCX or DCX-4S chassis
- **Brocade HBA feature support**
    - Beacon adjacent switch port from HCM
    - Fabric based boot LUN discovery
    - QoS nameserver support allowing query for QoS zone information
    - Support for FC Ping
- **Miscellaneous**
    - FC ping support between switches (ping switch WWN)
    - Provide path information via CLI
    - Frame Redirection support in interopmode 3 (McDATA Open Fabric Mode)
    - Support for M-EOSn's 239 Domain ID mode via FCR in interopmode 3
    - System-wide RASLOG
    - Port Auto-Disable support
    - Ethernet Port Bonding for management ports
    - New CLI command to configure F_Port receive buffer credits

New Feature Descriptions

Virtual Fabrics

- Virtual Fabrics (VF) is a new capability supported on the Brocade DCX, DCX-4S, 5300, and 5100 switches. Once enabled, VF allows the user to divide a single physical chassis or switch into multiple "logical switches" by assigning individual ports to a logical switch. Each of these logical switches is managed as a completely independent layer 2 Fibre Channel switch, and can be deployed in independent fabrics known as "logical fabrics."
- VF also allows the user to create a special logical switch known as the "base switch," used for connectivity to other base switches and also as a backbone fabric for Fibre Channel Routing. Individual logical fabrics may utilize this shared base fabric for connectivity to other switches, providing efficient use of resources by sharing common ISL and ICL connections among multiple logical fabrics.
- The Virtual Fabrics feature is part of the base Fabric OS and does not require a license. Virtual Fabrics is fully compatible with legacy Brocade products as well as M-series switches and directors.

FCR and FCIP Enhancements

- **FCIP (SCSI) Read Tape Pipelining** – Anticipates host read operations and buffers data to reduce latency from the FCIP WAN.

- **LSAN Tagging** – Provides special behavior for designated LSAN zones using either a new “speed” tag or “enforce” tag. The enforce tag allows individual FCRs to be configured to only import devices in specific LSAN zones, increasing scalability. The speed tag allows designated targets to remain imported, allowing sensitive hosts to discover targets much faster. This is useful when performing boot over LSAN operations.
- **SoTCP Enhancements** – Improved network congestion management in Slow Start Mode helps to prevent host I/O from timing out.
- **Support Pathinfo over MetaSAN** – Pathinfo command has been enhanced to provide path information across routed fabrics, especially useful when troubleshooting connectivity problems across routed fabrics.
- **Use FSPF cost in FCR backbone fabric** – Uses most efficient route to reach a destination fabric, preventing the use of an FCIP link when an ISL is available.
- **In-band management link over FCIP connections for the Brocade 7500** – Allows a management station to communicate with a remote 7500 through the GE ports. This allows a single management station located on the WAN side of the 7500 to communicate with the management interface on the CP for management tasks such as firmwaredownloads, snmp polling, snmp traps, trouble shooting, and configuration.

Enhanced Native Connectivity with McDATA Products

- **Frame Redirection --** Fabric OS v6.2.0 and M-EOS v9.9 now support Frame Redirection in McDATA Open Fabric Mode (interopmode 3) fabrics. Frame Redirection zones must be created and activated from FOS platforms.
- **FCR Support for M-EOSn 239 DID mode** – FOS platforms now support EX_Port connections to McDATA Open Fabric Mode Mi10ks using the 239 DID setting.

Security Enhancements

- **IPv6 Auto-configuration –** Configurable stateless IPv6 auto-configuration support.
- **IPSec with IPv6** – Supports greater security for management ports by providing configurable security policies for IPv4/6 addresses.
- **Switch-wide policy requiring HBA authentication** – New configurable switch-wide setting requires the FC-SP bit to be set in FLOGI. If bit is not set, the FLOGI is rejected and the port will be disabled.
- **RADIUS Enhancements** – New warning for RADIUS login allows users to configure how many days in advance they should be notified of password expiration.
- **LDAP Enhancements** – Added ability to provide an alternate UPN (userPrincipalName) to domain authentication.

Encryption Enhancements

- **Tape Encryption and Compression –** Backup applications supported for tape encryption with the 6.2 release include:
  - Veritas NetBackup 6.5
  - EMC Networker 7.4
  - HP Data Protector 6.0

Please contact your vendor regarding the use of other backup applications.

Optionally Licensed Software

Optionally licensed features in Fabric OS v6.2.0 include:

- Brocade Ports on Demand — Allows customers to instantly scale the fabric by provisioning additional ports via license key upgrade (applies to select models of switches).
- Brocade Extended Fabrics — Provides greater than 10km of switched fabric connectivity at full bandwidth over long distances (depending on platform this can be up to 3000km).
- Brocade ISL Trunking — Provides the ability to aggregate multiple physical links into one logical link for enhanced network performance and fault tolerance. Also includes Access Gateway ISL Trunking on those products that support Access Gateway deployment.
- Brocade Advanced Performance Monitoring — Enables performance monitoring of networked storage resources. This license includes the TopTalkers feature.
- High Performance Extension over FCIP/FC (formerly known as "FC-IP Services") (For the FR4-18i blade and Brocade 7500) — This license key also includes the FC-Fastwrite feature and IPsec capabilities.
- Brocade Accelerator for FICON – This license enables unique FICON emulation support for IBM's Global Mirror (formerly XRC) application (including Hitachi Data Systems HXRC and EMC's XRC) as well as Tape Pipelining for all FICON tape and virtual tape systems to significantly improve XRC and tape backup/recovery performance over virtually unlimited distance for 7500, upgraded 7500E and FR4-18i.
- Brocade Fabric Watch — Monitors mission-critical switch operations. Fabric Watch now includes new Port Fencing capabilities.
- FICON Management Server — Also known as "CUP" (Control Unit Port), enables host-control of switches in Mainframe environments.
- ICLs, or Inter Chassis Links — Provide dedicated high-bandwidth links between two Brocade DCX or DCX-4S chassis, without consuming valuable front-end 8G ports. Each DCX/DCX-4S must have the ICL license installed in order to enable the ICL connections. (Available on the DCX/DCX-4S only)
- Enhanced Group Management — This license, available only on the DCX, DCX-4S and other 8G platforms, enables full management of the device in a datacenter fabric with deeper element management functionality and greater management task aggregation throughout the environment. This license is used in conjunction with Brocade's Data Center Fabric Manager (DCFM) application software.
- Adaptive Networking — Adaptive Networking provides a rich framework of capability allowing a user to ensure high priority connections obtain the network resources necessary for optimum performance, even in congested environments. The QoS SID/DID Prioritization and Ingress Rate Limiting features are the first components of this license, and are fully available on all 8G platforms.
- Integrated Routing — This license allows ports in a DCX, DCX-4S, 5300, 5100, or Brocade Encryption Switch to be configured as EX_ports supporting Fibre Channel Routing. This eliminates the need to add an FR4-18i blade or use the 7500 for FCR purposes, and also provides

double the bandwidth for each FCR connection (when connected to another 8G-capable port).

- 7500E Upgrade (For the Brocade 7500E only) — This license allows customers to upgrade a 4-port (2 FC ports and 2 GE ports) 7500E base to a full 18-port (16 FC ports and 2 GE ports) 7500 configuration and feature capability. The upgraded 7500E includes the complete High Performance Extension license feature set.
- Encryption Performance Upgrade — This license provides additional encryption processing power. For the Brocade Encryption Switch or a DCX/DCX-4S, the Encryption Performance License can be installed to enable full encryption processing power on the BES or on all FS8-18 blades installed in the DCX/DCX-4S chassis.
- DataFort Compatibility — This license is required on the Brocade Encryption Switch/DCX/DCX-4S with FS8-18 blade(s) to read & decrypt NetApp DataFort-encrypted Disk LUNs. DataFort Compatibility License is also required on the Brocade Encryption Switch or DCX/DCX-4S Backbone with FS8-18 Encryption Blade(s) installed to write & encrypt the Disk LUNs in NetApp DataFort Mode (Metadata & Encryption Algorithm) so that DataFort can read & decrypt these disk LUNs. DataFort Mode tape encryption and compression is supported beginning with the FOS v6.2.0 release. Availability of the DataFort Compatibility license is limited; contact your vendor for details.
- Server Application Optimization — This new license introduced with FOS v6.2, when deployed with Brocade Server Adapters, 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.

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

Temporary License Support

The following licenses are available for 45-day temporary use, with a maximum of two temporary license per feature and per switch (90 days maximum):

- Fabric (E_port) license
- Extended Fabric license
- Trunking license
- High Performance Extension license
- Advanced Performance Monitoring license
- Adaptive Networking license (support is new in FOS v6.2)
- Fabric Watch license (support is new in FOS v6.2)
- Integrated Routing license (support is new in FOS v6.2)

Previously Licensed Software Now Part of Base FOS

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

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

Supported Switches

Fabric OS v6.2.0 supports the Brocade 200E, 300, 4012/4016/4018/4020/4024/4424/5410/5480/5424, 4100, 4900, 5000, 5100, 5300, 7500, 7600, 48000, Brocade Encryption Switch (BES) and DCX/DCX-4S. All supported products are qualified for Native Connectivity in interopmodes 2 and 3 for deployment in M-EOS fabrics with the exception of the Brocade 4100.

Access Gateway is also supported by Fabric OS v6.2.0, and is supported on the following switches: the Brocade 200E, 300, 5100, 4012, 4016, 4018, 4020, 4024, 4424, 5480 and 5424.

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

Technical Support

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

1. **General Information**
   - Technical Support contract number, if applicable
   - Switch model
   - Switch operating system version
   - Error numbers and messages received
   - **supportSave** command output
   - Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions
   - Description of any troubleshooting steps already performed and the results
   - Serial console and Telnet session logs
   - Syslog message logs
2. **Switch Serial Number**

   The switch serial number is provided on the serial number label, as shown here.

   FT00X0054E9

   The serial number label is located as follows:
   - Brocade 200E—On the nonport side of the chassis
   - Brocade 4100, 4900, and 7500/7500E—On the switch ID pull-out tab located inside the chassis on the port side on the left

- Brocade Encryption Switch, 300, 5000, 5100, and 5300—On the switch ID pull-out tab located on the bottom of the port side of the switch
- Brocade 7600—On the bottom of the chassis
- Brocade 48000 —Inside the chassis next to the power supply bays
- Brocade DCX—Bottom right of the port side
- Brocade DCX-4S—Back, upper left under the power supply

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

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

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

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

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

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

Important Notes

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

DCFM Compatibility

FOS v6.2.0 is fully compatible with Brocade's Data Center Fabric Manager (DCFM) v10.1.x management software. DCFM is a comprehensive SAN management application that enables end-to-end management of Brocade Data Center Fabrics. It is the next-generation product and the successor to existing Brocade management products, including Brocade Fabric Manager (FM) and Brocade Enterprise Fabric Connectivity Manager (EFCM).

DCFM is available in two versions: *DCFM Professional*, an application bundled with Brocade switches that is ideally suited for small and medium size businesses that need a light-weight management product to manage their smaller fabrics (one physical fabric at a time, up to 1,000 ports); and *DCFM Enterprise*, that is designed for enterprise-class customers and showcases unparalleled performance and scalability (24 physical fabrics, up to 9,000 switch ports). DCFM Enterprise configures and manages Brocade DCX Backbones, along with Brocade directors, routers, switches, and HBAs. It also supports Brocade fabric-based encryption capabilities for data-at-rest. Existing EFCM v9.6 and higher and FM v5.4 and higher customers are provided an easy migration path to DCFM Enterprise.

EFCM Compatibility

EFCM v9.7.4 is the minimum version of Brocade management software that should be used to manage Brocade switches deployed with FOS v6.2. EFCM v9.7.4 cannot manage the DCX-4S or platforms with the Virtual Fabrics feature enabled. For more information on migrating from previous versions of EFCM to EFCM v9.7.4, refer to the EFCM v9.7.4 Release Notes documentation.

Fabric OS Compatibility

The following table lists the earliest versions of Brocade software supported in this release, that is, the *earliest* supported software versions that interoperate. Brocade recommends using the *latest* software versions to get the greatest benefit from the SAN.

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

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

- 2Gb/4Gb platforms must operate with FOS v5.3.1b or later
- 4Gb/8Gb platforms must operate with FOS v6.1.0e, v6.1.1 or later (4Gb platforms may use v5.3.1b but are recommended to use the v6.x versions)
- M-EOS platforms must operate with M-EOS v9.8.0 or later for McDATA Fabric Mode (interopmode 2) or M-EOS 9.9.0 or later for Open Fabric Mode environments (interopmode 3)

For a list of the effective end-of-life dates for all versions of Fabric OS, visit the following Brocade Web site:

http://www.brocade.com/support/end_of_life.jsp

Supported Products and FOS Interoperability	
Brocade 2000-series switches	Not supported, end of support (December 2007)
Brocade 3000, 3200, 3800	v3.2.1c [1][6][9]
Silkworm 3014, 3016, 3250, 3850 and Brocade 3900, 4100, 4900, 24000, 7500, 7500E, 7600, 5000, 200E, 48000	v5.3.1b (2G and 4G platforms) and v6.1.0e and later [5] (4G platforms only)
Silkworm 12000	v5.0.x [6][9]
Brocade 4012, 4016, 4018, 4020, 4024, 4424	v5.3.1b, v6.1.0e and later [5]

Brocade 5410, 5480, 5424	v6.2.0
Brocade DCX, 300, 5100, 5300	v6.1.0e and later [5]
Brocade DCX-4S	v6.2.0
Brocade DCX with FS8-18 blade(s), Brocade Encryption Switch	v6.1.1_enc
Secure Fabric OS (on any model)	Not Supported
Mi10k, M6140, ED-6064, ES-3232, ES-4300, ES-4400, ES-4500, ES-4700 (McDATA Fabric Mode and Open Fabric Mode) [2] [4]	M-EOS v9.7.2 or later [3]
McDATA ED-5000 32-port FC director	Not Supported
Multi-Protocol Router interop	
Brocade 7420	XPath v7.4.1 [8]
Brocade 7500 and FR4-18i blade	v5.1.0 and higher [8]
McDATA SANRouters 1620 and 2640	M-EOSi v5.1.2 or v5.3.0 [7] [8] [10]

Table Notes:

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

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

[3] It is highly recommended that M-EOS products operate with the most recent version of M-EOS released and supported for interoperability. M-EOS 9.7.2 is the minimum version of firmware that is fully qualified to interoperate with FOS 6.2 or later. For support of frame redirection in McDATA Fabric Mode (interopmode 2), M-series products must use M-EOS v9.8 or later. For support of frame redirection in McDATA Open Fabric Mode (interopmode 3), M-series products must use M-EOS v9.9 or later. Only the ES-4400, ES-4700, M6140, and Mi10k may have devices directly attached that are having data encrypted or unencrypted.

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

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

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

[7] For Multi-Protocol router interop, FOS-based switches deployed in M-EOS fabrics should not be directly connected (via ISLs) to the M1620 / M2640 products, but rather attached to other M-EOSc/n switches and directors (M6140s, 4700s, Mi10ks, etc) running in McDATA Fabric Mode/Interopmode 2. McDATA Open Fabric Mode /Interopmode 3 is supported only with M-EOSi v5.3.

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

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

[10] M-series SANRouters (1620/2640) may not participate in a fabric that has encryption services from a Brocade Encryption Switch or FS8-18 Encryption blade.

Fabric OS v6.2.0 software is fully qualified and supports the blades for the 48000 platform noted in the following table:

48000 Blade Support Matrix	
Port blade 16, 32 and 48-port 4Gbit blades (FC4-16, FC4-32, FC4-48), 16, 32 and 48-port 8Gbit blade (FC8-16, FC8-32, FC8-48), and the 6-port 10G FC blade (FC10-6)	Supported with any mix and up to 8 of each. No restrictions around intermix. The 48000 must run Fabric OS v6.0 or later to support the FC8-16 port blade and Fabric OS v6.1 or later to support the FC8-32 and FC8-48 port blades.
Intelligent blade	Up to a total of 4 Intelligent blades (includes iSCSI, FCIP/FCR and Application blade), FC4-16IP, FR4-18i, and FA4-18 respectively. See below for intermix limitations, exceptions, and a max of each blade.
iSCSI blade (FC4-16IP)	Up to a maximum of 4 blades of this type
FC-IP/FC Router blade (FR4-18i)	Up to a maximum of 2 blades of this type. This can be extended under special circumstances but must be approved by Brocade's Product Team. Up to 8 FR4-18i blades can be installed if they are used only for FC Fastwrite or FCIP without routing.
Virtualization/Application Blade (FA4-18)	Up to a maximum of 2 blades of this type.

Fabric OS v6.2.0 software is fully qualified and supports the blades for the DCX/DCX-4S noted in the following table:

DCX/DCX-4S Blade Support Matrix	
16-, 32- and 48-port 8Gbit port blades (FC8-16, FC8-32, FC8-48) and the 6-port 10G FC blade (FC10-6)	Supported with FOS v6.0 and above with any mix and up to 8/4 of each. No restrictions around intermix.
Intelligent blade	Up to a total of 8/4 intelligent blades. See below for maximum supported limits of each blade.

FC-IP/FC Router blade (FR4-18i)	Up to a maximum of 4 blades of this type. This can be extended under special circumstances, but must be approved by Brocade’s Product Team. Up to 8 FR4-18i blades can be installed in a DCX if they are used only for FC Fastwrite or FCIP without routing.
Virtualization/Application Blade (FA4-18)	Up to a maximum of 4 blades of this type.
Encryption Blade (FS8-18)	Up to a maximum of 4 blades of this type.

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

Power Supply Requirements for Blades in 48k and DCX/DCX-4S Chassis

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

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

Secure Fabric OS

Secure Fabric OS (SFOS) is not compatible with FOS v6.2. Customers that wish to use the security features available in SFOS should upgrade to FOS v5.3 or later version, which includes all SFOS features as part of the base FOS. For environments with SFOS installed on switches that cannot be upgraded to FOS v5.3 or later version, FC routing can be used to interoperate with FOS v6.2.

FOS Feature Compatibility in Native Connectivity Modes

Some FOS features are not fully supported when operating in the native connectivity modes for deployment with M-EOS based products. All Brocade models that are supported by Fabric OS v6.2.0 support both intermodal 2 and 3 with the exception of the Brocade 4100.

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

FOS Features (supported in interopmode 0)	**FOS v6.2**	
IM = Interopmode	**IM 2**	**IM 3**
L2 FOS Hot Code Load	Yes	Yes
FOS Hot Code Load with FCR	Yes	Yes
Zone Activation Support	Yes	Yes[11]
Traffic Isolation Zones[1]	Yes	No
Frame Redirection (devices attached to FOS)[1]	Yes	Yes[11]
Frame Redirection (devices attached to M-EOS) [1]	Yes	Yes[11]
Frame Redirection over FCR[10]	Yes	Yes[11]
FCR Fabric Binding (route to M-EOS fabric with Fabric binding) [9]	Yes	Yes
L2 Fabric Binding	Yes	No*
DCC policies	No	No
SCC policies	Yes[4]	No*
E/Ex_Port Authentication	Yes	Yes
ISL Trunking (frame-level)	Yes[2]	Yes[2]
Dynamic Path Selection (DPS, exchange based routing)	Yes[3]	Yes[3]
Dynamic Load Sharing (DLS, port based routing)	Yes	Yes
Virtual Channels (VC RDY)	Yes[2]	Yes[2]
FICON Management Server (Cascading)	Yes	No*
FICON MIHPTO	Yes	No*
Full Scalability (to maximum M-EOS fabric limits)	Yes	Yes
Adaptive Networking: QoS	No	No
Adaptive Networking: Ingress Rate Limiting	No*	No*
Advanced Performance Monitoring (APM)	No*	No*
APM: TopTalkers	No*	No*
Admin Domains	No	No
Secure Fabric OS[5]	N/A	N/A

FOS Features (supported in interopmode 0)	**FOS v6.2**	
IM = Interopmode	**IM 2**	**IM 3**
Fabric Watch	Yes	Yes
Ports on Demand (POD)	Yes	Yes
NPIV	Yes	Yes
Timer Server function (NTP)	No	No
Open E_Port[6]	N/A	N/A
Broadcast Zoning	No	No
FDMI	No	No
Remote Switch	No	No
Port Mirroring	Yes	Yes
Extended Fabrics	Yes	Yes[7]
Alias Server	No	No
Platform Service	No	No
FCIP (VE_Ports)	Yes	Yes
IPFC (IP over FC)	Yes[8]	Yes[8]
M-EOS ALPA 0x13 configuration	Yes	Yes
VE to VEX Port	Yes	Yes
Integrated Routing[9]	Yes[9]	Yes
Domain Offset Support	No	No
239 Domain Support (available on Mi10k only)	N/A	Yes[12]
Masterless F_PORT Trunking (AG connect to FOS switches only)	Yes	Yes
FC10-6-to-FC10-6 ISL	Yes	Yes
RASLOG Events on duplicate WWNs	Yes	Yes
Virtual Fabrics	Yes	Yes
Logical Fabric using LISLs (XISLs in Base Fabric)	No	No

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

1. Requires M-EOS 9.7 or later for redirection between devices attached to FOS switches, M-EOS 9.8 for redirection between devices attached to M-EOS switches, M-EOS 9.9 for use in McDATA Open Fabric Mode. Supported M-EOS platforms include M4400, M4700, M6140, and Mi10k.
2. Only allowed between FOS-based switches
3. DPS is supported outbound from FOS-based switches. (M-EOS can provide reciprocal load balancing using OpenTrunking).
4. SCC policies only supported in conjunction with L2 Fabric Binding support
5. Not supported in FOS 6.0 or later
6. Mode 3 only qualified with M-EOS switches
7. Not on FCR
8. Only supported locally within the FOS switch
9. All routers (EX_Ports) must reside in a backbone fabric running in interopmode 0 only. Only edge fabrics with devices imported to the backbone fabric or other edge fabrics may be operating in IM2 or IM3.
10. To support Frame Redirection to an edge M-EOS fabric, there must be at least one FOS switch in the edge fabric to configure Frame Redirection Zones.
11. Only Frame Redirection Zones may be configured on FOS platforms and sent to fabrics operating in McDATA Open Fabric Mode (interopmode 3). M-EOS 9.9 is required to support FR Zones in McDATA Open Fabric Mode.
12. Supported via FC Routing only. All routers in the backbone must be running FOS v6.2.

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

Firmware Upgrades and Downgrades

Upgrading to Fabric OS v6.2.0 is only allowed from Fabric OS v6.1.0 or later. This policy to support only one-level migration, which began with FOS v6.0.0, provides more reliable and robust migrations for customers. By having fewer major changes in internal databases, configurations, and subsystems, the system is able to perform the upgrade more efficiently, taking less time and ensuring a truly seamless and non-disruptive process for the fabric. The one-release migration policy also reduces the large number of upgrade/downgrade permutations that must be tested, allowing Brocade to spend more effort ensuring the supported migration paths are thoroughly and completely verified.

All products supported by Fabric OS v6.1.0 or v6.1.1 can be upgraded to Fabric OS v6.2. The following is a list of products that can be upgraded to Fabric OS v6.2:

- 300, 4012/4016/4018/4020/4024/4424/5424/5410/5480, 4100, 4900, 5000, 5100, 5300, 7500, 7600, 200E, 48000, BES and DCX.

The DCX-4S may not be downgraded from FOS v6.2.

All downgrades from FOS v6.2.0 require a restart and are disruptive to traffic. Platforms supporting Virtual Fabrics must have the feature disabled prior to downgrading below v6.2.

To ensure non-disruptive Hot Code Load (HCL), neighbor switches should be operating with FOS v6.2.0 prior to loading FOS v6.2.0 on the following platforms:
4012, 4016, 4018, 4020, 4024, 4100, 200E

When upgrading to FOS v6.2.0 from FOS v6.1.0g or earlier, the CPs do not fully synchronize until both the new active and new standby CPs are running v6.2.0. This is normal behavior and the firmware upgrade is still not disruptive.

FOS does not support concurrent FC Routing (EX_Ports) and TopTalkers features. Upgrading to FOS v6.2.0 requires that one of these features be disabled first.

The Brocade Encryption Switch and DCX with one or more FS8-18 blades may not be downgraded below FOS v6.1.1_enc.

The Brocade Encryption Switch and DCX with one or more FS8-18 blades may not be downgraded below FOS v6.2.0 if HP SKM Key Vault is configured. Doing so will result in loss of encryption services in HP SKM environments.

When Tape Encryption is configured on BES or DCX/DCX-4S with FS8-18 blade, downgrading to v6.1.1_enc will result in loss of Tape Encryption Services.

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.

On the Brocade 300, M5424, 5470 and 5480, do not use –n option for downgrading from FOS v6.2 to prior versions. If –n option is used the firmware versions may get out of synchronization and can cause rolling kernel panics and switch is unrecoverable. The switch will have to be RMAed.

SAS Version Requirements for FA4-18 and Brocade 7600:

SAS v3.3.0 is the supported SAS version for FOS v6.2.0.

- When upgrading from FOS v6.1 to v6.2.0 and SAS 3.2.0 to SAS 3.30, first upgrade FOS v6.1 to v6.2.0 and then upgrade SAS from 3.2.0 to 3.3.0.
- When downgrading from FOS v6.2.0 to v6.1 and SAS 3.3.0 to SAS 3.2.0, first downgrade SAS from 3.3.0 to 3.2.0 and then downgrade FOS from v6.2.0 to v6.1.

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

FICON Support

The DCX-4S is not supported for FICON Cascading in interopmode 2 or 3 for use in mixed fabrics with M-EOS platforms.

Other Important Notes and Recommendations

Virtual Fabrics:

- On Virtual Fabrics capable platforms, the Virtual Fabrics feature must be enabled after upgrading to FOSv6.2.0 in order to utilize the related capabilities including Logical Switches and Logical Fabrics. On units that ship with FOS v6.2.0 or later installed, the Virtual Fabrics feature is enabled by default on capable platforms.
- When creating Logical Fabrics that include switches that are not Virtual Fabrics capable, it is possible to have two Logical Switches with different FIDs in the same fabric. Extra caution should be used to verify the FIDs match for all switches in the same Logical Fabric.
- The aptpolicy can be configured per logical switch. The Admin Guide indicates it is a chassis level setting.
- In order to support non-disruptive Hot Code Load on a Brocade 5100 with VF enabled, the total zoning DB size for the entire chassis should not exceed 1MB.
- A switch with Virtual Fabrics enabled may not use Port Mirroring or participate in a fabric that is using IP Filter or Password Database distribution or Administrative Domains. The Virtual Fabrics feature must be disabled prior to deploying in a fabric using these features.

Licensing Behavior:

- When operating a switch with Fabric OS v6.2, some licenses may display as “Unknown.” This is due to changes in licensing requirements for some features that no longer require a license key that may still be installed on a switch.

Encryption Behavior:

- Brocade encryption devices can be configured for either disk or tape operation. The ability to configure multiple Crypto-Target Containers defining different media types on a single encryption engine (Brocade Encryption Switch or FS8-18 Blade) is not supported. FS8-18 Encryption Blades can be configured to support different media types within a common DCX/DCX-4S chassis.
- When using Brocade Native Mode, in LKM installations, manual rekey is highly recommended. If auto rekey is desired, the key expiry date should be configured only when the LUN is created. Never modify the expiry date after configuring a LUN. If you modify the expiry time, after configuring the LUN the expiration date will not update properly.
- SKM is supported with Multiple Nodes and Dual SKM Key Vaults. Two-way certificate exchange is supported. Please refer to the Encryption Admin Guide for configuration information.
- The Brocade Encryption Switch and FS8-18 blade support registration of only one HPSKM Key Vault for FOS v6.2.0. Multiple HPSKMs Key Vaults can be clustered at the SKM server level. Registering of a second SKM key vault is not blocked. When the registered key vault connection goes down or the registered key vault is down, users are expected to either correct the connection with Key Vault or replace the failed SKM and re-register (deregister failed SKM entry and register the new SKM entry) on the Brocade Encryption Switch or FS8-18 blade. Users are expected to make sure that the replaced (new) SKM key vault is in sync with the rest of the SKM units in Cluster in terms of Keys Database (user manually syncs the Key Database from existing SKM Key Vault in Cluster to new or replacing SKM Key Vault using SKM Admin Guide Provided Key Synchronization methods).
- When the tape key expires in the middle of write operation on the tape, the key is used to append the data on the tape media. When the backup application rewinds the media and starts writing to Block-0 again and if the key is expired then a new key is created and used henceforth. The expired key thereafter is marked as read only and used only for restore of data from previously encrypted tapes.
- For dual LKM configuration on the Brocade Encryption Switch (BES) or a DCX/DCX-4S with FS8-18 blades as the primary and secondary key vaults, these LKM appliances must NOT be clustered (linked).
- The RKM Appliance A1.6, SW v2.2 is supported. The procedure for setting up the RKM Appliance with BES or a DCX/DCX-4S with FS8-18 blades is located in the Encryption Admin Guide.
- 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 for 6.2 release.
- HCL from FOS v6.1.1_enc to v6.2.0 is supported. Cryptographic operations and I/O will be disrupted but other layer 2 traffic will not.
- Relative to the BES and a DCX with FS8-18, all nodes in the Encryption Group must be at the same firmware level of FOS v6.2.0 before starting a rekey or First Time Encryption operation. Make sure that existing rekey or First Time Encryption operations complete

before upgrading any of the encryption products in the Encryption Group. Also, make sure that the upgrade of all nodes in the Encryption Group to FOS v6.2.0 completes before starting a rekey or First Time Encryption operation.

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

Method 1:

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

Method 2:

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

- A new LUN state is being introduced: **"Disabled (Key not in sync)."** This new state indicates re-keying was started on a remote EE but the local EE is not capable of starting re-key because it does not have the KeyID which was used by the remote EE in re-keying (i.e. newest key returned from key vault does not match with the KeyID used by remote EE). User needs to use "cryptocfg --discoverLUN <Container Name>" interface to re-enable the LUN only after the keys are synced between two key vaults properly.
- Both VMware and clustering technologies utilize SCSI reservations to control host IO access to LUNs. When BES/FS8-18 is performing a rekeying operation - first time encryption or otherwise - it accommodates the use of this methodology. In deployments which have multiple physical initiators accessing a target/LUN from an EE, FOS 6.2.0 does not have the ability to failover FTE/rekey operations within the EE.

  Therefore, during FTE/Rekey operations in these environments, only one physical initiator can be allowed to access the target/LUN combination – this for all EEs exposing the LUN.

  If only one initiator has access to a Target/LUN on a particular EE, then no configuration modification is required during FTE/Rekey operations.
- Direct FICON device connectivity is not supported for the Brocade Encryption Switch (BES) or the FS8-18 for front end User Ports. Also, FICON devices as part of Encryption or Clear-Text flows are not supported which means FICON devices cannot be configured as Crypto Target Containers on BES or FS8-18.
- Ensure that all encryption engines in the HA cluster (HAC), Data Encryption Key (DEK) cluster, or encryption group are online before invoking or starting rekey operations on LUN(s).Also ensure that all target paths for a LUN are online before invoking or starting rekey operations on LUN(s).

Frame Redirection

- In v6.2.0 Frame Redirection zoning is not allowed with Default Zoning (“all access” in IM0 and default zone in IM2). This was allowed in prior releases. There is no SW enforcement to block the upgrade.

Adaptive Networking/Flow-Based QoS Prioritization:

- When using QoS in a fabric with 4G ports or switches, FOS v6.0 or later must be installed on all products in order to pass QoS info. E_Ports from the DCX to other switches must come up AFTER 6.0 is running on those switches.
- Flow based QoS is NOT supported on FC8 blades in the Brocade 48000.
- Any products that are not capable of operating with FOS 6.0 may NOT exist in a fabric with Flow based QoS. Major problems will occur if previous generation 2G products exist in the fabric.
- For the Brocade 4100 and 5000, if all of the ports are E_Ports and the switch is upgraded to Fabric OS v6.2.0, the buffers on the E_Ports are changed to utilize the QoS model. If the switch is rebooted, 28 of 32 ports will come up in QoS mode; the last four ports will come up in buffer-limited mode. Workarounds include disabling long distance configuration for these ports or explicitly disabling QoS on other ports, freeing up buffers for the last four ports.
- The fix for the defect 250438 included in this release changes the default behavior of the Adaptive Networking QoS feature as follows upon firmware upgrade:
  - The default QoS behavior is changed to be “disabled” on 4G platforms.
  - The default QoS behavior is changed to be “disabled” on the “Extended Fabrics E-ports” on both 4G and 8G platforms.

  This fix solves the following unexpected behaviors that occurred when Adaptive Networking QoS feature was enabled by default in the previous FOS releases:

  - Splitting of a single trunk group into multiple trunk groups upon port toggle, since the toggled ports come online with QoS enabled while the remaining ports in the trunk group have QoS disabled.
  - Fewer buffer credits being made available to normal E-ports after a port toggle even when QoS is not being utilized.
  - Unexpected change to fill word configuration on an Extended Fabrics E-port after a port toggle.
    - If an Extended Fabrics E-port is originally using IDLE primitives as fill words, and if that port toggles, the fill word configuration will be changed to use ARB primitives.

  Note:

  After upgrading to this firmware release, if users want to enable Adaptive Networking QoS feature on 4G platforms, and on Extended Fabrics E-ports on both 4G and 8G platforms, they must do so explicitly through the available user interfaces.

FCR

- All FCR switches need to be running FOS v6.2.0 in order to support M-EOS 239 Domain Mode on the i10K

FCR Backbone Fabric ID changes:

- With FC8 blades, the switch must be disabled to change the backbone fabric ID
- With routing and dual backbone fabrics, the backbone fabric ID must be changed to keep the IDs unique.

Traffic Isolation over FCR

- All switches and Fibre Channel Routers both in edge and backbone fabrics must be running FOS v6.1.0 or later in order to support this feature.
- In order for Traffic Isolation over FCR to function properly, the associated TI zones in each fabric (edge and backbone) need to have failover ENABLED.

Integrated Routing

- To allow Hot Code Load on a Brocade 5100 when using Integrated Routing, the edge switch connected to the 5100 must be running Fabric OS v6.1 or later code.
- Integrated Routing EX_Ports are only supported in the base switch on a switch with VF enabled.
- Integrated Routing and TopTalkers are not concurrently supported in FOS v6.2. To use Integrated Routing, be sure to first disable TopTalkers prior to configuring EX_Ports.

Access Gateway

- When in Access Gateway mode, the Automatic Port Configuration policy may not work when attached to M-EOS switches. M-EOS ports should be set to G_port to prevent problems with port type discovery.

FCS Automatic Distribution

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

FIPS

- FIPS mode should not be enabled on the Brocade 200E. If FIPS is enabled, the 200E will not boot.

LDAP

- When using LDAP, downgrades from FOS v6.2.0 to prior releases requires user intervention. Authentication must be set to local and back to LDAP in order to continue using LDAP authentication.

FCAP

- Due to limitations with the certificates, FCAP authentication cannot be supported on user defined logical switches. FCAP will continue to function with existing certificates for non-VF and the default logical switch of VF enabled switches. (Note: authutil is not restricted from other logical switches, at this time, so this can still be enabled on unsupported LS.)
- pkicert(1.06) utility may cause evm errors, so each new switch should be isolated from fabric, in non-vf mode, to install new certificates.

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

FICON

- For the DCX, FICON CUP is not allowed with a 48-port blade in the Default Logical Switch. All ports on a 48 port blade must be assigned to a user-defined Logical Switch to use them in a FICON CUP enabled switch.

FL_Port (Loop) Support

- The FC8-48 blade now supports attachment of loop devices in the DCX and DCX-4S.
- Virtual Fabrics must be enabled on the chassis and loop devices may only be attached to ports on a 48-port blade assigned to a non-Default Logical Switch operating with the default 10-bit addressing mode (they may not be in the default Logical Switch).
- A maximum of 144 ports may be used for connectivity to loop devices in a single Logical Switch within a chassis.
- Loop devices continue to be supported when attached to ports on the FC8-16, FC8-32, FC4-16 and FC4-32 blades with no new restrictions.

Port Mirroring

- On the Brocade 5300, the port mirroring feature has a limitation where all port mirror resources must stay within the same ASIC port group. The resources are the configure mirror port, Source Device, and Destination Device or ISL, if the Destination Device is located on another switch. The ASIC port groups are 0-15, 16-31, 32-47, 48-63, and 64-79. The routes will be broken if the port mirror resources are spread across multiple port groups.
- Port Mirroring is not supported on a switch with the Virtual Fabrics feature enabled.

10G Interoperability

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

Port Fencing

- When the port fencing feature is enabled for ITW or CRC errors, the first set of errors detected on an active link that meet the custom high threshold level set by the user (or the default threshold level) is always ignored to account for expected link transition errors. The port is only disabled upon detection of a second set of errors, i.e. the next time the user-set threshold level (or default threshold level) is reached. This prevents a port from being disabled due to normal link transition behaviors.
- When using the Port Fencing feature, you must first run the fwalarmsfilterset command. This command enables the port and allows you to receive Port Fencing messages.
- Port Fencing can be inadvertently disabled from Web Tools. This happens when you do the following:
    1. Open the Fabric Watch configuration window.
    2. Check the "SNMP Trap" checkbox in the "Above" row.

This change in WebTools disables Port Fencing. If this happens, you must re-enable the Port Fencing bit from the command line interface.

Extended Fabrics and R_RDY Flow Control

Beginning with Fabric OS v5.1, Brocade supported the Extended Fabrics feature in conjunction with R_RDY flow control (R_RDY flow control mode can be enabled via portCfgISLMode command). R_RDY flow control mode that uses IDLE primitives does not support Brocade frame-based Trunking for devices such as Time Division Multiplexor (TDM.) In order to overcome this limitation and provide support for frame-based Trunking with Extended Fabrics, Fabric OS v6.2.0 has been enhanced to support interoperability with these distance extension devices.

Fabric OS v6.2.0 allows Extended Fabrics E_ports to operate in VC_RDY mode using either ARB or IDLE primitives as fill words. This allows frame-based Trunking to be supported on Extended Fabrics E-ports even when IDLE primitives are configured for these ports when operating in native VC_RDY mode. Prior to this change, frame-based Trunking was supported only when ARB primitives were used in VC_RDY mode. With Fabric OS v6.2, frame-based Trunking is supported on Extended Fabrics E_ports regardless of whether IDLE or ARB primitives are used when operating in native VC_RDY mode.

Implementation

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

Note:

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

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

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

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

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

8G Link Initialization & Fill Words

Background

The FC-PI Fibre Channel standard has defined the requirements for physical layer, it considers all aspects of transmit, receive and cable-plant performance requirements for optical and electrical links. The FC-PI standard has been modified to support new physical layer variants that operate at higher data rates than those specified in FC-PI-2. The standard enables interoperability of transmitter devices, receiver devices, interconnects, and components among different manufacturers. New variants include support for an 800 MB/s data rate. The previous implementation by Brocade was to use Idle's for link initialization and Idles as fill words. This works for 1Gb/ 2Gb / 4Gb and most 8Gb devices. However, some new 8Gb devices have problems with the use of Idle/Idle sequence at 8Gb. 8Gb switches, HBAs and smaller mid-range 8Gb storage devices have been out for nearly a year and have been using the Idle/Idle sequences without issue. We have found that some new 8Gb devices require the ARB (FF) / ARB (FF) sequence to have successful link initialization. For this Brocade has developed an implementation of ARB (FF) / ARB (FF) for initialization and fill words.

A new command has been created to configure the ARB/ARB implementation.

New Command

portCfgFillWord

Configures the fill word for a single 8G FC port.

Synopsis **portcfgfillword** [*slotnumber/*]*portnumber*, *mode*

Description Use this command to configure the fill word of an 8G FC port. This command is not applicable to non 8G FC port. This command disables and re-enables the port and the port comes online with the new fill word setting. The configuration is stored in nonvolatile memory and is persistent across switch reboots or power cycle.

Notes This configuration can not be set on VE_Ports or VEX_Ports.

Use the **portCfgShow** command to display user-configured fill word settings.

The execution of this command is subject to Admin Domain or Virtual Fabric restrictions that may be in place.

Operands This command has the following operands:

slotnumber For bladed systems only, specifies the slot number of the port to be configured, followed by a slash (/).

portnumber Specifies the number of the port to be configured, relative to its slot for bladed systems. Use **switchShow** for a listing of valid ports.

mode Specifies the fill word for portnumber. This operand is required. Valid values are one of the following:

0 IDLE in Link Init and IDLE as fill word (default).

1 ARB(ff) in Link Init and ARB(ff) as fill word.

Examples To set the fill word of a port to ARBFF-ARBFF:

```
switch:admin> portcfgfillword 2/3, 1
```

See Also **portCfgShow**

Behavior

Default mode	The only mode of operation in FOS 6.1 up to this time had been the Idle implementation. With the introduction of FOS v6.1.2 there will be the introduction of the new command to facilitate a change to the ARB implementation. FOS 6.2 specifically v6.2.0, v6.2.0a & v6.2.0b had defaulted to ARB/ARB for 8Gb devices. With the introduction of v6.2.0c the new command will default to mode 0 (Idle) and provide the user the ability to configure the ARB configuration.

Existing Product	For product in the field this change has no effect on current configurations. The mode is currently 0 and during a firmware upgrade the mode will remain 0 and no devices will be impacted. Should a new device be added to the configuration that requires the ARB sequence those ports can be configured at such time. Loading 6.2.0c will not automatically change the mode. In current configurations the mode will have to be changed manually. This change does not affect 1Gb/2Gb or 4Gb devices. Any of the settings of 0 or 1 have no affect on these devices. It only affects devices that negotiate or are fixed to 8Gb speeds.
Changing the mode on the fly after v6.2.0c has been installed.	The portCfgFillWord command will change the configuration parameter and automatically disable/enable the port for which the command invoked. Subsequent link initializations will use ARB(FF).
Other scenarios	The command has no effect on 1Gb / 2Gb /4Gb devices but the mode is persistent. If in the future, a device attempts to negotiate or is fixed to 8G the configured mode will take effect. The persistent configuration is on a port by port basis (i.e. if an 8Gb device was connected to a 2Gb or 4Gb optic and that optic was replaced with an 8Gb optic, then the current behavior of the mode is activated.)

Updated command message

When executing the lscfg --create command via the following syntax:

```
switch_128:FID128:admin> lscfg --create 1
About to create switch with fid=1. Please wait...
Logical Switch with FID (1) has been successfully created.
```

User should expect to see this revised message:

```
Logical Switch has been created with default configurations.
Please configure the Logical Switch with appropriate switch
and protocol settings before activating the Logical Switch.
```

Documentation Updates

This section provides information on last-minute additions and corrections to the documentation. The most recent Fabric OS v6.2.0 documentation manuals are available on the Brocade Partner Network: *http://partner.brocade.com/*

Brocade Fabric OS Administrator's Guide (Publication Number 53-1001185-01)

On page 9, in Chapter 1, under the heading "Setting the static addresses for the Ethernet network interface," remove the following example from step 3:

Example of setting logical switch (sw0)'s IPv6 address on an enterprise-class platform:

```
ecp:admin> ipaddrset –ipv6 –sw 0 ––add 1080::8:800:200C:417B/64
```

```
IP address is being changed...Done.
```

In chapter 2, "Managing User Accounts" on page 70 under the heading "RADIUS configuration with Admin Domains or Virtual Fabrics" replace the bullets:

- *HomeContext* is the designated home Virtual Fabric for the account. The valid values are between 1 to 128 and chassis context. The first valid HomeContext key-value pair is accepted by the switch, Additional HomeContext key-value pairs are ignored.

- *ContextRoleList* is a comma-separated list of Virtual Fabric ID numbers to which this account is a member. Valid numbers range from 1-128, inclusive. A dash between two numbers specifies a range. Multiple VFlist key-value pairs within the same or across the different Vendor-Type codes are concatenated. Multiple occurrences of the same VF ID number are ignored.

- *HomeLF* is the designated home Virtual Fabric for the account. The valid values are between 1 to 128 and chassis context. The first valid HomeLF key-value pair is accepted by the switch, additional HomeLF key-value pairs are ignored.

- *LFRoleList* is a comma-separated list of Virtual Fabric ID numbers to which this account is a member. Valid numbers range from 1-128, inclusive. A dash between two numbers specifies a range. Multiple Virtual Fabric list key-value pairs within the same or across the different Vendor-Type codes are concatenated. Multiple occurrences of the same Virtual Fabric ID number are ignored.

The paragraph following the bullets should read:

> RADIUS authentication requires that the account have a valid role through the attribute type *Brocade-Auth-Role*. The additional attribute values ADList, HomeAD, HomeLF, and LFRoleList are optional. If they are unspecified, the account can log in with AD0 as its member list and home Admin Domain or VF128 as its member list and home Virtual Fabric. If there is an error in the ADlist, HomeAD, LFRoleList, or HomeLF specification, the account cannot log in until the AD list or Virtual Fabric list is corrected; an error message is displayed.

At the top of page 71, the paragraph should read as follows:

> In the next example, on a Linux FreeRadius Server, the user takes the "zoneAdmin" role, with VFlist 2, 4, 5, 6, 7, 8, 10, 11, 12, 13, 15 17, 19, 22, 23, 24, 25, 29, 31 and HomeLF 1.

```
user300 Auth-Type := Local, User-Password == "password"
Brocade-Auth-Role = "zoneadmin",
Brocade-AVPairs1 = "HomeLF=1;LFRoleList=securityadmin:2,4-8,10"
Brocade-AVPairs2 = "LFRoleList=admin:11-13, 15, 17, 19;user:22-25,29,31"\
```

On page 77, "LDAP configuration and Microsoft Active Directory" the following bullets should be added:

- You can use the User-Principal-Name and not the Common-Name for AD LDAP authentication.

  To provide backward compatibility, support authentication based on the Common Name is still supported. Common Name based-authentication is not recommended for new installations.

- A user can belong to multiple groups as long as one of the groups has the same name as the Brocade role name. Among those groups, one group name must match with either the Brocade role or mapped to a switch role in the Brocade switch.

- A user can be part of any Organizational Unit (OU).

On page 79, the example is to add Virtual Fabrics:

> Example for adding Admin Domains

should be:

> Example for adding Virtual Fabrics

In Chapter 4, “Configuring Advanced Security” on page 120, the following HBA models should be added to the list of supported HBAs:

- Brocade Fibre Channel HBA models 415, 425, 815, 825

In chapter 4, “Configuring Advanced Security” on page 146 under the heading “Example of an End-to-End Transport Tunnel mode” replace the word BRCD7500 with Remote Host and replace steps 1 through 9 with the following:

> Secure traffic between two systems using AH protection with MD5 and configure IKE with pre-shared keys. The two systems are a switch, BROCADE300 (IPv4 address 10.33.74.13), and an external host (10.33.69.132).

1. On the system console, log in to the switch as Admin and enable IPsec.

   ```
   switch:admin> ipsecconfig -enable
   ```

2. Create an IPsec SA policy named AH01, which uses AH protection with MD5.

   ```
   switch:admin> ipsecconfig --add policy ips sa -t AH01 \
   -p ah -auth hmac_md5
   ```

3. Create an IPsec proposal IPSEC-AH to use AH01 as SA.

   ```
   switch:admin> ipsecconfig --add policy ips sa-proposal \
   -t IPSEC-AH -sa AH01
   ```

4. Configure the SA proposal's lifetime in time units.

   ```
   switch:admin> ipsecconfig --add policy ips sa-proposal \
   -t IPSEC-AH -lttime 280000 -sa AH01
   ```

5. Import the pre-shared key file (for example, ipseckey.psk) using the **secCertUtil** command.

6. Configure an IKE policy for the remote peer.

   ```
   switch:admin> ipsecconfig --add policy ike -t IKE01 \
   -remote 10.33.69.132 -id 10.33.74.13  -remoteid 10.33.69.132 \
   -enc 3des_cbc -hash hmac_md5 -prf hmac_md5 -auth psk \
   -dh modp1024 -psk ipseckey.psk
   ```

NOTE
IKE version ('-v' option) needs to be set to 1 (IKEv1) if remote peer is Windows XP/2K Host (Windows XP/2K does not support IKEv2)

7. Create an IPsec transform named TRANSFORM01 to use transport mode to protect traffic identified for IPsec protection and use IKE01 as key management policy.

```
switch:admin> ipsecconfig --add policy ips transform \
-t TRANSFORM01 -mode transport -sa-proposal IPSEC-AH -action \
protect -ike IKE01
```

8. Create traffic selectors to select the outbound and inbound traffic that needs to be protected.

```
switch:admin> ipsecconfig --add policy ips selector \
-t SELECTOR-OUT -d out -l 10.33.74.13 -r 10.33.69.132 \
-transform TRANSFORM01

 switch:admin> ipsecconfig --add policy ips selector \
 -t SELECTOR-IN -d in -l 10.33.69.132 -r 10.33.74.13 \
 -transform TRANSFORM01
```

9. Verify the IPSec SAs created with IKE using the **ipsecConfig −−show manual-sa −a** command.

10. Perform the equivalent steps on the remote peer to complete the IPsec configuration. Refer to your server administration guide for instructions.

On page 150, in Table 41, the row for IPSec applies to FCIP IPSec. For IPSec (Ethernet), only MD5 is blocked in FIPS mode. DH group 1 is FIPS compliant and is not blocked.

In Chapter 8, "Installing and Maintaining Firmware" on page 220, the following paragraph should be added to the caution statement:

> If you perform a firmware downgrade from Fabric OS v6.2.0 to v6.1.x on enterprise-class platforms, do not select the auto-reboot option when prompted (the default is no auto-reboot). Both of the CPs must be downgraded first and then rebooted at the same time to avoid 6.1/6.2 synchronization issues.

On page 290, in Chapter 10, in Table 69, for the FS8-18 blade, change the support under the Brocade 48000 (CP4) heading to 'unsupported'.

On page 351, in the section "Limitations and restrictions of Traffic Isolation," add the following items:

- Two N_Ports that have the same shared area cannot be configured in different TI zones. This limitation does not apply to E_Ports that use the same shared area.

- Ports that are in different TI zones cannot communicate with each other if failover is disabled, even if they are in the same (regular) zone.

> For example, the following figure shows two hosts and three targets in two TI zones. Assume that Host 1, Host 2, Target 1, Target 2, and Target 3 are also included in a regular zone, Zone A. Even though the hosts and targets are all in the same zone, if failover is disabled on the TI zones, traffic from Host 1 is isolated to the dashed line and Host 1 cannot communicate with Target 2. Likewise, traffic from Host 2 is isolated to the dotted line and Host 2 cannot communicate with Target 1.
>
> Host 1 *can* communicate with Target 3, however, because even though N_Port 3 is in a different TI zone than Host 1, Host 1 and Target 3 are connected to the same switch, with no E_Ports between.

In chapter 16, "Using the FC-FC Routing Service," under the section Supported Configurations on page 428, add the following note after the last paragraph:

> In configurations with two backbones connected to the same edge fabric, routing is not supported between edge fabrics that are not directly attached to the same backbone. Routing over multiple backbones is a multi-hop topology and is not allowed.

In chapter 20, "Configuring and Monitoring FCIP Extension Services," under the heading "Constraints for FC Fastwrite" on page 540, the following bullet should be added to the list of bullets:

- Connecting E_Ports to ports already configured for FC Fastwrite is not supported.

On page 420, in the section "QoS zones," replace the last paragraph on the page (the paragraph starting with "A QoS zone has a special name…") with the following:

> A QoS zone has a special name, to differentiate it from a regular zone. The format of the QoS zone name is as follows:
>
> For high priority: QOSH*id_xxxxx*
> For low priority: QOSL*id_xxxxx*
>
> Where *id* is a flow identifier that designates a specific virtual channel for the traffic flow and *xxxxx* is the user-defined portion of the name. For example, the following are valid QoS zone names:
>
> QOSH3_HighPriorityTraffic
> QOSL1_LowPriorityZone
>
> The switch automatically sets the priority for the "host,target" pairs specified in the zones based on the priority level (H or L) in the zone name.
>
> The flow *id* allows you to have control over the VC assignment and control over balancing the flows throughout the fabric. The *id* is from 1 – 5 for high priority traffic, which corresponds to VCs 10 – 14. For low priority traffic, the *id* is from 1 – 2, which corresponds to VCs 8 and 9. The *id* is optional; if it is not specified, the virtual channels are allocated using a round-robin scheme.

On page 424, in the section "Setting traffic prioritization," replace step 2 with the following:

2. Enter the **zoneCreate** command. The format varies depending on whether you want high or low priority traffic.

   - For high priority traffic, use the following syntax:

     ```
     zonecreate "QOSHid_zonename", "member[; member…]"
     ```

   - For low priority, use the following syntax:

     ```
     zonecreate "QOSLid_zonename", "member[; member…]"
     ```

   where:

   id A flow identifier that indicates a specific virtual channel to which the traffic is assigned. This value is from 1 – 5 for high priority traffic and from 1 – 2 for low priority traffic.
   zonename The user-defined part of the name of the zone to be created.
   member A member or list of members to be added to the zone. A zone member must be specified using WWN only.

In Section II, "Licensed Features," the chapter numbering is wrong. The correct chapter numbers should be:

Chapter 16, "Optimizing Fabric Behavior"
Chapter 17, "Using the FC-FC Routing Service"
Chapter 18, "Administering Advanced Performance Monitoring"
Chapter 19, "Administering Extended Fabrics"
Chapter 20, "Administering ISL Trunking"
Chapter 21, "Configuring and Monitoring FCIP Extension Services"
Chapter 22, "FICON Fabrics"
Chapter 23, "Configuring and Monitoring FICON Extension Services"

The chapter numbers referred to in the "Documentation Updates" section of this release note refer to the original chapter numbers.

Brocade Fabric OS Command Reference (Publication Number 53-1001186-01)

The following text should be added to the **bpPortloopbackTest** (page 55) and the **bpTurboramTest** commands (page 57) and the associated man pages on the switch:

- A **[−−slot** *slotnumber*] operand should be added to the syntax. This operand specifies the *slotnumber* and is required on bladed systems.

- The following text should be added to both commands: "Before running this diagnostic, you must disable the chassis and clear all logs using the following command sequence:
  1. **chassisdisable**
  2. **slotstatsclear**
  3. **diagclearerror −all**
  4. **burninerrclear**
  5. **cryptocfg −−disableEE** (if the encryption engine is in enabled state)"

This procedure disables the chassis, the encryption engine, and clears all logs. Failure to run this procedure will cause the diagnostic to abort with failure status.

On page 89, **cfgDefault** command and associated man page: The new −chassis parameter introduced in this release is currently unavailable. When you execute configdefault −chassis in the root or admin role, a permission denied message is displayed. Use the −all parameter instead.

On page 543, **portCfg** command and associated man page, the following should be changed:

- Under the ipf parameter, the sentence "The IP network connection between two 7500 routers or two **FC4-18i** blades is configured…" should read: "The IP network connection between two 7500 routers or two **FR4-18i** blades is configured…"

On page 787"systemVerification" command and associated man page, the following should be changed:

- Test target: "all switches in a system. " Should read "a switch or a chassis"
- The **-fru** *type* parameter is invalid and should not be used.
- The first note in the Notes section should read: "The switch must be offline for this command to run. If Virtual Fabrics are enabled on the switch, run chassisDisable to take all Logical Switches offline."
- The third note in the Notes section should read: "On platforms that include a security processor, you must disable the security processor by running **cryptocfg --disableEE** ***slot*** before running **systemVerification**. You must re-enable the security processor with **the cryptocfg -enablEE** ***slot*** command once system verification is complete."
- The following note should be added to the Notes section: "Do not perform any configuration changes such as **configUpload** or **configDownload** while the **systemVerification** test is in progress."

On page 853: The permission table in the command availability chapter, Appendix A, for the **aptpolicy** command incorrectly states that the command requires chassis permissions. This is not the case as this command is executed on a per logical switch basis. The context value for **aptpolicy** should read VF and the switch type is "All".

The following error should be corrected in the man page for the **configure** command:

- The man page currently states about the *Allow XISL use* parameter: "On the Brocade 5100 or 5300 default switch, the feature is disabled by default (default value: yes)."
- The description should be corrected to read: "On the Brocade 5100 or 5300 default switch, the feature is disabled by default (default value: no)."
- Note that the corresponding description in the Command Reference (page 107) is correct.

Fabric OS Troubleshooting and Diagnostics Guide (Publication Number 53-1001187-01)

On page 47, in the "Preinstallation Messages" section, append the first paragraph and following courier text with the following additional information:

The blocking cases, except the new cases specific to Fabric OS v6.2.0, can be removed. The blocking cases are not accumulative from version to version.

```
Downgrade is not allowed because VF is enabled. Please run
"lscfg --config" and "lscfg --delete" commands to remove
the non-default LS first, then run "fosconfig --disable vf"
to disable VF before proceeding."

Downgrade is not allowed because AG is enabled. Please run
"ag --modedisable" command to disable AG mode before
proceeding."

Non-disruptive firmwaredownload is not supported when
downgrading to 6.1. Please use firmwaredownload -s to
download the 6.1 firmware.

The FS8-18 (type 43) blade is not supported by the target
firmware. Please use slotshow to find out which slot it is
in and remove it first."

DCX-4S is not supported by the target firmware. Please try
to download another firmware.
```

Brocade Fabric Watch Administrator's Guide (Publication Number 53-1001188-01)

In Chapter 7, "Fabric Watch default settings," a number of default setting high thresholds were changed, as follows:

- On page 45, "Port Class Default Settings," the link failure count (high) setting was changed from 1000 to 500. The loss of synchronization count (high) was changed from 1000 to 500.
- On page 47, "E_Port Class Default Settings," the link failure count (high) setting was changed from 5 to 500. The loss of synchronization count (high) was changed from 1000 to 500.
- On page 49, "F/FL_Port Class Default Settings," the link failure count (high) setting was changed from 1000 to 500. The loss of synchronization count was changed from 1000 to 500.

In Chapter 8, on page 58, the example in step 3 is missing the Link Reset class. The new menu is as follows:

```
1 :  Link loss
2 :  Sync loss
3  : Signal loss
4  : Protocol error
5  : Invalid words
6  : Invalid CRCs
7  : RXPerformance
8  : TXPerformance
9  : State Changes
10 : Link Reset
11 : return to previous page
```

Fabric OS MIB Reference (Publication Number 53-1001156-01)

On page 605, add the following values to the swFCPortPhyState object:

- validating (10) The module is being validated.
- invalidModule (11) The module is invalid.

On page 781, add the following values to the fruClass object:

- 10: coreblade(10)
- 11: applicationblade(11)

Access Gateway Administrator's Guide (Publication Number 53-1001189-01)

The entry for the brocade 5100 in Table 11 (Access Gateway Default F_Port-to-N_Port Mapping) on page 55 should read as follows:

F_Ports are ports 0-31 and N_Ports are ports 32-39.

Brocade Encryption Administrator's Guide (Publication Number 53-1001201-02)

In Chapter 2, "*Encryption configuration using the management application*":

- On page 77, under the topic "Master Keys", the opening sentence should read, "When an RSA or SKM key vault is used".
- On page 78, the three bulleted items should include SKM, as follows:
  - **Backup master key**, which is enabled any time a master key exists when using an RSA or SKM key vault.
  - **Restore master key**, which is enabled when using an RSA or SKM key vault and either no master key exists or the previous master key has been backed up.
  - **Create new master key**, which is enabled when using an RSA or SKM key vault and either no master key exists or the previous master key has been backed up.

In Chapter 3, "*Encryption configuration using the CLI*":

- On page 95, the following lines should be removed from the Help command output.

```
--setEE [<slotnumber>] –routing <shared | partitioned>:
        Set encryption routing policy.
```

- On page 119, Step 2, "Set the RKM key vault type" should read "Set the SKM key vault type".

- On page 119, Step 3a, the cryptocfg command example should have the -KACcsr option rather than -KACCert, e.g., cryptocfg --export -scp **-KACcsr**.

- On page 122, step 14 is extraneous and should be removed.

- On page 125, the following topic should be added.

Generating and exporting the master key

You must generate a master key on the group leader, and export it to a backup location.

1. Generate the master key on the group leader.

   ```
   SecurityAdmin:switch>cryptocfg --genmasterkey
   ```

2. Export the master key to the key vault.

   ```
   SecurityAdmin:switch>cryptocfg -exportmasterkey
   ```

   This command prompts for a pass phrase.

   ```
   Enter the passphrase:
   ```

3. Enter the pass phrase when prompted. The pass phrase is used for the master key encryption. A pass phrase must be between 8 and 40 characters in length and can contain any character combination. Make a note of the key ID and the pass phrase. You will need the key ID and pass phrase if you should need to restore the master key from backup.

4. Export the master key to an SCP-capable external host:

   ```
   SecurityAdmin:switch cryptocfg --export -scp -currentMK <host IP>
   <host user> <host file path>
   ```

Brocade DCX Backbone Hardware Reference Manual (Publication Numbers 53-1000685-01 through -05)

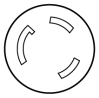
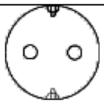
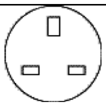
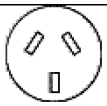
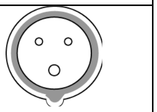
All references to the FC4-16IP blade (iSCSI blade) should be ignored. The DCX Backbone does NOT support the FC4-16IP.

The Power Cords table of Appendix A - Specifications should read as follows:

Power cords

The types of power cords provided with the Brocade DCX are specific to the country where it is installed. For each of these types of power cords (Table 5), the end that connects to the Brocade DCX has an IEC 60320/C19 cable connector. The AC power receptacles on each power supply are equipped with IEC 60320/C20 power connectors.

To order a power cord, contact your Brocade DCX supplier.

Country	Plug style				
	NEMA L6-20 USA, Canada, Mexico, other North American locations	CEE-7/7 “Schuko” Continental Europe/Ireland	BS-1363A United Kingdom/ Hong Kong	AS 3112 Australia/New Zealand	IEC-60309 32A-6h, 230 V~
					
Argentina					X
Australia				X	
Austria		X			
Bahrain			X		
Belgium		X			
Brazil	X				
Chile	X				
China, People’s Rep				X	
Czech, Rep. of					X
Denmark					X
Egypt					X
England					X
Finland					X
France		X			
Germany		X			
Greece		X			
Hong Kong		X			
Hungary			X		
India		X			
Indonesia					X
Ireland, North				X	
Ireland, South		X			
Israel			X		
Italy					X
Japan					X
Korea, South					X
Malaysia		Alternate			Recommended
Mexico	X				
Monaco		X			
Netherlands					X
New Zealand				X	
Norway					X
Poland					X
Portugal		X			
Puerto Rico	X				
Russia		X			
Saudi Arabia					X
Scotland					X
Singapore			X		
South Africa			X		
Spain					X
Sweden					X
Switzerland					X
Taiwan	x				
Turkey					X
United Arab Emirates		X			
United Kingdom/					X

Ireland					
United States	X				
Venezuela	X				
Yugoslavia					X

Brocade DCX-4S Hardware Reference Manual (Publication Number 53-1001191-01)

The entry for step 8 on page 65 should be deleted. When you pull the WWN card out by the pull tab (step 7), it unplugs directly from the backplane.

The entry for step 2 on page 66 should read as follows:

2. Hold the card by the pull tab and plug the card into the backplane. Use the Philips screwdriver and the captive screw to attach the WWN card to the chassis.

Brocade 5100 Hardware Reference Manual (Publication Number 53-1000854-02)

Table 1 on page 19 describes LED operation for the power supply. Following is an addition to this table.

LED Name	**LED Color**	**Status of Hardware**	**Recommended Action**
Power Supply Status	Flashing green	Power supply failure.	Replace power supply.

Brocade 7500 Extension Switches Hardware Reference Manual (Publication Number 53-1000026-04)

Table 4 on page 25 describes LED operation for the Fibre Channel ports. Following is an addition to this table that describes operation of the two GbE ports.

LED Name	**LED Color**	**Status of Hardware**	**Recommended Action**
Port Status	No light	No signal or light carrier (media or cable) detected.	Verify the unit power LED is on, and check the SFP and cable.

LED Name	LED Color	Status of Hardware	Recommended Action
		No SFP installed or faulty SFP.	Install or replace SFP.
	Steady green	An SFP is installed and functioning, and the link is up.	No action required.
	Flashing green	Activity on port.	No action required.
	Steady amber	SFP is installed, but not connected or the link is not up.	No action required.

Brocade 48000 Hardware Reference Manual (Publication Number 53-0000645-05)

A fully populated Brocade 48000 with eight FC8-32 or eight FC8-16 port blades does not have enough power with only one power supply. It is recommended that the 48000 be configured with four power supplies in this scenario. The blades will not power down or fail to power up unless three power supplies fail. A fully populated 48000 will continue to operate properly with two power supplies.

The Hardware Components section on page 2 should include the following sub-bullet beneath the "Modular hot-swappable field replaceable units (FRUs) bullet:

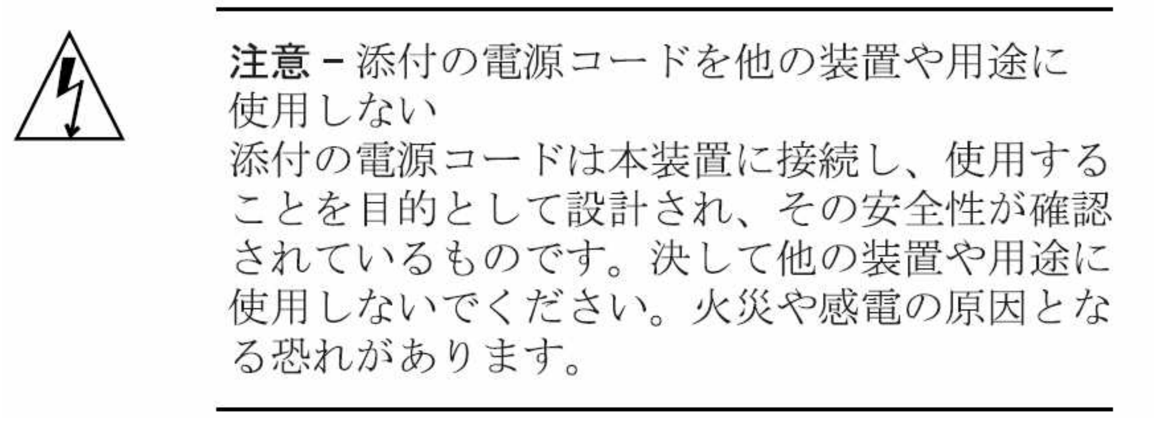
- Two power supplies are required at all times in a fully-populated 48000 chassis.

Brocade SilkWorm 200E Hardware Reference Manual (Publication Number 53-0000633-03)

Table 3-2 "System Status LED Patterns During Normal Operation" has the incorrect behavior listed in row three. Instead of reading *Slow-flashing green*, it should read *Flashing amber/green*.

Under "Regulatory Compliance" in "Product Specifications" (Appendix A), add the following statement:

Power Cords (Japan, Denan)



注意 – 添付の電源コードを他の装置や用途に使用しない

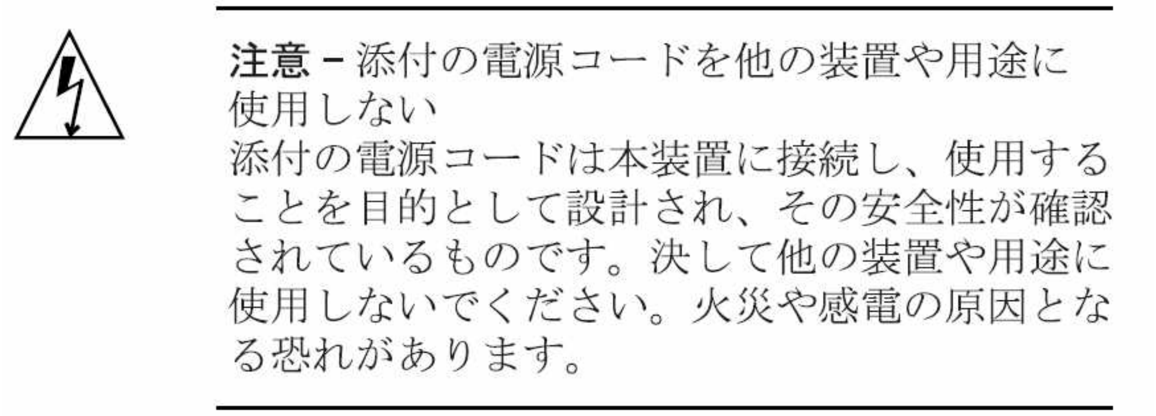
添付の電源コードは本装置に接続し、使用することを目的として設計され、その安全性が確認されているものです。決して他の装置や用途に使用しないでください。火災や感電の原因となる恐れがあります。

Attention: Never use the power cord packed with your equipment for other products.

Brocade SilkWorm Multiprotocol Router Model AP7420 Hardware Reference Manual (Publication Number 53-1000179-01)

Under “Regulatory Compliance” in “Specifications and Regulatory Compliance” (Appendix A), add the following statement:

Power Cords (Japan, Denan)



注意 – 添付の電源コードを他の装置や用途に使用しない

添付の電源コードは本装置に接続し、使用することを目的として設計され、その安全性が確認されているものです。決して他の装置や用途に使用しないでください。火災や感電の原因となる恐れがあります。

Attention: Never use the power cord packed with your equipment for other products.

Brocade Mi10K Director Installation and Service Manual (Publication Number 53-1000711-01)

Step 10 on page 2-13 should be the following:

> Change the IP address, subnet mask, and gateway address as directed by the customer. To change the addresses, type the following and press **Enter**.
>
> **system ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy zzz.zzz.zzz.zzz**
>
> The IP address is xxx.xxx.xxx.xxx, the subnet mask is yyy.yyy.yyy.yyy, and the gateway address is zzz.zzz.zzz.zzz, where the octets xxx, yyy, and zzz are decimals from zero through 255. If an address is to remain unchanged, type the current address in the respective field.

Brocade Fabric OS Message Reference (Publication Number 53-1001157-01)

On page 515, in Chapter 86, the “TRCK-1004” raslog messages are not logged in v6.2.0 due to feature deprecation.

Defects

Closed with Code Change Defects in Fabric OS v6.2.0g

This section lists defects closed in Fabric OS v6.2.0g. Note that when a workaround to an issue is available, it is provided.

Defect ID: DEFECT000236764	**Technical Severity**: Critical
Summary: Brocade Encryption Switch (BES) goes to 'faulty' state after test cycle that alternately reboots each BES in the configuration every 5 minutes.	
Symptom: BES goes to 'faulty' state after the weekend run that alternately reboots each BES in the configuration every 5 minutes.	
Feature: FC Services	**Function**: Other
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.1.1_enc	**Service Request ID**: 356483

Defect ID: DEFECT000237921	**Technical Severity**: High
Summary: Test tool reports data corruption during an overnight run.	
Symptom: The test continuously disables/enables the ISL links to force failover/failback between members of an HA cluster.	
Feature: Data Security	**Function**: Disk Encryption
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.1.1_enc	**Service Request ID**: 359931

Defect ID: DEFECT000245146	**Technical Severity**: High
Summary: Continuously disconnect/reconnecting the ISLs in the HA environment causes one of the Brocade Encryption Switches (BES) to go into faulty state.	
Symptom: While IOs and rekey are in progress, continously disconnect/reconnecting the ISLs in the HA environment causes the BES to go into 'faulty' state	
Feature: Data Security	**Function**: Disk Encryption
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	**Service Request ID**: 372889

Defect ID: DEFECT000245868	**Technical Severity**: High
Summary: Encrypted LUN gets into internal Encryption Engine (EE) LUN State: Disabled (key not in sync) as a result of rekeying and High Availability Cluster (HAC) / Data Encryption Key (DEK) cluster failover and failback.	
Symptom: Encrypted LUN is not available for crypto operations.	
Feature: Data Security	**Function**: Disk Encryption
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000245996	**Technical Severity**: High
Summary: Brocade Encryption Switch (BES) goes faulty as a result of alternately rebooting the two BES that have all the physical connectivities to the targets and initiators.	
Symptom: Faulty BES will not be available for crypto operations.	
Feature: Data Security	**Function**: Disk Encryption
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000246377	**Technical Severity**: High
Summary: After rebooting one Brocade Encryption Switch (BES) of a High Availability Cluster (HAC) that has connectivity to the physical targets and initiators, all the crypto targets are lost in the HAC cluster.	
Symptom: LUNs that were part of the lost crypto target containers are not available for crypto operations.	
Feature: Data Security	**Function**: Disk Encryption
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000246901	**Technical Severity**: High
Summary: Brocade Encryption Switch (BES) shows Encryption Engine busy when continuously and repeatedly disable/enable IO sync ports of the BES.	
Symptom: BES and Encryption Engine are not available for crypto operations.	
Feature: Data Security	**Function**: Disk Encryption
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000248165	**Technical Severity**: High
Summary: During stress test overnight run of rekey and ISL disable/enable, the test tool exited on write failure to encrypted LUNs.	
Symptom: During a stress test run of rekey + ISL disable/enable, the test tool running on a host in the fabric due to write failure to three drives. A second host writing to the same targets did not encounter this issue.	
Feature: Data Security	**Function**: Disk Encryption
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000248947	**Technical Severity**: High
Summary: While rekey operations are in progress, disrupting the IO sync link causes rekey operations to hang.	
Symptom: Affected re-key operations will hang and not make progress.	
Feature: Data Security	**Function**: Disk Encryption
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000248948	**Technical Severity**: High
Summary: Rekey operation hangs as a result of failing over to the path that no longer has access to the physical target	
Symptom: Rekey operation does not complete.	
Feature: Data Security	**Function**: Disk Encryption
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000250753	**Technical Severity**: High
Summary: As a result of I/O and crypto operations, three LUNs are in "Key ID Unvailable" state and one LUN indicates that inquiry failed	
Symptom: Three LUNs on container showing Key ID Unavailable, and one LUN showing inquiry failed. These LUNs are fully functional with no issues on all other containers.	
Workaround: Reboot the Encryption Engine (EE.)	
Feature: Data Security	**Function**: Infrastructure
Probability: Medium	**Risk of Fix**: Medium
Found in Release: FOS6.2.0	

Defect ID: DEFECT000253164	**Technical Severity**: High
Summary: Mixing FibreChannel FastWrite (FCFW) and Non-FCFW flows can cause dcam entries to not be set correctly.	
Symptom: When attempting to run a FCFW flow to a device port that already has Non-FCFW flows running to it, the FCFW flow appears to fail without seeing any kind of port filter counters incrementing, indicating that FCFW frames were seen.	
Feature: Field Escalation	**Function**: ASIC Driver
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000237521	**Technical Severity**: Medium
Summary: Rekey operation is restarted but hung after all the Encryption Engines (EEs) in the encryption group are rebooted.	
Symptom: Rekey operation hangs after all EEs are rebooted.	
Feature: Data Security	**Function**: Re-key
Probability: Low	**Risk of Fix**: Medium
Found in Release: FOS6.1.1_enc	**Service Request ID**: 358763

Defect ID: DEFECT000244112	**Technical Severity**: Medium
Summary: Rekeyed LUNs are in "Not Ready (Getting key from archive)" state when the key vault goes down and does not recover.	
Symptom: LUNs are stuck in the "Not Ready (Get key from archieve)" even after the key vault is brought back online. LUNs can't be recovered even after removing and re-adding them from/to the target container.	
Feature: Data Security	**Function**: Key Vault
Probability: Low	**Risk of Fix**: Medium
Found in Release: FOS6.2.0	**Service Request ID**: 371327

Defect ID: DEFECT000245009	**Technical Severity**: Medium
Summary: Persistently disabled GE port on a Brocade FR4-18i blade becomes disabled after hafailover.	
Symptom: A GE port on a Brocade FR4-18i blade is persistently disabled. After that hafailover is initiated. Once the system comes up after failover, the persistenly disabled GE port is in disabled state and not disabled persistent state.	
Feature: FCIP	**Function**: FCIP HA
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000250477	**Technical Severity**: Medium
Summary: Passive path LUN gets stuck in not ready (Get key from archive) state.	
Symptom: When running a test case that periodically downs the link to the key vault , the LUN go to "Not ready (Get key from archive)" state when Ethernet connection to primary key vault is broken.	
Feature: Data Security	**Function**: Key Vault
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Closed with Code Change Defects in Fabric OS v6.2.0f

This section lists defects closed in Fabric OS v6.2.0f. Note that when a workaround to an issue is available, it is provided.

Defect ID: DEFECT000227048	**Technical Severity**: High
Summary: Detected unexpected termination of Remote Procedure Call (RPC) daemon.	
Symptom: RPC Daemon application will crash, then will non-disruptively restart. The following error messages may be observed: [KSWD-1003] kSWD: Detected unexpected termination of: "[13]rpcd:0 ... [RAS-1001] First failure data capture (FFDC) event occurred. [SYSC-1004] Daemon rpcd restart successful.	
Feature: Field Escalation	**Function**: Management Services
Probability: Low	**Risk of Fix**: Medium
Found in Release: FOS5.3.0	**Service Request ID**: 333775

Defect ID: DEFECT000248707	**Technical Severity**: High
Summary: UNIX based host with FCFW enabled has problems with port disable/enable of HBA ports.	
Symptom: Server hangs after Brocade 7500 reboot.	
Feature: 4G ASIC Driver	**Function**: Zoning
Probability: Medium	**Risk of Fix**: Medium
Found in Release: FOS6.2.0	

Defect ID: DEFECT000244126	**Technical Severity**: Medium
Summary: If configdownload is performed via DCFM, switch authentication failure may be seen.	
Symptom: Authentication failure for clients using HTTP service.	
Workaround: Execute hafailover or hareboot.	
Feature: Mgmt Embedded - HTTP	**Function**: User Admin
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000244915	**Technical Severity**: Medium
Summary: Pathinfo command failure occurs when run on FOS 6.1, if the path traverses through FOS 6.2.x.	
Symptom: Pathinfo from 6.1 to 6.2.x fails with "Destination Domain Unreachable".	
Feature: Fabric Infrastructure	**Function**: Mgmt Server
Probability: High	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000245609	**Technical Severity**: Medium
Summary: Supportshow cli command output should complete without having to hit CR several times.	
Symptom: Supportshow output requires user intervention during output.	
Feature: Fabric Infrastructure	**Function**: Security-authentication
Probability: High	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000248796	**Technical Severity**: Medium
Summary: Console is not accessible on Brocade 5480.	
Symptom: Console is not accessible on embedded switch.	
Feature: Embedded Platform Services	**Function**: Bulova
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000250264	**Technical Severity**: Medium
Summary: Observed ASSERT on standby CP if ICL ports are in disabled state and moved to a different Logical Switch and hafailover is performed without enabling those ports.	
Symptom: ASSERT may be observed on the standby cp (soon to be active cp) when hafailover is issued with the signature: ASSERT - Failed expression: (area == sw->sw_pt[port]->full_fmt_area), file = /vobs/projects/springboard/build/swbd62/fabos/src/sys/dev/switch/switch_recov_ha.c, line = 1747, kernel mode.	
Feature: 8G Platform Services	**Function**: FOS Kernel Drivers
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.3.0	

Closed with Code Change Defects in Fabric OS v6.2.0e

This section lists defects closed in Fabric OS v6.2.0e. Note that when a workaround to an issue is available, it is provided.

Defect ID: DEFECT000236477	**Technical Severity**: High
Summary: Connectivity issues related to tape pipelining when dealing with FCR fames.	
Symptom: Frames can be dropped by the switch if a specific connectivity issue exists as a result of losing the original source ID in the REC command. Supportsave may panic occasionally when FC fastwrite is not enabled on the GE port.	
Feature: Field Escalation	**Function**: FCIP
Probability: Low	**Risk of Fix**: High
Found in Release: FOS6.0.0	**Service Request ID**: 353979

Defect ID: DEFECT000243085	**Technical Severity**: High
Summary: VEX port received bad SFID and frame cannot be routed to translate domain.	
Symptom: Continuous RTWR retries are seen on switch from BB fabric where fabricshow is missing IP address.	
Feature: FCR	**Function**: Integrated Routing
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.1.2	

Defect ID: DEFECT000246149	**Technical Severity**: High
Summary: Port Fencing - E-port Class Link Resets are not fencing.	
Symptom: RASLOG message will be presented indicating link resets are above threshold, but the port will not have been fenced, as expected.	
Feature: Fabric Infrastructure	**Function**: Fabric Watch
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000246519	**Technical Severity**: High
Summary: User entered FRU number via CLI is not being modified.	
Symptom: RNID data reporting same serial # for two different logical switches.	
Feature: FICON	**Function**: Ficud
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000246775	**Technical Severity**: High
Summary: Detected termination of process fabricd:4120 followed by software verify errors.	
Symptom: Brocade DCX is unresponsive.	
Feature: 8G Platform Services	**Function**: PID management
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000246908	**Technical Severity**: High
Summary: Partitioned Brocade DCX-4S panic'd after reset allegiance issued by multiple hosts.	
Symptom: FICUD terminates and switch reboots.	
Feature: FICON	**Function**: Ficud
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000246916	**Technical Severity**: High
Summary: SNMPd core file filled up the root file system on Brocade DCX-4S.	
Symptom: User will observe snmpd process being killed and error message "Detected termination of process snmpd:4636, hasm_swd.c, line: 168, comp:insmod, ltime:2009/03/08-20:20:07:011335". The panic will generate the core file that takes away space on the root file system.	
Feature: Mgmt Embedded - SNMP	**Function**: Other
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	**Service Request ID**: 373285

Defect ID: DEFECT000247176	**Technical Severity**: High
Summary: Node descriptors are missing for Brocade DCX and DCX-4S.	
Symptom: Missing Node descriptors (FICON RNID data)	
Feature: Pluto Platform Services	**Function**: Platform Services
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000247409	**Technical Severity**: High
Summary: Tapepipelining code begins to randomly send only data frames in an exchange to tape drive.	
Symptom: Tape job fails.	
Feature: FCIP	**Function**: FCIP Performance
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	**Service Request ID**: 375305

Defect ID: DEFECT000247757	**Technical Severity**: High
Summary: Portswap not working for ports 32-47 on 48 port blade	
Symptom: Portswap will not work on port 32-47 on 48 port blade from GUI	
Feature: FICON	**Function**: Ficud
Probability: High	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000248534	**Technical Severity**: High
Summary: RLIR's with LOL is being generated on 8G channels during CEC IML	
Symptom: During CEC IML of 8G channels, RLIR's are being generated by switch.	
Feature: 8G ASIC Driver	**Function**: PORT
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000248901	**Technical Severity**: High
Summary: Tapepipelining code on PI side does not close exchange upon a ELS RJT response to REC -- "invalid oxid/rxid combo"	
Symptom: Writing to tape would fail at random points along the write sequences. device would stop getting write data. Reading from tape would be unaffected.	
Feature: FCIP	**Function**: FCIP Performance
Probability: High	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000236136	**Technical Severity**: Medium
Summary: FC Fastwrite corrupts buffer pool upon TWB allocation failure on Proxy Initiator.	
Symptom: I/O fails.	
Feature: Field Escalation	**Function**: FCIP
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.1.1	

Defect ID: DEFECT000244615	**Technical Severity**: Medium
Summary: Web Tools shows high CPU usage (~80%) when port configuration operation is performed in DCX	
Symptom: CPU usage in Web Tools is showing high (70% – 80%) when port configuration operation is performed on a large system.	
Feature: WebMgmt	**Function**: Other
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000247054	**Technical Severity**: Medium
Summary: Supportsave may show parity errors on disabled ports.	
Symptom: Supportsave starting with FOS v6.1.2 has been updated to collect more data. As data is read from disabled ports, a parity error may be logged from those disabled and unused ports. A switch that has been upgraded from a lower code level, and never cold booted, may show this problem. No errors will be caused on enabled ports, or after a disabled port is enabled.	
Feature: Field Escalation	**Function**: ASIC Driver
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.1.0	

Defect ID: DEFECT000247602	**Technical Severity**: Medium
Summary: Blades are not shown in when a slot is hot plugged in to a DCX/DCX-4s	
Symptom: When a slot is hot plugged, its information will not appear on the GUI	
Feature: Mgmt Embedded - CAL	**Function**: Ports Admin
Probability: High	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000247663	**Technical Severity**: Medium
Summary: Observed frame drops and IFCCs with lossless feature.	
Symptom: Lossless DLS failed with dropped frame causing IFCC in presence of ICLs.	
Feature: 8G Platform Services	**Function**: Routing
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Closed with Code Change Defects in Fabric OS v6.2.0d

This section lists defects closed in Fabric OS v6.2.0d. Note that when a workaround to an issue is available, it is provided.

Defect ID: DEFECT000235613	**Technical Severity**: High
Summary: Memory leak found during E-port processing.	
Symptom: An E_port constantly going on and off due to other conditions can lead to an out-of-memory condition.	
Feature: Field Escalation	**Function**: Panic / OOM
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.1.0	**Service Request ID**: 346457

Defect ID: DEFECT000236118	**Technical Severity**: High
Summary: 8Gb storage device failed to detect 8Gb speed when port was locked as a G_port.	
Symptom: Certain 8Gb storage arrays are connecting to Brocade 8Gb switches as 4Gb devices when the switch port is locked as a G_port.	
Workaround: Instead of relying on auto-negotiation, lock the switch port at 8Gb.	
Feature: Field Escalation	**Function**: ASIC Driver
Probability: High	**Risk of Fix**: Low
Found in Release: FOS6.1.0	**Service Request ID**: 354645

Defect ID: DEFECT000237420	**Technical Severity**: High
Summary: Memory leak when querying connUnitPortFCId in Access Gateway (AG) mode and also when querying FcFeModuleName.	
Symptom: Switch panic due to "out of memory" trigger during hafailover/hareboot.	
Workaround: Avoid querying FcFeModuleName or (connUnitPortFCId in AG mode) MIB to avoid memory leak.	
Feature: Field Escalation	**Function**: Panic / OOM
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS5.3.1	**Service Request ID**: 348199

Defect ID: DEFECT000237701	**Technical Severity**: High
Summary: Observed kernel panic on a DCX in RTE module.	
Symptom: DCX will panic and hafailover during supportsave in rare occasions.	
Feature: Field Escalation	**Function**: FC Layer 2 Routing
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.1.1	**Service Request ID**: SR359167

Defect ID: DEFECT000237868	**Technical Severity**: High
Summary: Fabric Watch failed to initialize on fully populated DCX.	
Symptom: During HA recovery, management application reports switch health status as Marginal/Down. Traffic is not impacted, but DCFM call home will not be initiated.	
Feature: Field Escalation	**Function**: Management Services
Probability: Low	**Risk of Fix**: Medium
Found in Release: FOS6.1.0	

Defect ID: DEFECT000241933	**Technical Severity**: High
Summary: SNMP v3 user configuration reverts back to defaults after HAfailover.	
Symptom: When configuring SMNP v3 user configuration on any one of the user-defined USM configuration sets and during HAfailover, the SNMP configuration reverts back to default.	
Feature: Mgmt Embedded - SNMP	**Function**: Other
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	**Service Request ID**: 367427

Defect ID: DEFECT000242132	**Technical Severity**: High
Summary: Detected termination of 0.weblinker.fcg on DCX-4S.	
Symptom: May see messages like "KSWD-1002], 5766, SLOT 4 | FFDC | CHASSIS, WARNING, Brocade_DCX4S, Detected termination of process 0.weblinker.fcg:4837" on the console.	
Feature: FICON	**Function**: Ficud
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000242139	**Technical Severity**: High
Summary: Ports were found disabled after enabling Virtual Fabric (VF) through DCFM on Brocade 5100.	
Symptom: Some ports may be disabled after enabling VF through DCFM.	
Feature: FICON	**Function**: Ficud
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000242555	**Technical Severity**: High
Summary: Missing FICON interrupt on DCX-4S.	
Symptom: CUP did not respond in time before channel timed out.	
Feature: FC Services	**Function**: Name Server
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000242951	**Technical Severity**: High
Summary: Command "fddcfg –fabwideset" and other security commands fails with RCS transaction error.	
Symptom: May see error message like "Security Application returned Transaction Error, 0x1500000b".	
Feature: FC Services	**Function**: Fabric
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000243059	**Technical Severity**: High
Summary: When performing firmwareupgrade from FOS v6.1.x to v6.2.0 and reverting back by firmwarerestore from v6.2.0 to v6.1.x does not succeed and leaves CP with unrecoverable passwords.	
Symptom: Firmwarerestore will fail and leave the CP in inconsistent state and user may not be able to login.	
Workaround: Once passwords are blocked, booting into single-user mode is required with reset of the system passwords.	
Feature: Infrastructure	**Function**: Firmware Download
Probability: Medium	**Risk of Fix**: High
Found in Release: FOS6.2.0	

Defect ID: DEFECT000243349	**Technical Severity**: High
Summary: Disconneting/reconnecting the ISL on Brocade Encryption Switch while rekey in progress may result in new key creation failure.	
Symptom: Disconnecting/reconnecting the ISL while rekey operations are in progress, causes the rekey to hang. LUN state shows "Rekey ACK timeout."	
Feature: Data Security	**Function**: Disk Encryption
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	**Service Request ID**: 370041

Defect ID: DEFECT000243880	**Technical Severity**: High
Summary: CP panic with FICUd crash occurred during supportsave operation.	
Symptom: FICUd crash and CP reboot	
Workaround: This can be avoided by doing one of the following after enabling FMSMODE for the first time: - switchdisable/switchenable - hafailover - hareboot - reboot	
Feature: FICON	**Function**: Ficud
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000243959	**Technical Severity**: High
Summary: During rekey operations, continuously disconnect/reconnect the ISL links between 2 cluster nodes, causes one of the LUN to hang at "LUN discovery" state.	
Symptom: LUN may hang at "LUN discovery" state if ISL is continuously disconnected/reconnected.	
Feature: Data Security	**Function**: Disk Encryption
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	**Service Request ID**: 371035

Defect ID: DEFECT000244009	**Technical Severity**: High
Summary: All LUNs in a container are showing target offline.	
Symptom: Host will no longer have access to their LUNs through the crypto target containers.	
Feature: Data Security	**Function**: Disk Encryption
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000244987	**Technical Severity**: High
Summary: With tape pipelining active, the switch may return a good status without sending data.	
Symptom: Tape I/O may fail with errors.	
Feature: FCIP	**Function**: FCIP I/O
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	**Service Request ID**: 371297

Defect ID: DEFECT000245277	**Technical Severity**: High
Summary: Host detecting IFCCs errors to CUP Port.	
Symptom: IFCC errors	
Feature: FICON	**Function**: Ficud
Probability: High	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000246162	**Technical Severity**: High
Summary: Brocade Encryption Switch went Faulty when starting traffic.	
Symptom: Loss of LUNs to the Host	
Feature: Data Security	**Function**: Disk Encryption
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000246423	**Technical Severity**: High
Summary: Taking the RKM down while rekeys are in progress, causes one of the LUN gets stuck at state "Not ready (Key creation)".	
Symptom: Taking the RKM down while rekeys are in progress, causes one of the LUN gets stuck at state "Not ready (Key creation)".	
Feature: Data Security	**Function**: Disk Encryption
Probability: Low	**Risk of Fix**: Medium
Found in Release: FOS6.2.0	

Defect ID: DEFECT000226734	**Technical Severity**: Medium
Summary: When attempting to swap ports from the GUI, the operation may fail due to HTTP 500 error	
Symptom: Port Swap failing due to HTTP 500 error	
Workaround: No	
Feature: Mgmt Embedded - HTTP	**Function**: Ports Admin
Probability: High	**Risk of Fix**: Low
Found in Release: FOS6.1.1	

Defect ID: DEFECT000232767	**Technical Severity**: Medium
Summary: SNMP changes required to better support snmp mib.	
Symptom: Default snmpv3 sets different default values between FOS releases, mibcapability option of snmpconfig cannot control ficon mib.	
Workaround: No	
Feature: Field Escalation	**Function**: SNMP
Probability: Low	**Risk of Fix**: Medium
Found in Release: FOS6.1.1	

Defect ID: DEFECT000236582	**Technical Severity**: Medium
Summary: If second FDISC comes in before the switch responds to the first FDISC between the same pair of devices, the Access Gateway daemon panics.	
Symptom: Access Gateway daemon panic triggers switch reboot.	
Feature: Field Escalation	**Function**: Access Gateway
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS5.3.0	**Service Request ID**: 354129

Defect ID: DEFECT000238433	**Technical Severity**: Medium
Summary: Applications cannot distinguish between FA4-18 and Core blades on DCX using SNMP. Need to add two new FRU classes: "coreblade" and "applicationblade" class.	
Symptom: Applications cannot distinguish between FA4-18 and Core blades using SNMP.	
Feature: Mgmt Embedded - SNMP	**Function**: Switch Admin
Probability: High	**Risk of Fix**: Medium
Found in Release: FOS6.1.0	

Defect ID: DEFECT000242074	**Technical Severity**: Medium
Summary: Optimized SERDES setting for Brocade 5480.	
Symptom: No visible symptom.	
Feature: 8G ASIC Driver	**Function**: GE2 ASIC ports
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000242319	**Technical Severity**: Medium
Summary: Need to add two more values for SNMP port state that includes "validating (10)" module is being validated and "invalidModule (11)" module is invalid.	
Symptom: SNMP object "swFCPortPhyState" is getting invalid value 11.	
Feature: Mgmt Embedded - SNMP	**Function**: Other
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000242961	**Technical Severity**: Medium
Summary: WWN mapping for certain storage systems is incorrect.	
Symptom: With FOS v6.2.x, Web Tools reports a device incorrectly.	
Feature: WebMgmt	**Function**: Other
Probability: High	**Risk of Fix**: Low
Found in Release: FOS6.2.0	**Service Request ID**: 369495

Defect ID: DEFECT000243244	**Technical Severity**: Medium
Summary: As DCFM polling LUNs, the memory usage for weblinker is increased	
Symptom: Memory consumption goes high	
Feature: Data Security	**Function**: Infrastructure
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000243578	**Technical Severity**: Medium
Summary: With VF, deleting a FID while in the FID leads to undesirable conditions. The user is stuck in the FID and all commands run generate an error message.	
Symptom: In VF mode, after deleting a FID system may get into undesirable state and, commands run generate an error	
Feature: Fabric Infrastructure	**Function**: Security-login
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000243717	**Technical Severity**: Medium
Summary: Node descriptors are not shown for M-EOS switch in DCFM when using FOS switch as the seed switch.	
Symptom: The node descriptors are not shown for the Mi10k in DCFM when using FOS switch as the seed switch.	
Feature: Mgmt Embedded - CAL	**Function**: Other
Probability: High	**Risk of Fix**: Medium
Found in Release: FOS6.2.0	

Defect ID: DEFECT000243749	**Technical Severity**: Medium
Summary: Brocade 300 not responding to Link Reset primitives correctly	
Symptom: Devices may send an OLS and/or link reset	
Feature: 8G ASIC Driver	**Function**: C2 ASIC driver
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000244738	**Technical Severity**: Medium
Summary: Re-keys are getting stuck	
Symptom: Re-key progress halts.	
Feature: Data Security	**Function**: Re-key
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000245047	**Technical Severity**: Medium
Summary: Switchname mismatch between fabricinfo.html and switchname command from CLI	
Symptom: User sees a name difference between DCFM and Webtools.Beacuse the Switch name is not updated properly at fabricinfo.html.	
Feature: 8G Platform Services	**Function**: PID management
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000245846	**Technical Severity**: Medium
Summary: FICON fcip block count mismatch on read emulation.	
Symptom: Tape repositioning may be incorrect when split status responses received to backspace block commands.	
Feature: FCIP	**Function**: FCIP I/O
Probability: High	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000245865	**Technical Severity**: Medium
Summary: A LUN gets stuck in the Internal EE LUN State: Read Only (Internal metadata key is in RO state).	
Symptom: LUN will not be available for Host until the DiscoverLUN is issued	
Feature: Data Security	**Function**: Disk Encryption
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000245891	**Technical Severity**: Medium
Summary: Port Movement from DCFM should be All-or-nothing behavior.	
Symptom: When attempting to move ports from DCFM, some of the ports may be moved and others fail.	
Feature: Mgmt Embedded - CAL	**Function**: Other
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Closed with Code Change Defects in Fabric OS v6.2.0c

This section lists defects closed in Fabric OS v6.2.0c. Note that when a workaround to an issue is available, it is provided.

Defect ID: DEFECT000236118	**Technical Severity**: Critical
Summary: 8Gb storage device failed to detect 8Gb speed when port was locked as a G_port.	
Symptom: Certain 8Gb storage arrays are connecting to Brocade 8Gb switches as 4Gb devices when the switch port is locked as a G_port.	
Workaround: Instead of relying on auto-negotiation, lock the switch port at 8Gb.	
Feature: Field Escalation	**Function**: ASIC Driver
Probability: High	**Risk of Fix**: Low
Found in Release: FOS6.1.0	**Service Request ID**: 354645

Defect ID: DEFECT000226808	**Technical Severity**: High
Summary: Occasionally during the firmware upgrade process, the 1250 processor is still rebooting when the FCR routes are being processed, resulting in missing FCR routes and an inability to route traffic across VEX ports.	
Symptom: I/O running through VEX ports or devices imported/exported via VEX ports will be dropped after firmware upgrade.	
Feature: Field Escalation	**Function**: FCIP
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.0.0	

Defect ID: DEFECT000232995	**Technical Severity**: High
Summary: VI to PT routes are deleted following portdisable/enable on a Brocade FC4-48 blade.	
Symptom: VI is not able to login to Target following creation of FR zone and portdisable/enable for the host port.	
Feature: Field Escalation	**Function**: FC Layer 2 Routing
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.0.1	

Defect ID: DEFECT000239682	**Technical Severity**: High
Summary: Passwords were reset to default on Brocade DCX upgrade from FOS v6.1.1_enc2 to v6.2.0.	
Symptom: User unable to login.	
Feature: Fabric Infrastructure	**Function**: Security-login
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	**Service Request ID**: 363533

Defect ID: DEFECT000240056	**Technical Severity**: High
Summary: Channel receiving RSCN with missing ports in payload after HPF key on or off.	
Symptom: RSCN transmitted by the switch does not transmit all the port IDs in the payload.	
Feature: FC Services	**Function**: Name Server
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.1.1	

Defect ID: DEFECT000240927	**Technical Severity**: High
Summary: Data encryption backup jobs failing due to Brocade DCX crash and reboot when Top Talkers are enabled with Frame Redirection.	
Symptom: Encrypted tape backup job fails when Brocade DCX reboots.	
Workaround: Do not enable Top Talkers concurrently with functionality that is using frame redirection.	
Feature: FC Services	**Function**: Zoning
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000240955	**Technical Severity**: High
Summary: Discovered that a stable working encryption group had split after a successful I/O test run.	
Symptom: After successful DP test run, may observe “comm error” on the group leader.	
Feature: Data Security	**Function**: Infrastructure
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000241236	**Technical Severity**: High
Summary: While doing first time encryption to a LUN with more than 1 initiator active at the same time, rekey operations slowed signficantly.	
Symptom: Host applications can experience delays in the completion of their I/O requests.	
Workaround: 1. Disable the target ports. 2. Remove one initiator from the container. 3. Start the rekey. 4. Add the initiator back.	
Feature: Data Security	**Function**: Re-key
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000241969	**Technical Severity**: High
Summary: Software verify error occurred during supportsave on DCX and DCX-4S.	
Symptom: Software verify errors and IFCCs seen during supportsave.	
Feature: Fabric Infrastructure	**Function**: Security-login
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000242065	**Technical Severity**: High
Summary: FOS v6.2.0 does not provide Chassisinfo with snmpv1 without adding and configuring an snmpv3 user.	
Symptom: The first 6 objects in the system MIB are missing – this corresponds to the 'error: no such object' entries in the Hi-Track system table.	
Feature: Mgmt Embedded - SNMP	**Function**: Other
Probability: High	**Risk of Fix**: Low
Found in Release: FOS6.2.0	**Service Request ID**: 365711

Defect ID: DEFECT000242682	**Technical Severity**: High
Summary: VTs/VIs disappear when rebooting the Brocde Encryption Switch that has all the physical connections to targets and initiators.	
Symptom: VIs/VTs may disappear when rebooting the Brocde Encryption Switch.	
Feature: Data Security	**Function**: Disk Encryption
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	**Service Request ID**: 368783

Defect ID: DEFECT000242683	**Technical Severity**: High
Summary: Repeatedly disconnect/reconnecting the ISL links between the Brocade Encryption Switch in the HA cluster environment while rekey operations are in progress may cause data miscompare.	
Symptom: Disconnect/reconnecting the ISL links between Brocade Encryption Switch in HA cluster may cause data corruption.	
Feature: Data Security	**Function**: Disk Encryption
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	**Service Request ID**: 368785

Defect ID: DEFECT000242784	**Technical Severity**: High
Summary: Calculation of TX port and Filter number can incorrectly corrupt the Filter Redirect RAM	
Symptom: An internal recovery scheme can attempt to correct a valid Frame Redirection RAM Filter. This will cause one existing filter to be corrupted, potentially leading to misrouted frames. This is a very rare failure, but if encountered, one of the filter entries will be corrupted.	
Feature: 8G ASIC Driver	**Function**: C2 ASIC driver
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000242813	**Technical Severity**: High
Summary: Running configdefault may cause Kernel panic on Brocade 48000.	
Symptom: Observed Kernel panic after configdefault on Brocade 48000.	
Feature: Infrastructure	**Function**: VF infrastructure
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000243152	**Technical Severity**: High
Summary: Encryption group can't automatically recover after it is split into 2 different islands.	
Symptom: Encryption group won't automatically recover after it is split into 2 different islands.	
Feature: Data Security	**Function**: HA Cluster
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	**Service Request ID**: 302186

Defect ID: DEFECT000237198	**Technical Severity**: Medium
Summary: FOS upgrade on Brocade 3016 to FOS v5.3.x leaves the switch in an unusable state.	
Symptom: Customer was upgrading Brocade 3016 from FOS v5.0.x to v5.3.x and some units would not boot up afterword. After login, limited commands are available and switch fails cold recovery.	
Feature: Mgmt Embedded - SNMP	**Function**: Other
Probability: Medium	**Risk of Fix**: Medium
Found in Release: FOS5.3.1	

Defect ID: DEFECT000238430	**Technical Severity**: Medium
Summary: Switch panic when supportsave read invalid data on GE ports without FC Fastwrite enabled.	
Symptom: Unexpected switch panic.	
Feature: Field Escalation	**Function**: FCIP Flipper/ASIC
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.1.0	**Service Request ID**: 361287

Defect ID: DEFECT000239422	**Technical Severity**: Medium
Summary: FICON XRC times out on Brocade 7500 to DCX.	
Symptom: Specific third party drives not coming on line.	
Feature: FCIP	**Function**: FCIP I/O
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.1.1	**Service Request ID**: 361531

Defect ID: DEFECT000240677	**Technical Severity**: Medium
Summary: Enabled minimum FOS support for DWDM-SFP port media.	
Symptom: No visible symptom. Enabled new SFP support.	
Feature: Pluto Platform Services	**Function**: SysCtrl/EM
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000241032	**Technical Severity**: Medium
Summary: Switch did not indicate a warning when a PS/FAN FRU was removed.	
Symptom: Brocade 5100 did not indicate the warning in spite of PS/FAN FRU removal.	
Feature: WebMgmt	**Function**: Fabric Watch
Probability: High	**Risk of Fix**: Low
Found in Release: FOS6.2.0	**Service Request ID**: 363745

Defect ID: DEFECT000241777	**Technical Severity**: Medium
Summary: Reporting high temperature alarms on Brocade FS8-18 blades when the ambient temperature is 39C.	
Symptom: Customer may see high temperature alerts.	
Feature: System Controls/EM	**Function**: Pluto
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	**Service Request ID**: 367201

Defect ID: DEFECT000242074	**Technical Severity**: Medium
Summary: Optimized SERDES setting for Brocade 5480.	
Symptom: No visible symptom.	
Feature: 8G ASIC Driver	**Function**: GE2 ASIC ports
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Closed with Code Change Defects in Fabric OS v6.2.0b

This section lists defects closed in Fabric OS v6.2.0b. Note that when a workaround to an issue is available, it is provided.

Defect ID: DEFECT000235578	**Technical Severity**: High
Summary: CUP Port present CU-Busy on one path and never sending CU-End to clear busy	
Symptom: CUP can fail to send CUE when SAK is expecting it. A Logical Path will quit sending chains, if it does not receive a CUE, when expecting it. The CUP is still responsive, but the host is waiting for the CUE.	
Feature: FICON	**Function**: Ficud
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000237437	**Technical Severity**: High
Summary: In an HA cluster environment, Re-key operations can't be started on vendor storage LUNs.	
Symptom: In an HA cluster environment, Re-key operations can't be started on vendor storage LUNs.	
Feature: Data Security	**Function**: Disk Encryption
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.1.1_enc	**Service Request ID**: 358551

Defect ID: DEFECT000238428	**Technical Severity**: High
Summary: WWN card FRU replacement procedure not sending async reports to FICON host.	
Symptom: Customers won't know when a WWN card has been removed.	
Feature: FICON	**Function**: Ficud
Probability: High	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000239126	**Technical Severity**: High
Summary: ASIC Interrupt handling fix – single defect to address issues found while attempting to respond to ASIC generated interrupts.	
Symptom: Customer may experice high CPU load and unexpected blade errors.	
Feature: Field Escalation	**Function**: ASIC Driver
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.1.0	

Defect ID: DEFECT000239668	**Technical Severity**: High
Summary: Unable to configure port(s) using configdownload	
Symptom: Unable to configure ports using configdownload if the ports are not not physically present in the switch.	
Feature: Infrastructure	**Function**: Config Download
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000240443	**Technical Severity**: High
Summary: After a fosconfig --enable vf, followed by a fosconfig --disable vf, customer is unable to log in via telnet or serial port to the Brocade DCX. All accounts receive the error "Cannot assign valid AD at the login session".	
Symptom: After running fosconfig --enable vf and letting the switch reboot, logged back in, stepped through the configure command to validate the new options against the documentation (nothing was changed). Then ran fosconfig --disable vf, and let the switch reboot. When attempting to log back into the switch, received the error "Cannot assign valid AD at the login session", and was disconnected.	
Workaround: Don't change VF mode until dual CP chassis is in sync	
Feature: Infrastructure	**Function**: VF infrastructure
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	**Service Request ID**: 365207

Defect ID: DEFECT000237196	**Technical Severity**: Medium
Summary: Unable to activate a new PDCM Matrix with Webtools	
Symptom: When activating saved PDCM Matrix from ‘Activate CUP Port Connectivity Configuration’ dialog in WebTools, with “Active=Save Mode” checked, WebTools displays error.	
Workaround: Activate the same PDCM Matrix from WebTools, with “Active=Save Mode” checked from ‘Edit CUP Port Connectivity Configuration’ window.	
Feature: FICON	**Function**: Ficud
Probability: High	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000237675	**Technical Severity**: Medium
Summary: Onboard Administrator used to manage Brocade 5480 is not able to read the switchname	
Symptom: TheOnboard Administrator will not display the switchname	
Workaround: Switch name can be displayed from FOS CLI command - switchname	
Feature: Embedded Platform Services	**Function**: Bulova
Probability: High	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000237918	**Technical Severity**: Medium
Summary: Beta regression: switchdisable & switchenable on Base switch with active E2E I/O, all frames dropped one one direction of bi-directional I/O afterwards and never recovered itself, monitorred sts_tx_timeout counter keep increased on E-EX port.	
Symptom: Edge to Edge data frames not recovered after switchdisable & switchenable on a Base switch.	
Workaround: stop I/O and restart I/O may help to recover.	
Feature: 8G ASIC Driver	**Function**: C2 ASIC driver
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000238392	**Technical Severity**: Medium
Summary: EVA4400 controllers crashing when servers with qlogic hba's have access to encrypted luns are rebooted	
Symptom: EVA4400 controllers crashing when servers with vendor HBAs have access to encrypted luns are rebooted.	
Feature: FC Services	**Function**: Name Server
Probability: High	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000238526	**Technical Severity**: Medium
Summary: Unexpected software call traceback error messages are being displayed on the console.	
Symptom: Console occasionally displays call traceback messages. End of printout has Software Verify errors.	
Feature: Pluto Platform Services	**Function**: Platform Services
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000239664	**Technical Severity**: Medium
Summary: Even with Lossless DLS feature enabled, there may be a few frame drops when a trunk port comes online	
Symptom: Even with Lossless DLS feature enabled, there may be a few frame drops when a trunk port comes online	
Feature: 8G ASIC Driver	**Function**: Routing
Probability: Low	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Defect ID: DEFECT000239822	**Technical Severity**: Medium
Summary: supportsave: USB: interactive mode stores all files illegally in switch root directory instead of the USB device	
Symptom: When using supportsave in interactive mode with a USB stick selected for storage, the supportsave files are stored in the switch root directory and not the USB device. This can also result in compact flash storage overflow.	
Feature: RAS	**Function**: FFDC/Supportsave
Probability: Medium	**Risk of Fix**: Low
Found in Release: FOS6.2.0	

Closed with Code Change Defects in Fabric OS v6.2.0a

This section lists defects closed in Fabric OS v6.2.0a. Note that when a workaround to an issue is available, it is provided.

Defect ID: DEFECT000238444	**Technical Severity:** High
Summary: In B2E routed environment, when user executes Pathinfo command in BB querying for xlate domain, the switch may panic.	
Feature: FC Services	**Function:** FSPF
Risk of Fix: Low	
Reported In Release: FOS6.2.0	

Defect ID:	DEFECT000225796	**Technical Severity:**	Medium
Summary:	Brocade switch is sending RSCN event Qualifier as 0x20 for FOS 6.1.x and 0x08 FOS v6.1.0g and FOS v6.2.0.		
Symptom:	Some OS/HBA combinations take down FC link when N_port generated RSCN are delivered by switch with 0x08 or 0x20 as event qualifier. Revert back to FOS v6.0 way of sending as 0x0.		
Feature:	FOS Software	**Function:**	Fabric Services
Risk of Fix:	Medium	**Probability:**	High
Reported In Release:	FOS 6.1.0_8e	**Service Request ID:**	332317

Defect ID:	DEFECT000237341	**Technical Severity:**	Medium
Summary:	When upgrading a switch with an FC10-6 blade from FOS v6.1 to v6.2, the standby CP may go into a rolling reboot.		
Feature:	8G Platform Services	**Function:**	Routing
Risk of Fix:	Low		
Reported In Release:	FOS6.2.0		

Defect ID:	DEFECT000238215	**Technical Severity:**	Medium
Summary:	In routed environment, after upgrading to v6.2.0, command 'fcrfabricshow' displays ex-port # as 0		
Feature:	8G FCR	**Function:**	FCR CLI
Risk of Fix:	Low		
Reported In Release:	FOS6.2.0		

Defect ID:	DEFECT000230294	**Technical Severity:**	High
Summary:	Out of Memory condition on switch occurred, due to memory leak in nsd process.		
Symptom:	Mixed fabric running in Interopmode2, switch hafailover/hareboot occurs due to out of memory occurrence.		
Feature:	FC Services	Function:	Name Server
Risk of Fix:	Low		
Reported In Release:	FOS6.2.0		

Defect ID: DEFECT000239111	**Technical Severity:** High
Summary: Switches leaking memory slowly over extended period while being managed by DCFM.	
Feature: Mgmt Embedded - SNMP	**Function:** Switch Admin
Risk of Fix: Low	
Reported In Release: FOS6.2.0	

Appendix: Additional Considerations for FICON Environments

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

FICON Configurations

Cascading of directors and switches is limited to one hop for a FICON environment with the following exceptions:

- Up to three hops are supported for FCIP with a pair of Brocade 7500 switches used for FCIP extension. The following FCIP configuration is supported for DCX:

  "DCX – ICL-DCX –7500 – 7500 -   DCX – ICL- DCX".

- The DCX Backbone with Inter Chassis Links (ICLs) consists of two cascading domains. These ICLs should be considered the same as very high speed ISL trunks.

  The fabric security attributes must be configured and 2-byte link addressing must be used whenever a channel connected to one chassis needs to reach a control unit connected to a port on the other chassis. The ICLs provide ample bandwidth in a controlled environment which allows the hop to be disregarded from a service perspective. Therefore, the following configuration is supported:

  "DCX – ICL-DCX – ISL- DCX – ICL- DCX".

  When configuring this way, care should be taken with other ISL connections to avoid multi-hop conditions. System architects can treat a pair of DCX directors connected via ICLs as a single entity.

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

Area	Comments
8Gb/sec Links	When changing from an existing synchronization method using IDLEs to run FICON at 8 Gb/sec, Brocade recommends using ARBff (fill words). Information on this configuration can be found in the *Important Notes* section of this document under *8G Link Initialization & Fill Words*. This is a disruptive change. IBM FICON channels and devices configured for 8Gb/sec should set the switch/director to ARBff using command portcfgfillword
Firmware Downloads	It is recommended to stop I/O traffic that is going through fixed port switches (4100, 4900, 5100, 5300, 7500) prior to downloading firmware in a fabric running FOS version less than 6.2.0g since this may cause the ports to be reset resulting in generation of IFCCs. This is resolved in fabrics running 6.2.0g or later.
Firmware Downloads	Replacement of a CP card in the Brocade 48000 may cause disruption of I/O traffic. Brocade recommends that the CP be replaced during a scheduled downtime to prevent disruption in FICON environments.
Manageability	Brocade recommends using DCFM for managing the following environments: pure FOS based fabrics, mixed FOS and M-EOS fabrics where the FOS switch/director is the seed switch. EFCM is the recommended management software for M-EOS only fabrics when a FOS switch or director can not be used as the seed switch.
Manageability	In a mixed fabric environment, an M-EOS switch must be principal switch if the fabric is in Interopmode 2 (McDATA Fabric Mode) .

Manageability	FOS 6.2.0e and later support Port Fencing configuration for switches through the Command Line Interface (CLI). Assistance from service support should be enlisted to enable this feature. With DCFM 10.1.x Port Fencing can be done through DCFM menu.
Manageability	It is suggested that default parameters for Port Fencing be used to avoid taking ports down for normal fabric events.
Manageability	Firmware download is executed sequentially if ECFM is used for downloading code to FOS switches.
Manageability	As a "Best Practice" for deploying FOS switches/directors into a FICON environment, verify the FOS version shipped with the most current FOS recommendation. It is recommended to update all FOS switch/directors to the same FOS levels for production.
Manageability	Fabric administrators should check the Link Incident Report (LIR - Port x "FF") for any failed component incidents in switches/directors as these are not reported to z/OS through the CUP.
Manageability	Node descriptor information is obtained through the Element Manager instead of the fabric wide node descriptor list when using DCFM to manage M-EOS switches.
Manageability	When DCFM 10.1.3 is used for managing TI zones, zone propagations may experience a timeout. This issue will be resolved in later FOS releases.
Optics	Brocade recommends using 50 micron multimode fiber optic cabling rated at 2000 MHz-km (OM3 fiber) for connecting to 8 Gb/sec short wavelength (SX) small form factor pluggable optics (SFPs). Other 50 micron and 62.5 micron multimode fiber may be used as an alternative, but distance limitations may exist.
Serviceability	If a port card is removed from a system with Virtual Fabrics enabled and replaced by a port card with fewer ports, the missing ports will not be able to be removed which results in configuration change problems. To prevent this, the ports should be removed from the Logical Switch they are assigned to prior to the card being removed.
Serviceability	Performance of optical links depends upon the cleanliness of the cables and connectors, especially at 8 Gb/sec or higher speeds. Consult with your switch and cable vendors for proper cable maintainence.
Traffic Isolation Zones	Enable Lossless DLS when activating Traffic Isolation (TI) Zones to avoid any traffic disruption.
Traffic Isolation Zones	Beginning with the FOS 6.0.2e release, Traffic Isolation (TI) Zoning with FICON now supports enabling or disabling of the failover option. Assistance from service support should be sought before attempting to enable this feature.
Virtual Fabrics	Virtual Fabrics (VF) is supported in FICON environments beginning with FOS 6.2.0e. Execute fosconfig --show to check if VF is enabled. Using DCFM to disable VF can result in empty message boxes resulting in confusion.