IronWare Software Release R07.2.00a for Brocade FESX, FSX, SX, FCX, FGS, FGS-STK, FLS, FLS-STK, and FWS Switches

Release Notes v1.0

November 15, 2010

Document History

Document Title	Summary of Changes	Publication Date
IronWare Software Release 07.2.00a for Brocade FESX, FSX, SX, FCX, FGS, FGS-STK, FLS, FLS-STK, and FWS Switches Release Notes v1.0	New document	November 2010

Contents

Supported devices

This software release applies to the following Brocade FastIron switches:

- FastIron X Series:
  - FastIron Edge Switch X Series (FESX)
  - FastIron Edge Switch X Series Expanded (FESXE)
  - FastIron SuperX Switch (FSX)
  - FastIron SX 800, 1600, and 1600-ANR
- FastIron GS (FGS) and FastIron LS (FLS)
- FastIron GS-STK (FGS-STK) and FastIron LS-STK (FLS-STK)
- FastIron CX (FCX)
- FastIron WS (FWS)

Summary of enhancements

This section lists the enhancements in software release 07.2.00 and later.

Summary of enhancements in R07.2.00a

There are no enhancements in release 07.2.00a. Release 07.2.00a contains software fixes; however, software release 07.2.00a has a different Interprocessor Communications (IPC) version for FCX, FGS-STK, and FLS-STK. Refer to the section "Upgrading the software" on page 33 for details.

Summary of enhancements in FSX R07.2.00

Table 1 lists the enhancements in software release 07.2.00 for FESX, FSX, and SX devices.

Table 1 Enhancements in FSX R07.2.00

Feature	Description	Refer to the *FastIron Configuration Guide*, section entitled...
New hardware - SX-FI48GPP interface module with 2:1 oversubscription and PoE+ support	48-port 10/100/1000 Mbps (RJ45) Ethernet POE interface module	Refer to the *Brocade FastIron X Series Chassis Hardware Installation Guide*
POE+ support on the SX-FI48GPP interface module	The SX-FI48GPP interface module supports Power over Ethernet (POE) and Power over Ethernet Plus (POE+), compliant with the standards described in the IEEE 802.3af and 802.3at specifications for delivering in-line power.	Configuring Power Over Ethernet

Feature	Description	Refer to the *FastIron Configuration Guide*, section entitled...
Hitless management: • Layer 2 and Layer 3 Hitless failover • Layer 3 Hitless OS upgrade	This release adds support for Layer 2 and Layer 3 hitless failover as well as Layer 3 hitless OS upgrade. Releases prior to 07.2.00a support Layer 2 hitless OS upgrade only. These high-availability features enable the standby management module to take over the active role with no loss of data traffic during a software failure, hardware failure, or operating system upgrade.	Hitless management on the FSX 800 and FSX 1600
OSPF graceful restart	OSPF graceful restart is a high-availability routing feature that minimizes disruption in traffic forwarding, diminishes route flapping, and provides continuous service during a system restart, switchover, failover, or hitless OS upgrade. During such events, routes remain available between devices.	OSPF graceful restart
BGP4 graceful restart	BGP4 graceful restart is a high-availability routing feature that minimizes disruption in traffic forwarding, diminishes route flapping, and provides continuous service during a system restart, switchover, failover, or hitless OS upgrade. During such events, routes remain available between devices.	BGP4 graceful restart
DHCP Server support in the Layer 2 and full Layer 3 software image	FastIron devices can be configured to operate as a DHCP server. A DHCP server allocates IP addresses for specified periods of time (known as leases) and manages the IP address pools and the binding (leased addresses) database.	DHCP Server
DHCP Client-Based Auto-update	Enables Layer 2 and base Layer 3 devices to automatically obtain leased IP addresses through a DHCP server, negotiate address lease renewal, and obtain flash image and configuration files.	DHCP Client-Based Auto-Configuration and Flash image update
DHCP Server with IP helper	DHCP server and IP helper address are supported together on the same port.	DHCP Server and Configuring an IP helper address
Ability to disable DHCP Server on the management port	You can configure the DHCP Server to silently discard DHCP client requests received on the management port.	Disabling DHCP Server on the management port

Feature	Description	Refer to the *FastIron Configuration Guide*, section entitled...
QoS for the SX-FI48GPP module	The SX-FI48GPP module supports QoS for packets in an oversubscribed environment. QoS configuration and functionality is different on the SX-FI48GPP compared to other interface modules.	Configuring Quality of Service
Buffer profiles on the SX-FI48GPP module	To increase or decrease the queue depth limits for a port on the SX-FI48GPP module, you must configure a buffer profile that defines the queue depth limits, and apply the buffer profile to the port.	Dynamic buffer allocation for QoS priorities for FastIron X Series devices
IGMP snooping querier enhancement	You can use the **show ip multicast vlan** command to display the querier information for a VLAN. This command displays the VLAN interface status and if there is any other querier present with the lowest IP address.	Displaying querier information
Flexible VE numbering	When configuring virtual routing interfaces on a device, you can now specify a number from 1 through 4095. However, the total number of virtual routing interfaces that are configured must not exceed the system-max limit of 512.	Assigning an IP address to a virtual interface
New SNMP MIBs	SNMP MIB support has been added for the following features: • Dynamic ARP Inspection • DHCP snooping • IP Source Guard • EMCP	IronWare MIB Reference Guide

Summary of enhancements in FCX R07.2.00

Table 2 lists the enhancements in software release 07.2.00 for FCX devices.

Table 2 Enhancements in FCX R07.2.00

Feature	Description	See the *FastIron Configuration Guide*, section entitled...
Hitless stacking: • Layer 2 and Layer 3 Hitless switchover • Layer 2 and Layer 3 Hitless failover	Hitless stacking is a high-availability feature set that enables the Standby Controller to take over the active role with sub-second or no loss of data traffic during a hardware or software failure.	FCX hitless stacking
OSPF graceful restart	OSPF graceful restart is a high-availability routing feature that minimizes disruption in traffic forwarding, diminishes route flapping, and provides continuous service during a system restart, switchover, or failover. During such events, routes remain available between devices.	OSPF graceful restart
BGP4 graceful restart	BGP4 graceful restart is a high-availability routing feature that minimizes disruption in traffic forwarding, diminishes route flapping, and provides continuous service during a system restart, switchover, or failover. During such events, routes remain available between devices.	BGP4 graceful restart
Private VLANs on tagged ports	For FCX devices only, this release supports private VLANs on tagged ports. Previous releases support private VLANs on untagged ports only.	Configuring private VLAN
IGMP snooping querier enhancement	You can use the **show ip multicast vlan** command to display the querier information for a VLAN. This command displays the VLAN interface status and if there is any other querier present with the lowest IP address.	Displaying querier information
Flexible VE numbering	When configuring virtual routing interfaces on a device, you can now specify a number from 1 through 4095. However, the total number of virtual routing interfaces that are configured must not exceed the system-max limit of 512.	Assigning an IP address to a virtual interface

Feature	Description	See the *FastIron Configuration Guide*, section entitled...
DHCP Server with IP helper	DHCP server and IP helper address are supported together on the same port.	DHCP Server and Configuring an IP helper address
Ability to disable DHCP Server on the management port	You can configure the DHCP Server to silently discard DHCP client requests received on the management port.	Disabling DHCP Server on the management port
New SNMP MIBs	SNMP MIB support has been added for the following features: • Dynamic ARP Inspection • DHCP snooping • IP Source Guard • EMCP	IronWare MIB Reference Guide

Summary of enhancements in FGS R07.2.00

Table 3 lists the enhancements in software release 07.2.00 for FGS, FGS-STK, FLS, FLS-STK, and FWS devices.

Table 3 Enhancements in FGS R07.2.00

Feature	Description	See the *FastIron Configuration Guide*, section entitled...
IGMP snooping querier enhancement	You can use the **show ip multicast vlan** command to display the querier information for a VLAN. This command displays the VLAN interface status and if there is any other querier present with the lowest IP address.	Displaying querier information
Flexible VE numbering	When configuring virtual routing interfaces on a device, you can now specify a number from 1 through 4095. However, the total number of virtual routing interfaces that are configured must not exceed the system-max limit of 512.	Assigning an IP address to a virtual interface
DHCP Server with IP helper	DHCP server and IP helper address are supported together on the same port.	DHCP Server and Configuring an IP helper address

Feature	Description	See the *FastIron Configuration Guide*, section entitled...
New SNMP MIBs	SNMP MIB support has been added for the following features: • Dynamic ARP Inspection • DHCP snooping • IP Source Guard • EMCP	IronWare MIB Reference Guide

CLI differences in IronWare release R07.2.00a

The *FastIron Configuration Guide* and the section "Configuration notes and feature limitations" in these release notes describe the CLI differences in IronWare release 07.2.00a compared with earlier releases. No CLI commands have been deprecated for this release.

Configuration notes and feature limitations

This section contains configuration notes and describes some feature limitations in this release.

48-port 10/100/1000 Mbps Ethernet POE (SX-FI48GPP) interface module limitations

The following configuration limitations apply to this module:

- Q-in-Q and SAV (VLAN stacking) are not supported on this module.
- For systems with this module and IPv4 or IPv6 interface modules or management modules with user ports:
    - GRE tunnels and IPv6 over IPv4 tunnels are not supported.

      NOTE: If the SX-FI48GPP module is inadvertently inserted in a system that has IPv4 or IPv6 interface modules, or a management module with user ports, existing tunnels will be taken down immediately. To recover, you must physically remove the module that caused the mix-and-match condition, then disable and re-enable the tunnel interfaces.

    - Legacy ports and 48 Gbps copper ports cannot be members of the same trunk.
- Virtual cable testing (CLI command **phy cable-diag tdr**) is not supported on the SX-FI48GPP module in software release 07.2.00.

New limit for IPv4 system-max ip-cache

Starting in software release 07.2.00, for FCX and FastIron X Series devices, the maximum value for system-max ip-cache (IPv4) is reduced from 256000 to 32768. When you upgrade to release 07.2.00 and if your configuration has an ip-cache value greater than 32768, it will be automatically reduced to 32768.

IronView Network Manager (INM) limitation

INM version 3.3.01 and later does not support download of the 07.2.00 router images (SXL07200.bin and SXR07200.bin). Also, with INM version 03.3.01 and later, it will take approximately six minutes to upload the Layer 2 switch image (SXS07200.bin) from the FastIron switch to a TFTP server.

ACL Statistics on FGS, FLS, and FWS devices

The FGS, FLS, and FWS do not support the use of traffic policies for ACL statistics only (CLI command **traffic-policy** <*TPD name*> **count**). However, these models do support the use of traffic policies for ACL statistics together with rate limiting traffic policies. For more information, refer to "Enabling ACL statistics with rate limiting traffic policies" in the *FastIron Configuration Guide*.

IGMP Snooping feature limitation on FESX, FSX, and SX devices

High CPU utilization will occur when IGMP Snooping and PIM/DVMRP routing are enabled simultaneously on a FESX, FSX, or SX router. With IGMP Snooping and PIM/DVMRP Routing enabled simultaneously on a given system, IP Multicast data packets received in the snooping VLAN(s) will be forwarded to client ports via the hardware; however, copies of these packets will also be received and dropped by the CPU.

Show interface brief command output

If a port name is longer than 5 characters, the port name will be truncated in the output of the **show interface brief** command.

ICMP redirect messages

In software release 07.2.00, ICMP redirect messages are *disabled* by default, whereas in prior releases, ICMP redirect messages are *enabled* by default.

- If ICMP redirect messages were enabled prior to upgrading to release 07.2.00, you will need to re-enable this feature after upgrading to 07.2.00. To do so, enter the **ip icmp redirect** command at the global CONFIG level of the CLI.
- If ICMP redirect messages were disabled prior to upgrading to release 07.2.00, the configuration (**no ip icmp redirect)** will be removed from the configuration file after upgrading to 07.2.00, since this feature is now disabled by default. In this case, ICMP redirect messages will not be sent and no further action is required.

Enabling and Disabling DHCP-client service on FSX Base Layer 3 devices

By default, DHCP-client service is enabled. If the DHCP-Server is connected to an interface on a FSX Base L3 device, the interface is assigned a leased IP address. To disable DHCP-client service on an interface on a FSX Base L3 device, and assign a new IP address, enter the following commands.

Note: In release 07.2.00, the DHCP-client service feature can only be enabled or disabled on a FSX Base L3 device by performing the following steps.

---

1. Remove the dynamic IP address assigned to the interface. For example, enter a command such as the following.

```
FastIron(config-if-e1000-3/1)# no ip address 10.10.10.10/24
```

Syntax: no ip address <ip-address>

2. Assign a new IP address to the interface. For example, enter a command such as the following.

```
FastIron(config-if-e1000-3/1)# ip address 10.10.2.1/24
```

Syntax: ip address <ip-address>

3. To save the configuration, enter the **write memory** command on the CLI as displayed in the following example.

```
FastIron(config)# write memory
FastIron(config)# end
```

4. Reload the FSX Base L3 device by entering the following command:

```
FastIron# reload
```

The DHCP-client service feature is now removed from the interface.

To enable DHCP-client service on an interface on a FSX Base L3 device when a static IP address is assigned to the interface, enter the following commands.

1. Remove the static IP address assigned to the interface. For example, enter a command such as the following.

```
FastIron(config-if-e1000-3/1)# no ip address 10.10.10.10/24
```

Syntax: no ip address <ip-address>

2. To save the configuration, enter the **write memory** command on the CLI as displayed in the following example.

```
FastIron(config)# write memory
FastIron(config)# end
```

3. Reload the FSX Base L3 device by entering the following command:

```
FastIron# reload
```

Once the device has reloaded, the DHCP-client service will start up and a new dynamic IP address is assigned to the interface. The DHCP-client service feature is now enabled on the interface.

Note regarding Telnet and Internet Explorer 7

The Telnet function in Web management does not work with Internet Explorer version 7.0.5730. The system goes to "telnet://10.43.43.145" page when the user clicks web/general system configuration/ (telnet) in Internet Explorer version 7.0.5730. This is a known issue for Internet Explorer. To work around this issue, you must download and install a patch for IE 7. To do so, go to http://www.lib.ttu.edu.tw/file/IE7_telnet.reg.

Note regarding US-Cert advisory 120541

In order to address the SSL and TLS vulnerability issue discussed in US-Cert advisory 120541, the Web server re-negotiation feature has been disabled in this release so that SSL re-negotiation requests *will not* be honored by the Brocade IP device Web server.

Based on Cert advisory 120541, the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols are vulnerable to Man-In-The-Middle (MITM) attacks. Vulnerability is in the way SSL and TLS protocols allow re-negotiation requests, which may allow a MITM to inject arbitrary requests into an application HTTP protocol stream. This could result in a situation where the MITM may be able to harm the Brocade IP device through the Web Management interface.

For more information regarding Cert advisory 120541, refer to the following links:

http://extendedsubset.com/?p=8

http://www.links.org/?p=780

http://www.links.org/?p=786

http://www.links.org/?p=789

http://blogs.iss.net/archive/sslmitmiscsrf.html

http://www.ietf.org/mail-archive/web/tls/current/msg03948.html

https://bugzilla.redhat.com/show_bug.cgi?id=533125

http://lists.gnu.org/archive/html/gnutls-devel/2009-11/msg00014.html

http://cvs.openssl.org/chngview?cn=18790

http://www.links.org/files/no-renegotiation-2.patch

http://blog.zoller.lu/2009/11/new-sslv3-tls-vulnerability-mitm.html

https://svn.resiprocate.org/rep/ietf-drafts/ekr/draft-rescorla-tls-renegotiate.txt

http://www.educatedguesswork.org/2009/11/understanding_the_tls_renegoti.html

Feature support

These release notes include a list of supported features in IronWare software for the FastIron devices supported in this release. For more information about supported features, refer to the manuals listed in Additional resources.

Supported management features

Table 4 lists the supported management features. These features are supported in the Layer 2, base Layer 3, edge Layer 3, and full Layer 3 software images.

Table 4 Supported management features

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
802.1X accounting	Yes	Yes	Yes	Yes	Yes
AAA support for console commands	Yes	No	No	No	Yes
Access Control Lists (ACLs) for controlling management access	Yes	Yes	Yes	Yes	Yes
Alias command	Yes	Yes	Yes	Yes	Yes
Combined DSCP and internal marking in one ACL rule	Yes	No	No	No	No
Single source address for the following packet types: • Telnet • TFTP • Syslog • SNTP • TACACS/TACACS+ • RADIUS • SSH • SNMP	Yes	No	No	No	No
DHCP client-based auto-configuration	No	Yes	Yes	Yes	Yes
DHCP server	Yes	Yes	Yes	Yes	Yes
Disabling TFTP access	Yes	No	No	No	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
Hitless management: • Hitless switchover • Hitless failover • Hitless OS upgrade	Yes (FSX 800 and FSX 1600 only)	No	No	No	See next line item
Hitless stacking management: • Hitless stacking switchover • Hitless stacking failover	No	No	No	No	Yes
IronView Network Manager (optional standalone and HP OpenView GUI)	Yes	Yes	Yes	Yes	Yes
Remote monitoring (RMON)	Yes	Yes	Yes	Yes	Yes
Retaining Syslog messages after a soft reboot	Yes	Yes	Yes	Yes	Yes
sFlow support for IPv6 packets	Yes	Yes	Yes	Yes	Yes
sFlow version 2	Yes	Yes	Yes	Yes	Yes
sFlow version 5 (default)	Yes	Yes	Yes	Yes	Yes
Industry-standard Command Line Interface (CLI), including support for: • Serial and Telnet access • Alias command • On-line help • Command completion • Scroll control • Line editing • Searching and filtering output • Special characters	Yes	Yes	Yes	Yes	Yes
Show log on all terminals	Yes	Yes	Yes	Yes	Yes
SNMP v1, v2, v3	Yes	Yes	Yes	Yes	Yes
SNMP V3 traps	Yes	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
Specifying the maximum number of entries allowed in the RMON Control Table	Yes	No	No	No	Yes
Specifying which IP address will be included in a DHCP/BOOTP reply packet	Yes	No	No	No	Yes
Traffic counters for outbound traffic	Yes	No	No	No	No
Web-based GUI	Yes	Yes	Yes	Yes	Yes
Web-based management HTTPS/SSL	Yes	Yes	Yes	Yes	Yes

Supported security features

Table 5 lists the supported security features. These features are supported in the Layer 2, base Layer 3, edge Layer 3, and full Layer 3 software images.

Table 5 Supported security features

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
802.1X port security	Yes	Yes	Yes	Yes	Yes
802.1X authentication RADIUS timeout action	Yes	Yes	Yes	Yes	Yes
802.1X dynamic assignment for ACL, MAC filter, and VLAN	Yes	Yes	Yes	Yes	Yes
Access Control Lists (ACLs) for filtering transit traffic • Support for inbound ACLs only. Outbound ACLs are not supported.	Yes	Yes	Yes	Yes	Yes
Address locking (for MAC addresses)	Yes	Yes	Yes	Yes	Yes
AES Encryption for SNMP v3	Yes	Yes	Yes	Yes	Yes
AES Encryption for SSH v2	Yes	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
Authentication, Authorization and Accounting (AAA): • RADIUS • TACACS/TACACS+	Yes	Yes	Yes	Yes	Yes
Denial of Service (DoS) attack protection: • Smurf (ICMP) attacks • TCP SYN attacks	Yes	Yes	Yes	Yes	Yes
DHCP Snooping	Yes	Yes	Yes	Yes	Yes
Dynamic ARP Inspection	Yes	Yes	Yes	Yes	Yes
EAP Pass-through Support	Yes	Yes	Yes	Yes	Yes
HTTPS	Yes	Yes	Yes	Yes	Yes
IP Source Guard	Yes	Yes	Yes	Yes	Yes
Local passwords	Yes	Yes	Yes	Yes	Yes
MAC address filter override of 802.1X	Yes	Yes	Yes	Yes	Yes
MAC address filtering (filtering on source and destination MAC addresses)	Yes	Yes	Yes	Yes	Yes
Ability to disable MAC learning	Yes	Yes	Yes	Yes	Yes
Flow-based MAC address learning	Yes	No	No	No	Yes
MAC port security	Yes	Yes	Yes	Yes	Yes
Multi-device port authentication	Yes	Yes	Yes	Yes	Yes
Support for Multi-Device Port Authentication together with:					
• Dynamic VLAN assignment	Yes	Yes	Yes	Yes	Yes
• Dynamic ACLs	Yes	Yes	Yes	Yes	Yes
• 802.1X	Yes	Yes	Yes	Yes	Yes
• Dynamic ARP inspection with dynamic ACLs	Yes	No	No	No	No

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
• DHCP snooping with dynamic ACLs	Yes	No	No	No	No
• Denial of Service (DoS) attack protection	Yes	No	No	No	Yes
• Source guard protection	Yes	Yes	Yes	Yes	Yes
• ACL-per-port-per-VLAN	Yes	Yes	Yes	Yes	Yes
Multi-device port authentication password override	Yes	Yes	Yes	Yes	Yes
Multi-device port authentication RADIUS timeout action	Yes	Yes	Yes	Yes	Yes
Secure Copy (SCP)	Yes	Yes	Yes	Yes	Yes
Secure Shell (SSH) v2	Yes	Yes	Yes	Yes	Yes
Packet filtering on TCP Flags	No	Yes	Yes	Yes	Yes
DHCP Relay Agent information (DHCP Option 82)	Yes	Yes	Yes	Yes	Yes
Web Authentication	Yes	Yes	Yes	Yes	Yes

Supported system-level features

Table 6 lists the supported system-level features. These features are supported in the Layer 2, base Layer 3, edge Layer 3, and full Layer 3 software images.

Table 6 Supported system-level features

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
10/100/1000 port speed	Yes	Yes	Yes	Yes	Yes
16,000 MAC addresses per switch (FastIron devices)	Yes	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
32,000 MAC addresses per switch	Yes	No	No	No	Yes
ACL-based mirroring	Yes	Yes	Yes	Yes	Yes
ACL-based fixed rate limiting	Yes	Yes	Yes	Yes	Yes
ACL-based adaptive rate limiting	Yes	No	No	No	Yes
ACL filtering based on VLAN membership or VE port membership	Yes	Yes	Yes	Yes	Yes
ACL logging of denied packets (IPv4)	Yes	Yes	Yes	Yes	Yes
ACL statistics	Yes	Yes	Yes	Yes	Yes
ACLs to filter ARP packets	Yes	Yes	Yes	Yes	Yes
Auto MDI/MDIX detection	Yes	Yes	Yes	Yes	Yes
Auto-negotiation	Yes	Yes	Yes	Yes	Yes
Automatic removal of Dynamic VLAN for 802.1X ports	Yes	Yes	Yes	Yes	Yes
Automatic removal of Dynamic VLAN for MAC authenticated ports	Yes	No	No	No	No
Byte-based broadcast, multicast, and unknown-unicast rate limits	Yes	No	No	No	No
Packet-based broadcast, multicast, and unknown-unicast rate limits	Yes	Yes	Yes	Yes	Yes
DiffServ support	Yes	Yes	Yes	Yes	Yes
Digital Optical Monitoring	Yes	Yes	Yes	Yes	Yes
Displaying interface names in Syslog messages	Yes	Yes	Yes	Yes	Yes
Displaying TCP and UDP port numbers in Syslog messages	Yes	Yes	Yes	Yes	Yes
Dynamic buffer allocation for QoS priorities	Yes	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
Flow control: • Responds to flow control packets, but does not generate them	Yes	Yes	Yes	Yes	Yes
Inbound rate limiting (port-based fixed rate limiting on inbound ports)	Yes	Yes	Yes	Yes	Yes
Foundry Discovery Protocol (FDP) / Cisco Discovery Protocol (CDP)	Yes	Yes	Yes	Yes	Yes
Generic buffer profile	No	Yes	Yes	Yes	Yes
Layer 2 hitless switchover and Layer 2 hitless failover **NOTE:** For details about this feature, refer to the *Brocade FastIron X Series Chassis Hardware Installation Guide*	Yes FSX 800 and FSX 1600 only	No	No	No	No
LLDP	Yes	Yes	Yes	Yes	Yes
LLDP-MED	Yes	Yes	Yes	Yes	Yes
MAC address filter-based mirroring	No	Yes	Yes	Yes	Yes
Multi-port static MAC address	Yes	Yes	Yes	Yes	Yes
Multiple Syslog server logging (up to six Syslog servers)	Yes	Yes	Yes	Yes	Yes
Outbound rate limiting (port-based and port- and priority-based rate limiting on outbound ports)	No	Yes	Yes	Yes	No
Outbound rate shaping	Yes	No	No	No	Yes
Path MTU Discovery	Yes	No	No	No	Yes
Port flap dampening	Yes	Yes	Yes	Yes	Yes
Port mirroring and monitoring (mirroring of both inbound and outbound traffic on individual ports)	Yes	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
Power over Ethernet (POE)	Yes (POE-enabled Interface modules with POE power supply)	Yes (FGS-POE only)	Yes (FGS-POE-STK only)	Yes (FWS-POE and FWS-G-POE only)	Yes (FCX-S-HPOE only)
Power over Ethernet (POE)+ with 2:1 oversubscription	Yes (SX-FI48GPP module only)	No	No	No	Yes (FCX-S-HPOE only)
Priority mapping using ACLs	Yes	Yes	Yes	Yes	Yes
Protected link groups	Yes	Yes	Yes	Yes	Yes
Layer 2 stacking rapid failover and switchover	No	No	No	No	Yes
Static MAC entries with option to set traffic priority	Yes	Yes	Yes	Yes	Yes
Symmetric flow control • Can transmit and receive 802.1x PAUSE frames	No	No	No	No	Yes
System time using a Simple Network Time Protocol (SNTP) server or local system counter	Yes	Yes	Yes	Yes	Yes
Virtual Cable Testing (VCT) technology	Yes	Yes	Yes	Yes	Yes

Supported Layer 2 features

Layer 2 software images include all of the management, security, and system-level features listed in the previous tables, plus the features listed in Table 7.

Table 7 Supported Layer 2 features

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
802.1D Spanning Tree Support: • Enhanced IronSpan support includes Fast Port Span, Fast Uplink Span, and Single-instance Span • Up to 254 spanning tree instances for VLANs	Yes	Yes	Yes	Yes	Yes
802.1p Quality of Service (QoS): • Strict Priority (SP) • Weighted Round Robin (WRR) • Combined SP and WRR • 8 priority queues	Yes	Yes	Yes	Yes	Yes
802.1s Multiple Spanning Tree	Yes	Yes	Yes	Yes	Yes
802.1W Rapid Spanning Tree (RSTP)	Yes	Yes	Yes	Yes	Yes
802.3ad link aggregation (dynamic trunk groups)	Yes	Yes	Yes	Yes	Yes
ACL-based rate limiting QoS	Yes	Yes	Yes	Yes	Yes
BPDU Guard	Yes	Yes	Yes	Yes	Yes
Dynamic Host Configuration Protocol (DHCP) Assist	Yes	Yes	Yes	Yes	Yes
IGMP v1/v2 Snooping Global	Yes	Yes	Yes	Yes	Yes
IGMP v3 Snooping Global	Yes (*,G)	Yes (S,G)	Yes (S,G)	Yes (S,G)	Yes (S,G)
IGMP v1/v2/v3 Snooping per VLAN	Yes	Yes	Yes	Yes	Yes
IGMP v2/v3 Fast Leave (membership tracking)	Yes	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
Interpacket Gap (IPG) adjustment	Yes	Yes	Yes	Yes	Yes
IP MTU (individual port setting)	Yes	No	No	No	Yes
Jumbo frames: • Up to 10240 bytes, or • Up to 10232 bytes in an IronStack	Yes	Yes	Yes	Yes	Yes
Link Aggregation Control Protocol (LACP)	Yes	Yes	Yes	Yes	Yes
Link Fault Signaling (LFS) for 10G	Yes	Yes	Yes	Yes	Yes
MAC-Based VLANs, including support for dynamic MAC-Based VLAN activation	No	Yes	Yes	Yes	Yes
Metro Ring Protocol 1 (MRP 1)	Yes	Yes	Yes	Yes	Yes
Metro Ring Protocol 2 (MRP 2)	Yes	Yes	No	Yes	Yes
Extended MRP ring IDs from 1 – 1023	Yes	No	No	No	Yes
MLD Snooping V1/V2: • MLD V1/V2 snooping (global and local) • MLD fast leave for V1 • MLD tracking and fast leave for V2 • Static MLD and IGMP groups with support for proxy	Yes	Yes	Yes	Yes	Yes
Multicast static group traffic filtering (for snooping scenarios)	No	Yes	Yes	Yes	Yes
PIM-SM V2 Snooping	Yes	Yes	Yes	Yes	Yes
PVST/PVST+ compatibility	Yes	Yes	Yes	Yes	Yes
PVRST+ compatibility	Yes	Yes	Yes	Yes	Yes
Remote Fault Notification (RFN) for 1 G fiber	Yes	Yes	Yes	Yes	Yes
Root Guard	Yes	Yes	Yes	Yes	Yes
Single link LACP	Yes	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
Super Aggregated VLANs	Yes	Yes	Yes	Yes	Yes
Trunk groups: • Trunk threshold for static trunk groups • Flexible trunk group membership • Option to include Layer 2 in trunk hash calculation (FGS, FLS, FWS only)	Yes	Yes	Yes	Yes	Yes
Topology groups	Yes	Yes	Yes	Yes	Yes
Uni-directional Link Detection (UDLD) (Link keepalive)	Yes	Yes	Yes	Yes	Yes
Uplink Ports within a Port-Based VLAN	Yes	Yes	Yes	Yes	Yes
VLAN Support: • 4096 maximum VLANs • 802.1Q with tagging • 802.1Q-in-Q tagging • Dual-mode VLANs • GVRP • Port-based VLANs • Protocol VLANs (AppleTalk, IPv4, dynamic IPv6, and IPX • Layer 3 Subnet VLANs (Appletalk, IP subnet network, and IPX) • VLAN groups • Private VLANs	Yes	Yes	Yes	Yes	Yes
VLAN-based mirroring	No	Yes	Yes	Yes	Yes
VoIP Autoconfiguration and CDP	Yes	Yes	Yes	Yes	Yes
Virtual Switch Redundancy Protocol (VSRP)	Yes	Yes	Yes	Yes	Yes
VSRP-Aware security features	Yes	Yes	Yes	Yes	Yes
VSRP and MRP signaling	Yes	Yes	Yes	Yes	Yes
VSRP Fast Start	Yes	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
VSRP timer scaling	Yes	Yes	Yes	Yes	Yes

Supported base Layer 3 features

Base Layer 3 software images include all of the management, security, system, and Layer 2 features listed in the previous tables, plus the features listed in Table 8.

NOTE: FCX devices will not contain a base Layer 3 image. The features in this table will be supported on the full Layer 3 image for these devices.

Table 8 Supported base Layer 3 features

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
BootP/DHCP Relay	Yes	Yes	Yes	Yes	Yes
Equal Cost Multi Path (ECMP) load sharing	Yes	Yes	Yes	Yes	Yes
IP helper	Yes	Yes	Yes	Yes	Yes
RIP V1 and V2 (advertising only)	Yes	Yes	Yes	Yes	Yes
Routing for directly connected IP subnets	Yes	Yes	Yes	Yes	Yes
Static IP routing	Yes	Yes	Yes	Yes	Yes
Virtual Interfaces (up to 512)	Yes	Yes	Yes	Yes	Yes
Virtual Router Redundancy Protocol (VRRP)	Yes	Yes	Yes	Yes	Yes
VRRP timer scaling	Yes	Yes	Yes	Yes	Yes

Supported edge Layer 3 features

Edge Layer 3 software images include all of the management, security, system, Layer 2, and base Layer 3 features listed in the previous tables, plus the features shown in Table 9.

NOTE: Edge Layer 3 images are supported in the FastIron (hardware) models listed in Table 9. These features are also supported with software-based licensing. For details, refer to the chapter "Software-based Licensing" in the *FastIron Configuration Guide*.

Table 9 Supported edge Layer 3 features

Category and description	FGS-EPREM FLS-EPREM FWS-EPREM FWSG-EPREM
OSPF V2 (IPv4)	Yes
Full RIP V1 and V2	Yes
Route-only support (Global configuration level only)	Yes
Route redistribution	Yes
1020 routes in hardware maximum	Yes
VRRP-E	Yes

Supported full Layer 3 features

Full Layer 3 software images include all of the management, security, system, Layer 2, base Layer 3 and edge Layer 3 features listed in the previous tables, plus the features listed in Table 10 .

NOTE: Full Layer 3 features are supported in the FastIron (hardware) models listed in Table 10. These features are also supported with software-based licensing. For details, refer to the chapter "Software-based Licensing" in the *FastIron Configuration Guide*.

Table 10 Supported full Layer 3 features

Category and description	FESX-PREM FSX-PREM FSX 800-PREM FSX 1600-PREM	FCX
Active host routes	Yes (6,000)	Yes (16,000)
Anycast RP	Yes	No
BGP4 graceful restart	Yes (FSX 800 and FSX 1600 only)	Yes (ADV models in a stack)
BGP4	Yes	Yes (ADV models)
Distance Vector Multicast Routing Protocol (DVMRP) V2 (RFC 1075)	Yes	No
Internet Group Management Protocol (IGMP) V1, V2, and V3 (for multicast routing scenarios)	Yes	Yes
ICMP Redirect messages	Yes	Yes
IGMP V3 fast leave (for routing)	Yes	Yes
IPv4 point-to-point GRE IP tunnels	Yes (IPv6 devices only)	No
IPv6 Layer 3 forwarding[1]	Yes	No
IPv6 over IPv4 tunnels in hardware[1]	Yes	No

Category and description	FESX-PREM FSX-PREM FSX 800-PREM FSX 1600-PREM	FCX
IPv6 Redistribution[1]	Yes	No
IPv6 Static Routes[1]	Yes	No
Multiprotocol Source Discovery Protocol (MSDP)	Yes	No
OSPF graceful restart	Yes (FSX 800 and FSX 1600 only)	Yes (FCX models in a stack)
OSPF V2	Yes	Yes
OSPF V3 (IPv6)[1]	Yes	No
Protocol Independent Multicast Dense mode (PIM-DM) V1 (draft-ietf-pim-dm-05) and V2 (draft-ietf-pim-v2-dm-03)	Yes	Yes
Protocol Independent Multicast Sparse mode (PIM-SM) V2 (RFC 2362)	Yes	Yes
PIM passive	Yes	Yes
Policy-Based Routing (PBR)	Yes	Yes
RIPng (IPv6)[1]	Yes	No
Route-only support (Global CONFIG level and Interface level)	Yes	Yes
Route redistribution (including BGP4)	Yes	Yes (BGP4 supported on ADV models only)

[1] This feature requires IPv6-series hardware and a valid software license. For details, refer to the chapter "Software-based Licensing" in the *FastIron Configuration Guide*.

Category and description	FESX-PREM FSX-PREM FSX 800-PREM FSX 1600-PREM	FCX
Routes in hardware maximum: • FESX4 – up to 128K routes • FESX6 – up to 256K routes • FESX6-E – up to 512K routes • FSX – up to 256K routes • FCX – up to 16K routes	Yes	Yes
Static ARP entries	Yes (up to 6,000)	Yes (up to 1,000)
VRRP-E	Yes	Yes
VRRP-E slow start timer	Yes	Yes
VRRP-E timer scale	Yes	Yes

Supported IPv6 management features

Table 11 shows the IPV6 management features that are supported in Brocade devices that can be configured as an IPv6 host in an IPv6 network, and in devices that support IPv6 routing.

Table 11 Supported IPv6 management features

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
Link-Local IPv6 Address	Yes	Yes	Yes	Yes	Yes
IPv6 Access List (management ACLs)	Yes	Yes	Yes	Yes	Yes
IPv6 copy	Yes	Yes	Yes	Yes	Yes
IPv6 ncopy	Yes	Yes	Yes	Yes	Yes
IPv6 debug	Yes	Yes	Yes	Yes	Yes
IPv6 ping	Yes	Yes	Yes	Yes	Yes
IPv6 traceroute	Yes	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
DNS server name resolution	Yes	Yes	Yes	Yes	Yes
HTTP/HTTPS	Yes	Yes	Yes	Yes	Yes
Logging (Syslog)	Yes	Yes	Yes	Yes	Yes
RADIUS	Yes	Yes	Yes	Yes	Yes
SCP	Yes	Yes	Yes	Yes	Yes
SSH	Yes	Yes	Yes	Yes	Yes
SNMP	Yes	Yes	Yes	Yes	Yes
SNMP traps	Yes	Yes	Yes	Yes	Yes
SNTP	Yes	Yes	Yes	Yes	Yes
TACACS/TACACS+	Yes	Yes	Yes	Yes	Yes
Telnet	Yes	Yes	Yes	Yes	Yes
TFTP	Yes	Yes	Yes	Yes	Yes

Unsupported features

Table 12 lists the features that are not supported on the FastIron devices. If required, these features are available on other Brocade devices.

Table 12 Unsupported features

System-level features not supported
• ACL logging of permitted packets
• Broadcast and multicast MAC filters
• Outbound ACLs
Layer 2 features not supported
• SuperSpan

System-level features not supported
• VLAN-based priority
Layer 3 features not supported
• AppleTalk routing
• BGP4+
• Foundry Standby Router Protocol (FSRP)
• IPv6 Multicast Routing
• IPX routing
• IS-IS
• Multiprotocol Border Gateway Protocol (MBGP)
• Multiprotocol Label Switching (MPLS)
• Network Address Translation (NAT)

Software image files for IronWare release R07.2.00a

Table 13 lists the software image files that are available for IronWare Release 07.2.00a.

Table 13 Software image files

Device	Boot Image	Flash Image
FESX FSX FSX 800 FSX 1600	SXZ07200.bin	SXS07200a.bin (Layer 2) or SXL07200a.bin (base Layer 3) or SXR07200a.bin (full Layer 3)
FGS FLS FWS	FGZ05000.bin	FGS07200a.bin (Layer 2) or FGSL07200a.bin (base Layer 3) or FGSR07200a.bin (edge Layer 3)
FGS-STK FLS-STK	FGZ05000.bin	FGS07200a.bin (Layer 2) or FGSL07200a.bin (base Layer 3)
FCX	GRZ07100.bin	FCXS07200a.bin (Layer 2) or FCXR07200a.bin (Layer 3)

Factory pre-loaded software

Table 14 lists the software that is factory-loaded into the primary and secondary flash areas on the device.

Table 14 Factory pre-loaded software

Model	Software Images	
	Primary Flash	Secondary Flash
FESX FSX FSX 800 FSX 1600	Layer 2	Base Layer 3
FESX PREM FSX PREM FSX 800 PREM FSX 1600 PREM	Full Layer 3	Layer 2

Model	Software Images	
	Primary Flash	Secondary Flash
FGS FGS-STK FLS FLS-STK FWS	Layer 2	Base Layer 3
FGS EPREM FLS EPREM FWS EPREM	Edge Layer 3	Layer 2
FCX	Layer 2	Layer 3

Upgrading the software

Use the procedures in this section to upgrade the software.

Important notes about upgrading or downgrading the software

NOTE: For other important notes that may apply when upgrading or downgrading the software, refer to Configuration notes and feature limitations on page 10.

Note the following when upgrading to software release 07.2.00a:

- Software release 07.2.00a has a different Interprocessor Communications (IPC) version for FCX, FGS-STK, and FLS-STK devices. Units in a stack must have the same IPC version in order to communicate. Therefore, when upgrading from release 07.2.00 or earlier to 07.2.00a, you must first download the 07.200a image to every unit in the stack, before reloading the entire stack. Otherwise the stack cannot be built and will not operate. After downloading the image to every unit in the stack, enter the **show flash** command at any level of the CLI to ensure that every unit in the stack has the correct image.
- To upgrade an FWS device running software version 04.3.00 to version 07.2.00, you must first upgrade to release 04.3.02 before upgrading to 07.2.00. For instructions on how to upgrade to release 04.3.02, see the 04.3.02 release notes.
- To upgrade FGS standalone devices from software release 04.3.02 to version 07.2.00 with the intent of forming a stack, first upgrade the units individually (in standalone mode) without connecting the stacking cables. After upgrading all of the FGS units, you can then connect the stacking cables.
- If FGS-STK or FLS-STK devices are upgraded from software release 04.3.00 non-stacking mode to release 07.2.00 stacking mode, these devices may lose some port-related functions. If you are upgrading from a pre-stacking release to a stacking release, refer to "Converting from a pre-stacking image to a stacking image" in the *FastIron Configuration Guide*.

Note the following when downgrading from software release 07.2.00a:

- FCX-F devices require software release 06.1.00 or later.
- If software-based licensing is in effect on the device and the software is downgraded to pre-release 07.1.00, software-based licensing will not be supported.
- If FCX units In an IronStack are downgraded from software release 07.2.00 to release 06.0.00, in some instances, the units may not be able to form a stack. This will occur if there is a mismatch of BGP capability within the stack (i.e., some units support it and others do not). If you encounter this problem, contact Brocade Technical Support for assistance.
- For FCX units, the 10G module name differs in software release 07.2.00 compared to releases 07.0.01b and 07.0.01c. Therefore, if an FCX is downgraded from software release 07.2.00 to release 07.0.01b or 07.0.01c, the stacking port configuration will be lost and the unit will not be able to join the stack.
- If FGS-STK or FLS-STK units in an IronStack are downgraded from software release 07.2.00 to release 04.3.00, these units may lose some port-related functions since 04.3.00 does not support stacking. The same issue applies when FGS or FLS (standalone) devices that use stack-unit ID 2 or greater are downgraded from release 07.2.00 to 04.3.00. This will occur because the default non-stacked port numbering scheme in release 4.3.00 and earlier is **0**/*x*/*x*, versus the new non-stacked port numbering scheme in 7.0 which is **1**/*x*/*x*. After downgrading from release 7.0.01b to 4.3.00 or earlier, all configuration items relating to port numbers will be invalid and will need to be reprogrammed in the switch.

Upgrading the software to the new release

This section describes how to upgrade the software to run release 07.2.00a.

Upgrading the boot code

To upgrade the boot code, perform the following steps.

1. Place the new boot code on a TFTP server to which the Brocade device has access.
2. Copy the boot code from the TFTP server into flash memory. To do so, enter a command such as the following at the Privileged EXEC level of the CLI.

   copy tftp flash <*ip-addr*> <*image-file-name*> **bootrom**

   You should see output similar to the following.

```
FWS648POE Router# Flash Memory Write (8192 bytes per
dot).........................
(Boot Flash Update)Erase.........Write.............
TFTP to Flash Done
```

NOTE: Brocade recommends that you use the **copy tftp flash** command to copy the boot code to the device during a maintenance window. Attempting to do so during normal networking operations may cause disruption to the network.

3. Verify that the code has been successfully copied by entering the following command at any level of the CLI.

   show flash

   The output will display the compressed boot ROM code size and the boot code version.

4. Upgrade the flash code as instructed in the following section.

Upgrading the flash code

To upgrade the flash code, perform the following steps.

1. Place the new flash code on a TFTP server to which the Brocade device has access.
2. Copy the flash code from the TFTP server into flash memory. To do so, use the **copy** command at the Privileged EXEC level of the CLI.

   copy tftp flash <*ip-addr*> <*image-file-name*> **primary | secondary**

   You should see output similar to the following.

```
FWS648POE Router# Flash Memory Write (8192 bytes per dot)
.......................
.....................................................................
.....................................................................
.....
TFTP to Flash Done
```

3. Verify that the flash code has been successfully copied by entering the following command at any level of the CLI.

   NOTE: For units in an IronStack, when upgrading from one major release to another (for example, from software release 07.1.00 to 07.2.00), make sure that every unit has the same code. If you reload the stack while units are running different code versions, the units will not be able to communicate.

   show flash

   If the flash code version is correct, go to step 4, otherwise, go back to step 1.

4. Once you have completed the upgrade, you must reboot the device to complete the upgrade process. Use one of the following commands:

   - **reload** (this command boots from the default boot source, which is the primary flash area by default)
   - **boot system flash primary** | **secondary**

   A confirmation step may occur after a boot system flash primary/secondary command is entered and gives an administrator the opportunity to make last minute changes or corrections before performing a reload. The example below shows the confirmation step.

```
FWS648POE Router# boot system flash primary
Are you sure? (enter 'Y' or 'N'): y
```

5. For FGS-STK and FLS-STK devices equipped with upgraded memory DIMMs, EEPROM, or both, if you encounter a problem after reloading the software, make sure the device has the correct boot code version and the following (if applicable) are installed correctly:

   - EEPROM
   - Memory DIMM

   NOTE: If the stacking EEPROM is missing or is not installed correctly, or if you have installed the wrong EEPROM, you will see an error message on the console. For details, see the *FastIron Configuration Guide.*

6. For devices in an IronStack, make sure all devices are running the same software image. See Confirming software versions (IronStack devices) in the next section.

Confirming software versions (IronStack devices)

All units in an IronStack must be running the same software image. To confirm this, check the software version on all devices that you want to add to your IronStack. Upgrade any units that are running older versions of the software before you build your stack.

1. Telnet, SSH, or connect to any of the console ports in the stack.
2. Enter the **show version** command. Output similar to the following is displayed.

   The output displays the software version and label that is currently installed on the devices. To check if you have the correct software version, refer to the section "*Software* image files for IronWare release R07.2.00a" on page32.

```
FCX Router# show version
Copyright (c) 1996-2010 Brocade Communications Systems, Inc.
    UNIT 1: compiled on Jun 17 2010 at 18:20:53 labeled as FCXS07200
                (4211643 bytes) from Primary automation/FCXS07200.bin
        SW: Version 07.2.00T7f1
    UNIT 2: compiled on Jun 17 2010 at 18:20:53 labeled as FCXS07200
                (4211643 bytes) from Primary automation/FCXS07200.bin
        SW: Version 07.2.00T7f1
    UNIT 3: compiled on Jun 17 2010 at 18:20:53 labeled as FCXS07200
                (4211643 bytes) from Primary automation/FCXS07200.bin
        SW: Version 07.2.00T7f1
    UNIT 4: compiled on Jun 17 2010 at 18:20:53 labeled as FCXS07200
                (4211643 bytes) from Primary automation/FCXS07200.bin
        SW: Version 07.2.00T7f1
  Boot-Monitor Image size = 369292, Version:07.1.00T7f5 (grz07100)
HW: Stackable FCX648-PREM (PROM-TYPE FCX-ADV-U)
```

NOTE: If any unit in the IronStack is running an incorrect version of the software, the unit will appear as non-operational. You must install the correct software version on that unit for it to operate properly in the stack. For more information, refer to "Copying the flash image to a stack unit from the Active Controller" in the *FastIron Configuration Guide*.

Technical support

Contact your switch supplier for the 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
    - Device model
    - Software release version
    - Error numbers and messages received
    - Detailed description of the problem, including the switch or network behavior immediately following the problem, and specific questions
    - Description of any troubleshooting steps already performed, with the results
2. Switch Serial Number

Getting help or reporting errors

Web access

The Knowledge Portal (KP) contains the latest version of this guide and other user guides for the product. You can also report errors on the KP.

Log in to my.Brocade.com, click the Product Documentation tab, then click on the link to the Knowledge Portal (KP) to find the latest document.

While in the Knowledger Portal, you can click on Cases > Create a New Ticket to report an error. Make sure you specify the document title in the ticket description.

E-mail and telephone access

Go to http://www.brocade.com/services-support/index.page for the latest e-mail and telephone contact information.

Additional resources

For more information about the products supported in this software release, refer to the following publications.

Document Title	Contents
FastIron Configuration Guide	Provides configuration procedures for system-level features, enterprise routing protocols, and security features.
Brocade FastIron GS and GS-STK Compact Switch Hardware Installation Guide	Describes the hardware as shipped. Provides installation instructions, hardware maintenance procedures, hardware specifications, and

Document Title	Contents
Brocade FastIron LS and LS-STK Compact Switch Hardware Installation Guide *Brocade FastIron WS Hardware Installation Guide* *Brocade FastIron CX Hardware Installation Guide* *Brocade FastIron X Series Chassis Hardware Installation Guide* *Brocade FastIron Compact Switch Hardware Installation Guide (for FESX switches)*	compliance information.
IronWare MIB Reference	Simple Network Management Protocol (SNMP) Management Information Base (MIB) objects.
FastIron CX Web Management Interface User Guide	Describes the Graphical User Interface (GUI) and procedures for monitoring and configuring various features of the FastIron CX series switches using the GUI.

Defects

This section lists the closed and opened defects in this release.

Customer reported defects closed with code in Release R07.2.00a

The following table lists the customer defects fixed in this release.

Defect ID: DEFECT000310725	**Technical Severity:** Medium
Summary: Deploying an ACL that has already been imported in INM fails.	
Symptom: After Importing the ACLs that are configured on the device using INM, re-deploying the same ACLs to the device fails.	
Probability: High	
Feature: FCX ACL	**Function:** ACL(all aspects of ACLs - IPV4)
Reported In Release: FI 07.1.00	**Service Request ID:** 00256462

Defect ID: DEFECT000318336	**Technical Severity:** Medium
Summary: When 'any-icmp-type' keyword is in ACL, INM shows SQL error while trying to import an ACL.	
Probability: Medium	
Feature: FCX Network Management	**Function:** INM Support
Reported In Release: FI 07.1.00	**Service Request ID:** 254263

Defect ID: DEFECT000320839	**Technical Severity:** High
Summary: In a two unit stack with Trunk, the recovery following a stack fail over may experience a transient traffic loss.	
Symptom: In a two unit stack, the recovery following a stack fail over may experience a transient traffic loss.	
Workaround: In a two unit stack after the stack fail over, increase the stack priority of the newly elected Active controller to the highest priority in the stack before the previous active controller rejoins the stack.	
Probability: High	
Feature: FCX Platform Specific features	**Function:** system bringup
Reported In Release: FI 07.2.00	

Defect ID: DEFECT000321502	**Technical Severity:** Medium
Summary: A prompt with the incorrect VIF appears when VRRP VRID is configured.	
Workaround: This is a display issue. You can ignore this safely.	
Probability: High	
Feature: SX Layer3 Control Protocols	**Function:** VRRP/VRRP-E and slow-start timer-

	VRRP-E timer scale
Reported In Release: FI 07.2.00	**Service Request ID:** 00264000

Defect ID: DEFECT000322232	**Technical Severity:** Critical
Summary: The switch may reload when the "qd-descriptor" command is removed from the configuration file.	
Symptom: The switch reloads.	
Workaround: Downgrade to 7.0.01c code.	
Probability: High	
Feature: FCX Layer1 features	**Function:** Dynamic buffer allocation
Reported In Release: FI 07.2.00	**Service Request ID:** 264521

Defect ID: DEFECT000322362	**Technical Severity:** Critical
Summary: When SSH DSA challenge-response (Public key) authentication is configured, you are logged in directly to privileged mode without entering a password.	
Symptom: When SSH DSA challenge-response authentication configured, the behavior is different between FESX devices running release 5100c & those running 7100a.	
Probability: High	
Feature: SX Management Functionality	**Function:** IPv4/V6 SSH Service
Reported In Release: FI 07.1.00	**Service Request ID:** 260815

Defect ID: DEFECT000322468	**Technical Severity:** Medium
Summary: The default value of "system-max ip-cache" is set to 10,000 instead of 32,768.	
Workaround: Before upgrading ot release 07.2.00, manually configure "system-max-ip-cache" to 32,768.	
Probability: Medium	
Feature: SX Platform Specific features	**Function:** system bringup
Reported In Release: FI 07.2.00	**Service Request ID:** 264798

Defect ID: DEFECT000325694	**Technical Severity:** High
Summary: SX1600 device may experience an unexpected reload when a module is hot inserted.	
Symptom: The router reloaded.	
Probability: High	
Feature: SX Platform Specific features	**Function:** HotSwap
Reported In Release: FI 07.2.00	**Service Request ID:** 263199

Customer reported defects closed with code in Release R07.2.00

The following table lists the customer defects fixed in this release.

Defect ID: DEFECT000274991	**Technical Severity:** Medium
Summary: DHCP snooping is not working when the interface has a permit ACL configured.	
Symptom: DHCP Snooping is not working.	
Probability: Medium	
Feature: SX ACL	**Function:** DHCP Snooping functionality
Reported In Release: FI 05.1.00	**Service Request ID:** 235477

Defect ID: DEFECT000275889	**Technical Severity:** Medium
Summary: A combo fiber port does not link up after speed-duplex configuration changes are made to the combo port.	
Symptom: Fiber combo port does not link up.	
Probability: High	
Feature: FCX Layer1 features	**Function:** link status - speed and duplex status
Reported In Release: FI FGS 04.3.02	**Service Request ID:** 239384

Defect ID: DEFECT000281635	**Technical Severity:** Medium
Summary: Dynamically changing the bridge priority of an STP bridge that is currently not the root bridge, may cause the bridge to assume the root role temporarily.	
Symptom: Dynamically changing the bridge priority of an STP bridge that is currently not the root bridge, may cause the bridge to assume the root role temporarily.	
Probability: High	
Feature: SX L2 Control	**Function:** Spanning Tree Protocols
Reported In Release: FI 04.2.00	**Service Request ID:** 241821

Defect ID: DEFECT000284904	**Technical Severity:** Medium
Summary: The router does not advertize Summary LSA when the area of a loopback interface is changed.	
Probability: Medium	
Feature: SX Layer3 Control Protocols	**Function:** OSPFV2 - IPV4
Reported In Release: FI 05.1.00	**Service Request ID:** 225995

Defect ID: DEFECT000285227	**Technical Severity:** Medium
Summary: Combo fiber port does not link up after speed-duplex configuration changes are made to the combo port.	
Feature: FCX Layer1 features	**Function:** link status - speed and duplex status
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000287375	**Technical Severity:** High

Summary: In the base Layer3 and Layer3 software, when sflow is enabled, packets with priority 1 that are destined to the CPU are dropped.	
Symptom: In the base Layer3 and Layer3 software, when sflow is enabled, packets with priority 1 that are destined to the CPU are dropped.	
Probability: Medium	
Feature: SX L2 Forwarding	**Function:** VLAN Manager
Reported In Release: FI 07.0.01	**Service Request ID:** 241991

Defect ID: DEFECT000288606	**Technical Severity:** Medium
Summary: With MSTP configured, adding and removing VLANs from the switch may cause brief packet loss.	
Symptom: There may be brief packet loss when adding a port to a VLAN running MSTP.	
Probability: Medium	
Feature: SX L2 Control	**Function:** Spanning Tree Protocols
Reported In Release: FI 04.1.00	**Service Request ID:** 237710

Defect ID: DEFECT000289865	**Technical Severity:** Medium
Summary: Wrong Fan Failed message is displayed for FWS648G-non POE.	
Symptom: Fan error messages seen.	
Probability: High	
Feature: FCX Platform Specific features	**Function:** Chassis/fan/power supplies/temperature sensors
Reported In Release: FI 07.0.01	**Service Request ID:** 246043

Defect ID: DEFECT000297038	**Technical Severity:** Medium
Summary: Some packets which need to be fragmented are getting delayed, causing packet loss.	
Symptom: Some packets which need to be fragmented are getting delayed, causing packet loss.	
Probability: Medium	
Feature: SX Layer 3 Forwarding - IPV4 and IPV6	**Function:** IP MTU & Fragmentation
Reported In Release: FI 05.1.00	**Service Request ID:** 245120

Defect ID: DEFECT000298345	**Technical Severity:** Medium
Summary: sflow does not work for stacked units for IPV6 sflow collector.	
Symptom: sflow does not work for FGS stacked units (stack unit 2 and more) if sflow collector is configured for IPv6.	
Probability: High	
Feature: FCX Network Management	**Function:** sFlow
Reported In Release: FI 07.0.01	**Service Request ID:** 247804

Defect ID: DEFECT000299696	**Technical Severity:** Medium
Summary: The router may reload when processing syslog messages at the same time a SSH or Telnet session is disconnected from the router.	
Symptom: The router reloads.	
Probability: Low	
Feature: SX Management Functionality	**Function:** IPv4/V6 SSH Service
Reported In Release: FI 04.1.00	

Defect ID: DEFECT000301723	**Technical Severity:** Critical
Summary: The router may become unresponsive when using the Web GUI to modify ports.	
Symptom: The router may become unresponsive when using the Web GUI to modify ports.	
Probability: High	
Feature: SX Management Functionality	**Function:** HTTPs/HTTP
Reported In Release: FI 07.0.01	**Service Request ID:** 251238

Defect ID: DEFECT000301729	**Technical Severity:** Medium
Summary: An error message may be seen when configuring the IPv6 MTU of 1266 or higher on IPv4 Tunnel interfaces.	
Symptom: IPv6 error message seen.	
Probability: High	
Feature: SX Layer 3 Forwarding - IPv4 and IPv6	**Function:** IP MTU & Fragmentation
Reported In Release: FI 07.0.00	**Service Request ID:** 00246171

Defect ID: DEFECT000301801	**Technical Severity:** Medium
Summary: “sh media" does not display the correct optic type.	
Symptom: “sh media" does not display the correct optic type.	
Probability: Medium	
Feature: FCX Layer1 features	**Function:** Digital Optical Monitoring
Reported In Release: FI 05.0.00	**Service Request ID:** 0242604

Defect ID: DEFECT000301950	**Technical Severity:** High
Summary: Access point advertisements may not be forwarded correctly.	
Symptom: Access point advertisements are not forwarded correctly.	
Probability: High	
Feature: SX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Data Forwarding
Reported In Release: FI 07.0.01	

Defect ID: DEFECT000301985	**Technical Severity:** Medium
Summary: In certain situations, replies to DNS queries are not acknowledged by the system.	
Feature: SX Network Management	**Function:** DNS
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000302157	**Technical Severity:** Medium
Summary: If the switch is configured for a single span, and it has ~200+ VLANs then the switch reloads once the "show span" command is entered.	
Symptom: The router reloads.	
Probability: Medium	
Feature: FCX L2 Control	**Function:** single spanning-tree
Reported In Release: FI 07.0.01	**Service Request ID:** 251502

Defect ID: DEFECT000302183	**Technical Severity:** Medium
Summary: The "CR" option is not correct for some commands.	
Symptom: "CR" option is not correct with the following commands: 1)With command “no ip address”. 2)With command “area 1 stub”.	
Probability: Medium	
Feature: FCX Management Functionality	**Function:** CLI and parser
Reported In Release: FI 07.0.01	**Service Request ID:** 251446

Defect ID: DEFECT000302360	**Technical Severity:** High
Summary: Some directly connected IP addresses are not reachable, even though ARP table shows the correct ARP entry.	
Symptom: Directly connected IP address are not reachable, even though ARP table shows the correct ARP entry.	
Probability: Medium	
Feature: SX Layer 3 Forwarding – Ipv4 and IPv6	**Function:** Host Networking stack (IPv4 and IPv6)
Reported In Release: FI 03.2.00	

Defect ID: DEFECT000302453	**Technical Severity:** Medium
Summary: With SSH enabled, the router may reload when reading an invalid memory location.	
Symptom: Router reload	
Probability: Low	
Feature: SX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Host Networking stack (IPV4 and IPV6)
Reported In Release: FI 05.1.00	**Service Request ID:** 251208

Defect ID: DEFECT000302583	**Technical Severity:** Medium
Summary: After issuing "copy flash flash ?" command, the switch does not display the correct output.	
Feature: FCX Management Functionality	**Function:** CLI and parser
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000302605	**Technical Severity:** Critical
Summary: If the default gateway of the switch is configured for a broadcast address, the switch may reload when receiving lots of large SNMP packets.	
Feature: FCX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Data Forwarding
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000302679	**Technical Severity:** Medium
Summary: Setting the time zone using SNMP will result in wrong time zone in the running config.	
Symptom: Changing the time zone value with snmpset results in a different time zone being shown in the running config. For example if you deploy a CST time zone (GMT-6) using snmpset then you will see GMT+1 on the device in the running config.	
Probability: High	
Feature: FCX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 07.0.01	**Service Request ID:** 251329

Defect ID: DEFECT000303729	**Technical Severity:** Medium
Summary: ACL logging is not working for members in a stack.	
Feature: FCX ACL	**Function:** ACL Accounting
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000303834	**Technical Severity:** Medium
Summary: Per-user IP ACLs on 802.1x does not work correctly.	
Workaround: Use Filter-ID attribute instead of Per-user IP ACLs.	
Probability: Medium	
Feature: FCX ACL	**Function:** 802.1x authentication
Reported In Release: FI 07.0.01	**Service Request ID:** 247590

Defect ID: DEFECT000303853	**Technical Severity:** High
Summary: Unable to configure VRRP in base layer 3 code.	
Feature: SX Layer3 Control Protocols	**Function:** VRRP/VRRP-E and slow-start timer-VRRP-E timer scale
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000304263	**Technical Severity:** Medium
Summary: UDP port 1027 is open to IPv6 on FESX	
Symptom: UDP port 1027 is open to IPv6 on FESX	
Probability: High	
Feature: SX Network Management	**Function:** TFTP Configuration- Software V4/V6
Reported In Release: FI 05.1.00	**Service Request ID:** 250941

Defect ID: DEFECT000304524	**Technical Severity:** High
Summary: The system may reload in a rare case of an invalid entry in the ARP table.	
Symptom: Router reload	
Probability: Low	
Feature: SX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Host Networking stack (IPV4 and IPV6)
Reported In Release: FI 07.0.01	**Service Request ID:** 253309

Defect ID: DEFECT000304625	**Technical Severity:** Critical
Summary: The router may reload when doing a SNMP MIB walk.	
Feature: SX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000305623	**Technical Severity:** Medium
Summary: CMD Port option not available on extended ACL range	
Symptom: Lines of ACL removed from configuration.	
Probability: High	
Feature: SX ACL	**Function:** ACL(all aspects of ACLs - IPV4)
Reported In Release: FI 07.0.00	**Service Request ID:** 254496

Defect ID: DEFECT000306417	**Technical Severity:** Medium
Summary: Show command output will sometimes hang or be truncated when parsing data from standby or member units of a stack.	
Feature: FCX Management Functionality	**Function:** CLI and parser
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000306952	**Technical Severity:** High
Summary: Ports are removed from the running VLAN configuration.	
Feature: FCX L2 Forwarding	**Function:** VLAN Manager
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000307116	**Technical Severity:** Critical
Summary: The FGS may reload when performing "write mem" when snmpv3 user profile is configured.	
Feature: FCX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000309028	**Technical Severity:** High
Summary: Policy Based Routing may not forward correctly after ARPs age out or new ARPs are learned.	
Feature: SX Layer 3 Forwarding - IPV4 and IPV6	**Function:** PBR
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000311241	**Technical Severity:** High
Summary: IPV6 management traffic is sent to an incorrect next hop.	
Symptom: Unable to establish an IPV6 management session to the switch.	
Probability: Low	
Feature: SX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Data Forwarding
Reported In Release: FI 05.1.00	**Service Request ID:** 241304

Defect ID: DEFECT000315402	**Technical Severity:** Medium
Summary: No syslog or SNMP trap is sent if an external RPS2-EIF goes down.	
Feature: SX Network Management	**Function:** SYSLOG
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000315930	**Technical Severity:** Medium
Summary: Change of MSTP root bridge priority may cause long network convergence.	
Feature: SX L2 Control	**Function:** 802.1s
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000316883	**Technical Severity:** Medium
Summary: Stack Master LED illuminates green even though it is running in standalone mode.	
Symptom: In FLS running software version 4.3.03 or later, the Stack Master LED always illuminates green even though it is running in standalone mode.	
Probability: High	
Feature: FCX Platform Specific features	**Function:** Chassis/fan/power supplies/temperature sensors
Reported In Release: FI FGS 04.3.03	**Service Request ID:** 259120

Defect ID: DEFECT000318038	**Technical Severity:** Medium
Summary: The switch may reload if you issue “no owner prio <pri>” command before you configure “owner”.	
Feature: SX Layer3 Control Protocols	**Function:** VRRP/VRRP-E and slow-start timer-VRRP-E timer scale
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000278649	**Technical Severity:** Medium
Summary: The command 'gig-default auto-gig' does not appear in the running configuration.	
Symptom: The command 'gig-default auto-gig' does not appear in the running configuration.	
Workaround: No. If the connected end with all ports are same Gigabit configuration, gig-default config in global level would be workaround.	
Probability: Medium	
Feature: SX Layer1 features	**Function:** link status - speed and duplex status
Reported In Release: FI 05.1.00	**Service Request ID:** 239173

Defect ID: DEFECT000301157	**Technical Severity:** High
Summary: sFlow is not sampling the traffic on the standby and member units on a FGS/FLS stack.	
Feature: FCX Network Management	**Function:** sFlow
Reported In Release: FI 07.2.00	

Defect ID: DEFECT000304374	**Technical Severity:** Medium
Summary: snAgGblDynMemUtil MIB object does not return the correct value.	
Feature: SX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 07.2.00	

Defect ID: DEFECT000309430	**Technical Severity:** High
Summary: The switch may run out of available memory when there is continual SNMP polling to the device.	
Symptom: Router reloaded.	
Probability: Medium	
Feature: SX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 07.0.01	**Service Request ID:** 259419

Defect ID: DEFECT000310242	**Technical Severity:** High
Summary: DHCPS: Released IP addresses are withheld from distribution if an ARP entry exists for that IP Address.	
Feature: FCX DHCP	**Function:** Server
Reported In Release: FI 07.2.00	

Defect ID: DEFECT000310243	**Technical Severity:** High
Summary: "Show ip dhcp-server flash" and "Show ip dhcp-server bind" does not use page-view.	
Feature: FCX DHCP	**Function:** Server
Reported In Release: FI 07.2.00	

Defect ID: DEFECT000310245	**Technical Severity:** High
Summary: When you have a server with 500+ clients active in the binding database, the command "show ip dhcp-server bind" and "show ip dhcp-server flash" outputs will be truncated after 474 lines, preventing an administrator from seeing all clients.	
Feature: FCX DHCP	**Function:** Server
Reported In Release: FI 07.2.00	

Defect ID: DEFECT000310246	**Technical Severity:** High
Summary: Summary: Address distribution is staring with .2 when the first ip address in the pool is .1	
Feature: FCX DHCP	**Function:** Server
Reported In Release: FI 07.2.00	

Customer reported defects closed without code in Release R07.2.00

The following table lists the customer defects fixed in this release.

Defect ID: DEFECT000284861	**Technical Severity:** Medium
Summary: FESX6 does not send ICMPv6 packet with 1452 byte.	
Symptom: FESX6 does not send ICMPv6 packet with 1452 byte.	
Reason Code: Already Fixed in Release	**Probability:** High
Feature: SX Layer 3 Forwarding - IPV4 and IPV6	**Function:** IP MTU & Fragmentation
Reported In Release: FI 05.0.00	**Service Request ID:** 246171

Open defects in Release R07.2.00

The following table lists the defects that are open in this release.

Defect ID: DEFECT000279513	**Technical Severity:** High
Summary: Sflow stops sampling after changing the configuration from a very large sampling rate to a very small sampling rate.	
Symptom: Sflow stops sampling after changing the configuration from a very large sampling rate to a very small sampling rate.	
Workaround: Perform "no sflow enable" and "sflow enable", then sflow starts to work again.	
Feature: FCX Network Management	**Function:** sFlow
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000319621	**Technical Severity:** High
Summary: On SX 800/1600 with zero port management module and only SX-48GC line modules, multicast over GRE tunnels is not functional.	
Symptom: On SX 800/1600 with zero port management module and only SX-48GC line modules, multicast over GRE tunnels is not functional.	
Workaround: This issue does not happen if the chassis has a non-zero port management module or at least one IPV6 or IPV4 line module.	
Feature: SX L2/L3 Multicast Features	**Function:** PIM Sparse
Reported In Release: FI 07.2.00	

Defect ID: DEFECT000266855	**Technical Severity:** Medium
Summary: When reloading a unit, ports on the unit keep "up" to the neighbors. If it is a cross-module trunk, connectivity can be affected.	
Symptom: The ip interface of the trunk is UP, the OSPF neighbor adjacency may timeout.	
Workaround: Do not configure a "dead-interval" less than the default 40 seconds, so that the Reload will be completed prior to the expiration of "dead-interval". Or even configure it larger than the default such as 60 seconds.	
Feature: FCX Layer3 Control Protocols	**Function:** OSPFV2 - IPV4
Reported In Release: FI 06.0.00	

Defect ID: DEFECT000269117	**Technical Severity:** Medium
Summary: lldpLocManAddrTable and lldpRemManAddrTable do not display correct IPv4 and IPv6 address.	
Symptom: lldpLocManAddrTable and lldpRemManAddrTable do not display correct IPv4 and IPv6 address.	
Feature: FCX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 07.0.00	**Probability:** Medium

Defect ID: DEFECT000275416	**Technical Severity:** Medium
Summary: Web Management does not force stack priority become after first reload. A second reload is required.	
Symptom: A second reload is required to change stack priority via web management	
Feature: FCX Network Management	**Function:** Web Management
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000278971	**Technical Severity:** Medium
Summary: After the ASBR creates a summary LSA, the more specific LSAs are not flushed from neighbor routers.	
Symptom: Customer creates summary for external routes to conserve system resource, but they will not achieve the goal until the LSAs are aged out on neighbor routers, and the maximum waiting time could be 1800 seconds. Since the ASBR which originates these LSA will not flush them with an age of 3600, a reload may be necessary.	
Workaround: May require a reload.	
Feature: FCX Layer3 Control Protocols	**Function:** OSPFV2 - IPV4
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000279775	**Technical Severity:** Medium
Summary: LLDP does not show syslog message under 'show log' command.	
Symptom: LLDP syslog message is not seen under system log file.	
Feature: FCX L2 Control	**Function:** LLDP
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000281430	**Technical Severity:** Medium
Summary: When a virtual-nei is present on an edge router, ECMP will not be effective for OSPF external routes.	
Symptom: When a virtual-nei is present on an edge router, ECMP will not be effective for OSPF external routes.	
Feature: FCX Layer3 Control Protocols	**Function:** OSPFV2 - IPV4
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000286397	**Technical Severity:** Medium
Summary: "no global-stp" is lost after a reload. No failover or switch-over.	
Symptom: After reloading the FCX unit, the command "no global-stp" is lost.	
Workaround: The user will have to reconfigure this command after a reload.	
Feature: FCX Management Functionality	**Function:** CLI and parser
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000288329	**Technical Severity:** Medium
Summary: BGP Route Reflector NEXT_HOP attribute in BGP update packet is overwritten to reflector's ip address instead of originator's ip address when reflecting iBGP route to another iBGP peers, if next-hop-self is configured toward those IBGP peers	
Symptom: BGP Route Reflector NEXT_HOP attribute in BGP update packet is overwritten to reflector's ip address instead of originator's ip address when reflecting iBGP route to another iBGP peers, if next-hop-self is configured toward those IBGP peers	
Feature: SX Layer3 Control Protocols	**Function:** BGP
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000288331	**Technical Severity:** Medium
Summary: Stacking: User-defined stacking-ports (on member units) may be overwritten after the stack is formed (though the master stacking ports are NOT)	
Symptom: Stacking: User-defined stacking-ports (on member units) may be overwritten after the stack is formed (though the master stacking ports are NOT)	
Feature: FCX Stacking	**Function:** stack-ports
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000289135	**Technical Severity:** Medium
Summary: Multicast traffic is duplicated at PIM Group RXer when traffic passes thru IGMP Proxy router.	
Symptom: Multicast traffic is duplicated at PIM Group RXer when traffic passes thru IGMP Proxy router. The multicast stream must traverse through the PIM IGMP Proxy router to reach the destination router for the bug to occur. So, if the PIM VE Group RXer port is located on the same router as the IGMP Proxy VE, then there is no issue.	
Workaround: A topology work-around is to configure IP multicast RXers, but not sources, at the edge of a network in an IGMP VLAN/VE. That is, configure the network so all IP multicast sources are directly connected to an IP multicast router enabled VE.	
Feature: FCX L2/L3 Multicast Features	**Function:** IGMP proxy in L3 multicast
Reported In Release: FI 07.1.00	**Probability:** High

Defect ID: DEFECT000296533	**Technical Severity:** Medium
Summary: Changing port flow control setting on the port (flow, no flow, flow neg-on) should flap link reset setting and update peer but it does not.	
Symptom: Changing port flow control setting on the port (flow, no flow, flow neg-on) should flap link reset setting and update peer but it does not.	
Workaround: Manual port up/down may be required	
Feature: FCX Layer1 features	**Function:** Symmetric Flow Control
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000296833	**Technical Severity:** Medium
Summary: Device will close down a telnet management session as soon as it receives a FIN even if output is pending.	
Symptom: Device will close down a telnet management session as soon as it receives a FIN even if output is pending.	
Feature: FCX Management Functionality	**Function:** IPV4/V6 Telnet Service
Service Request ID: 246740	
Reported In Release: FI 07.0.01	

Defect ID: DEFECT000298768	**Technical Severity:** Medium
Summary: Copying an image from the flash (primary or secondary) to an external tftp server takes longer time than previous versions.	
Symptom: Copying an image from the flash (primary or secondary) to an external tftp server takes longer time than previous versions. This issue does not have any impact when copying an image from the TFTP server to the system flash.	
Workaround: No workaround is available at this time.	
Feature: SX Network Management	**Function:** TFTP Configuration- Software V4/V6
Reported In Release: FI 07.2.00	**Probability:** High

Defect ID: DEFECT000309517	**Technical Severity:** Medium
Summary: Web management only allows ve configuration from 1 to 255.	
Symptom: User can only configure ve 1 to 255 from web management. Flexible ve configuration which allows ve numbering from 1 to 4095 using CLI is not available in web management.	
Workaround: User can use CLI to configure ve number other than 1 to 255.	
Feature: SX Network Management	**Function:** Web Management
Reported In Release: FI 07.2.00	**Probability:** Medium

Defect ID: DEFECT000309525	**Technical Severity:** Medium
Summary: DHCP discover packets are sent out the management interface even though there is an IP address configured for the management interface.	
Symptom: DHCP discover packets are sent out the management interface even though there is an IP address configured for the management interface. The source IP of the DHCP discover packets is the IP address configured for the management interface.	
Feature: SX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Host Networking stack (IPV4 and IPV6)
Reported In Release: FI 07.2.00	**Probability:** High

Defect ID: DEFECT000311921	**Technical Severity:** Medium
Summary: When trial license and permanent license are installed on the system, the trial license will never expire but keeps sending syslog messages.	
Symptom: Customer will see that license is going to expire for every one hour . This happens only when the valid trial license and permanent license are present on the box.	
Workaround: Delete trial license, when the permanent license is installed.	
Feature: FCX SW License	**Function:** Other
Reported In Release: FI 07.2.00	**Probability:** High

Defect ID: DEFECT000319339	**Technical Severity:** Medium
Summary: On FWS and FGS platforms, DHCP Snooping does not work with an ACL configured on the same port with multiple tagged VLANs	
Symptom: On the FWS and FGS platforms, if DHPC Snooping is configured on the same port for multiple tagged VLANs and an ACL is configured on that port or the port that the DHCP server is located on, then only the 1st DHCP client on that port will be added to the DHCP Snooping table.	
Workaround: There is no workaround if you want to use ACLs on ports that have this feature enabled. You will need to remove the ACL on the ports in order for DHCP Snooping to work properly.	
Feature: FCX ACL	**Function:** DHCP Snooping functionality
Reported In Release: FI 07.2.00	**Probability:** Medium

Defect ID: DEFECT000319853	**Technical Severity:** Medium
Summary: On FCX, IP source guard configured at interface level on tagged ports may impact DHCP snooping and DAI functionality configured on these VLANs.	
Symptom: On FCX, IP source guard configured at interface level on tagged ports may impact DHCP snooping and DAI functionality configured on these VLANs.	
Workaround: With acl-per-port-per-vlan enabled, configure IP source guard at the VLAN level for each port.	
Feature: FCX ACL	**Function:** DHCP Snooping functionality
Reported In Release: FI 07.2.00	**Probability:** Medium

Defect ID: DEFECT000320487	**Technical Severity:** Medium
Summary: FCX stack does not use the persistent MAC after a reload if hitless fail-over is disabled.	
Symptom: FCX stack does not use the persistent MAC after a reload if hitless fail-over is disabled.	
Workaround: Use 'stack mac' instead of 'persistent mac'.	
Feature: FCX Stacking	**Function:** Master-Standby election
Reported In Release: FI 07.2.00	

Defect ID: DEFECT000320773	**Technical Severity:** Medium
Summary: On Stacking Member Units, modifying an ACL while it is applied by 802.1x dynamic ACL clients will not be effective.	
Symptom: On Stacking Member Units, modifying an ACL while it is applied by 802.1x dynamic ACL clients will not be effective.	
Workaround: Do "clear dot1x mac-sessions" after applying the ACLs.	
Feature: FCX ACL	**Function:** 802.1x authentication
Reported In Release: FI 07.2.00	**Probability:** Medium