BROCADE

IronWare Software Release R07.2.02r

Release Notes v1.0

November 6, 2015

Document History

Document Title	Summary of Changes	Publication Date
IronWare Software Release 07.2.02r for Brocade FESX, SuperX, FSX, FCX, FGS, FGS-STK, FLS, FLS-STK, and FWS Switches Release Notes v1.0	New document	November 2015

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 (SuperX)
    - FastIron SX 800, 1600, and 1600-ANR (FSX or SX)
- 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 in IronWare release R07.2.02r

Release 07.2.02r contains software fixes. There are no enhancements in this release.

Summary of enhancements in IronWare release R07.2.02q

Release 07.2.02q contains software fixes. There are no enhancements in this release. This release supports only Brocade FESX, FSX, and FCX devices.

Summary of enhancements in IronWare release R07.2.02p

Release 07.2.02p contains software fixes. There are no enhancements in this release.

Summary of enhancements in IronWare release R07.2.02n

Release 07.2.02n contains software fixes. There are no enhancements in this release.

Summary of enhancements in IronWare release R07.2.02m

Release 07.2.02m contains software fixes. There are no enhancements in this release.

Summary of enhancements in IronWare release R07.2.02k

Release 07.2.02k contains software fixes. There are no enhancements in this release.

Summary of enhancements in IronWare release R07.2.02j

Release 07.2.02j contains software fixes. There are no enhancements in this release.

Summary of enhancements in IronWare release R07.2.02h

Release 07.2.02h contains software fixes. There are no enhancements in this release.

Summary of enhancements in IronWare release R07.2.02g

The following are the enhancements in R07.2.02g:

- SNTP with MD5 authentication
- SNTP Server Support per RFC 4330. The following commands are introduced with this feature:
    - sntp server-mode [use-local-clock [stratum <*stratum-number*>]] [authentication-key <*key-string*>]
    - show sntp server-mode
    - sntp broadcast client
    - sntp broadcast server

These enhancements are documented in the section Updates to SNTP feature.

Summary of enhancements in IronWare release R07.2.02f

There are no enhancements in software releases R07.2.02e – R07.2.02f

Configuration note:

When the Active FCX unit in a stack comes online after being offline, it is expected behavior that for a few seconds data packets sent to the static trunk port on this original Active unit will need to be retransmitted. In sensitive environments, it is recommended that link-keepalive be configured on any static trunk ports or dynamic trunk LACP be used instead of static trunk configuration.

Summary of enhancements in IronWare release R07.2.02

This section lists the enhancements in software release 07.2.02.

Summary of enhancements in FSX R07.2.02

Table 1 lists the enhancements in software release 07.2.02 for FESX, SuperX, and FSX devices.

Table 1 Enhancements in FSX R07.2.02

Feature	Description	Refer to the *FastIron Configuration Guide*, section entitled...
PoE firmware upgrade via CLI	You can install PoE firmware from the TFTP server on a FastIron switch with the CLI command.	"Installing PoE Firmware"
Hitless support for FSX 800 and FSX 1600 devices: • PBR • GRE Tunnels • IPv6 to IPv4 Tunnels	This release adds support for PBR, GRE, IPv6 to IPv4 Tunnels and PBR over GRE. Configured PBR, GRE, or IPv6 to IPv4 Tunnels will operate in a hitless manner on FSX 800 and FSX 1600 devices only.	"Hitless management on the FSX 800 and FSX 1600"

Feature	Description	Refer to the *FastIron Configuration Guide*, section entitled...
Multi-range VLANs	The multi-range VLAN feature allows you to use a single command to create and configure multiple VLANs.	"Multi-range VLAN"
DHCP Server	All FastIron devices can be configured to operate as a DHCP server. A DHCP server allocates IP addresses for a specified period of time (known as a lease) and manages the IP address pools and the binding (leased addresses) databases.	"DHCP Server"

New SNMP MIBs	SNMP MIB support has been added for the following features:
	• 802.1x authentication
	• Support for MIBs in RFC 2932, RFC 2933 and RFC 2934
	• Power Over Ethernet MIB with the following tables:
	  • snAgentPoeGbl
	  • snAgentPoeModuleTable
		IronWare MIB Reference Guide

Summary of enhancements in FCX R07.2.02

Table 2 lists the enhancements in software release 07.2.02 for FCX devices.

Table 2 Enhancements in FCX R07.2.02

Feature	Description	See the *FastIron Configuration Guide*, section entitled...
Fast Uplink Span	Fast Uplink Span transitions the forwarding of traffic to one of the redundant ports in the Fast Uplink Span group in one second bypassing listening and learning port states.	"Fast Uplink Span"
Hitless support for PBR	This release adds support for Hitless PBR on FCX devices.	"Configuring Rule-Based IP Access Control Lists (ACLs)"
Multi-range VLANs	The multi-range VLAN feature allows you to use a single command to create and configure multiple VLANs.	"Multi-range VLAN"

Feature	Description	See the *FastIron Configuration Guide*, section entitled...
PoE firmware upgrade via CLI	You can install PoE firmware from the TFTP server on a FastIron switch with the CLI command.	"Installing PoE Firmware"
Software-based licensing for BGP	To enable BGP4 with the **router BGP** command, a BGP license is required.	"Configuring BGP4 (IPv4)"
User-configurable buffer profile	This buffer profile is a simpler form of allocation of qd descriptors and qd buffers. This allows you to define a template of buffer allocations to be used on a per port basis on the devices.	"User-configurable buffer profiles on FLS, FGS and FCX"
User-configurable scheduler profile on FLS, FGS and FCX	The user-configurable scheduler profile is a template that defines either scheduling mechanism or schedule profile or both for egress queues.	"User-configurable scheduler profile on FLS, FGS and FCX"
DHCP Server	All FastIron devices can be configured to operate as a DHCP server. A DHCP server allocates IP addresses for a specified period of time (known as a lease) and manages the IP address pools and the binding (leased addresses) databases.	"DHCP Server"
New SNMP MIBs	SNMP MIB support has been added for the following features: • 802.1x authentication • Support for MIBs in RFC 2932, RFC 2933 and RFC 2934 • Power Over Ethernet MIB with the following table: • snAgentPoeUnitTable (stacking systems)	*IronWare MIB Reference Guide*

Summary of enhancements in FGS R07.2.02

Table 3 lists the enhancements in software release 07.2.02 for FGS, FGS-STK, FLS, FLS-STK, and FWS devices.

Table 3 Enhancements in FGS R07.2.02

Feature	Description	See the *FastIron Configuration Guide*, section entitled...
Fast Uplink Span	Fast Uplink Span transitions the forwarding of traffic to one of the redundant ports in the Fast Uplink Span group in one second bypassing listening and learning port states.	"Fast Uplink Span"
Multi-range VLANs	The multi-range VLAN feature allows you to use a single command to create and configure multiple VLANs.	"Multi-range VLAN"
DHCP Server	All 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"
New SNMP MIBs	SNMP MIB support has been added for the following features: • 802.1x authentication • Support for MIBs in RFC 2932, RFC 2933 and RFC 2934 • Power Over Ethernet MIB with the following table: • snAgentPoeUnitTable (stacking systems)	*IronWare MIB Reference Guide*
User-configurable buffer profile	This buffer profile is a simpler form of allocation of qd descriptors and qd buffers. This allows you to define a template of buffer allocations to be used on a per port basis on the devices.	"User-configurable buffer profiles on FLS, FGS and FCX"
User-configurable scheduler profile on FLS, FGS and FCX	The user-configurable scheduler profile is a template that defines either scheduling mechanism or schedule profile or both for egress queues.	"User-configurable scheduler profile on FLS, FGS and FCX"

CLI differences in IronWare release R07.2.02

The *FastIron Configuration Guide* and the section Documentation Updates in these release notes describe the CLI differences in IronWare release 07.2.02 compared with earlier releases. No CLI commands have been deprecated for this release.

Documentation Updates

This section contains documentation updates in this release.

Updates to SNTP feature

Release 07.2.02g introduces updates to the SNTP feature.

Specifying an SNTP server

You can configure the Brocade device to consult up to three SNTP servers for the current system time and date. The first server configured will be used unless it becomes unreachable, in which case the Brocade device will attempt to synchronize with the other SNTP servers (if any) in the order in which they were configured.

Brocade devices do not retain time and date information across power cycles. Unless you want to reconfigure the system time counter each time the system is reset, Brocade recommends that you use the SNTP feature as described below.

To identify an SNTP server with IP address 208.99.8.95 to act as the clock reference for a Brocade device, enter the following.

```
Brocade(config)# sntp server 208.99.8.95
```

Syntax: [no] **sntp server** { <*ip-address*> | <*hostname*> | **ipv6** <*ipv6-address*> } [<*sntp-version*>] [**authentication-key** <*key-ID*> <*key-string*>]

The <*sntp-version*> parameter specifies the SNTP version the server is running and can be from 1 – 4. The default is 4. The SNTP version is automatically set to 4, unless a different SNTP version is specified in the device startup configuration. You can configure up to three SNTP servers by entering three separate **sntp server** commands.

The order in which the SNTP servers are configured is the order in which they are consulted. The server that was configured first is the first server consulted after the poll cycle; the next server will be consulted only if a positive ACK is not received from the first one.

To specify an IPv6 address for the SNTP server, use the **ipv6** option.

The **authentication-key** option allows you to configure an authentication key for communication with the SNTP server. When the authentication key is configured for an SNTP client, it is used only for an SNTP unicast client. You must assign a unique server <key-ID> and pre-share <key-string>. The <key-ID> and pre-share <key-string> are used together to create the MD5 checksum. The MD5 checksum is used for authentication for request and reply messages with the SNTP server. The <key-ID> is the symmetric key shared with the upstream server, and accepts values from 1 to 4,294,967,295. The <key-string> is the authentication string itself, and can take up to 16 characters. If the <key-string> variable consists of only numerical characters, you must enclose the numerical characters in double quotes.

Modification of the authentication key fields is not supported. To change the key ID or key string, remove the time server using the **no sntp server...** command, then reconfigure the server with the new key.

By default, the Brocade device polls its SNTP server every 30 minutes (1800 seconds). To configure the Brocade device to poll for clock updates from a SNTP server every 15 minutes, enter the following.

```
Brocade(config)# sntp poll-interval 900
```

Syntax: **[no] sntp poll-interval** <*16-131072*>

To display information about SNTP associations, enter the **show sntp associations** command.

```
Brocade# show sntp associations
  address          ref clock       st   when   poll   delay   disp
 ~207.95.6.102     0.0.0.0         16    202      4     0.0      5.45
 ~207.95.6.101     0.0.0.0         16    202      0     0.0      0.0
* synced, ~ configured
```

Syntax: **show sntp associations**

The following table describes the information displayed by the **show sntp associations** command.

Table 4 Output from the show sntp association command

Field	Description
(leading character)	One or both of the following:*Synchronized to this peer ~Peer is statically configured
address	IP address of the peer
ref clock	IP address of the peer reference clock, or the reference ID of the external clock source if the peer is stratum 1. Examples of external clock source IDs: GPS, CDMA, WWV (Ft.Collins US Radio 2.5, 5, 10, 15 MHz), CESM (calibrated Cesium clock), etc.
st	NTP stratum level of the peer
when	Amount of time since the last NTP packet was received from the peer. A negative number indicates the system has never received any synchronization message from the specified server.
poll	The poll interval of the peer relative to the server.
delay	The total delay time in milliseconds along the path to the root clock.
disp	The dispersion of the root path in milliseconds.

To display detailed information about SNTP associations, enter the **show sntp associations details** command.

```
Brocade# show sntp associations details
208.99.8.95 configured,insane, unsynched,invalid, stratum 16
ref ID 0.0.0.0,time 0.0 (Jan  1 00:00:00)
our mode client, peer mode unspec, our poll intvl 15, peer poll intvl 0
root delay 0.0 msec, root disp 0.0
delay  0 msec, offset  0 msec
precision 2**0, version 0
org time 0.0 (Jan  1 00:00:00)
rcv time 0.0 (Jan  1 00:00:00)
xmt time 0.0 (Jan  1 00:00:00)
```

Syntax: **show sntp associations details**

The following table describes the information displayed by the **show sntp associations** details command.

Table 5 Output from the show sntp associations details command

Field	Description
IP address	The IP address of the SNTP server. The IP address is an IPv4 or an IPv6 address.
configured or dynamic	The SNTP server is either configured, or the last responsive broadcast server that is found dynamically.
authenticated	If MD5 authentication is enabled for the peer.
sane or insane	If the SNTP server passes sanity checks.
synched or unsynched	If the system is synchronized or unsynchronized to the NTP peer.
valid or invalid	If the peer time is valid or invalid.
stratum	The NTP stratum level of the peer.
reference ID	The IP address of the peer (if any) to which the unit is synchronized. The reference ID can also refer to the external clock source if the peer is stratum 1. Examples of external clock source IDs: GPS, CDMA, WWV (Ft.Collins US Radio 2.5, 5, 10, 15 MHz), CESM (calibrated Cesium clock), etc.
time	The reference time stamp.
our mode	The mode relative to the peer. The mode can be a client or a broadcast client.
peer mode	Peer mode relative to us.
our poll intvl	The system poll interval relative to the peer.
peer poll intv	The poll interval of the peer relative to the server.
root delay	The total delay time in milliseconds along the path to the root clock.
root disp	The dispersion of the root path in milliseconds.
delay	The round trip delay to the peer in milliseconds.
offset	The offset of the peer clock relative to the system clock.
precision	The precision of the system clock in Hz.
version	The NTP version of the peer. The version can be from 1 - 4.
org time	The original timestamp of the system clock. The original timestamp is what the client has sent to the server.

Field	Description
rcv time	The receive timestamp of the system clock.
xmt time	The transmit timestamp of the system clock.

To display information about SNTP status, enter the **show sntp status** command.

```
Brocade# show sntp status
Clock is synchronized, stratum = 4, reference clock = 10.70.20.23
precision is 2**-20
reference time is 3489354594.3780510747
clock offset is 0.0000 msec, root delay is 0.41 msec
root dispersion is 0.11 msec, peer dispersion is 0.00 msec
sntp poll-interval is 10 secs
```

Syntax: show sntp status

The following table describes the information displayed by the **show sntp status** command.

Table 6 Output from the show sntp status command

Field	Description
unsynchronized	System is not synchronized to an NTP peer.
synchronized	System is synchronized to an NTP peer.
stratum	NTP stratum level of the upstream time server.
reference clock	IP address of the peer reference clock, or the reference ID of the external clock source if the peer is stratum 1. Examples of external clock source IDs: GPS, CDMA, WWV (Ft.Collins US Radio 2.5, 5, 10, 15 MHz), CESM (calibrated Cesium clock), etc.
precision	Precision of this system's clock (in Hz)
reference time	Reference time stamp
clock offset	Offset of clock to synchronized peer
root delay	Total delay along the path to the root clock
root dispersion	Dispersion of the root path
peer dispersion	Dispersion of the synchronized peer
sntp poll-interval	Shows how often the Brocade device polls for clock updates from an SNTP server.

Configuring the device as an SNTP server

You can configure the Brocade device to function as an SNTP server to its downstream clients. When using the device as an SNTP server, you can also set it to use its own internal clock as the reference source if an upstream server becomes unavailable.

To use the device as an SNTP server, enter a command such as the following at the Privileged EXEC level.

```
Brocade(config)# sntp server-mode use-local-clock authentication-key abc123
Brocade(config)# write memory
```

The above example configures the device to operate as an SNTP server with the local clock as a reference backup and an authentication key of "abc123" and writes the configuration changes to memory.

Syntax: [**no] sntp server-mode** [**use-local-clock** [**stratum** <*stratum-number*>]] [**authentication-key** <*key-string*>]

The **use-local-clock** option causes the Brocade device to use the local clock as a reference source if an upstream reference source becomes unavailable. The SNTP stratum number is set to 1 by default. You may specify a different stratum number using the stratum option; <stratum-number> must be between 1 and 15. When the internal clock is serving as the SNTP reference source, the Brocade device will use the specified stratum number (or the default value of 1). When it is synchronized with the upstream server, the Brocade device will use the upstream server's stratum number plus 1.

If you do not include the **use-local-clock** option the Brocade device will function as specified by RFC 4330: when the Brocade device loses upstream synchronization, it will respond to client SNTP requests with a "kiss-of-death" response (stratum value=0).

To enable the **use-local-clock** option, you must set the internal clock of the Brocade device either by SNTP synchronization (see "Specifying an SNTP server" on page 17) or by using the clock set command (see "Setting the system clock" on page 30). Until the internal clock is set, the Brocade device will continue to rely exclusively on an upstream SNTP server if one is reachable. If none, the SNTP server of the Brocade device is disabled (down).

To require a code string for authentication of SNTP communication from clients, use the **authentication-key** option and enter a key string of up to 16 characters. When this option is used, authentication parameters are required in clients' SNTP request messages. If authentication fails, the Brocade device will reply with stratum 0 and a reference ID code of "CRYP" (cryptographic authentication or identification failed), and messages received without the required parameters will be dropped.

NOTE: Once entered, the authentication key cannot be viewed. Using the show running-config command will show output similar to the following when an authentication key has been set:

```
sntp server-mode authentication-key 2 $QHMiR3NzQA=
```

The **2** indicates that the key is encrypted using base-64 encryption; the characters following the **2** are the encrypted authentication string.

You cannot enable or disable the **use-local-clock** option (or its stratum number) or change the authentication string when the SNTP server is up. To change these settings after enabling SNTP server mode, you must disable server mode using the command **no sntp server-mode**, then re-enable it with the new parameters.

Displaying SNTP server information

Use the **show sntp server-mode** command to display the status of the SNTP server and its configuration.

```
Brocade# show sntp server-mode
Status            : up
```

```
Stratum           : 4
Authentication    : md5
Clock source      : 10.50.2.121
Last upstream sync: 15:55:00 Pacific Sun Jul 5 2009

Last 5 unique responses sent to downstream clients :
Client Address           Reference Time
10.1.50.23               16:10:32 Pacific Sun Jul 5 2009
10.1.52.34               15:50:40 Pacific Sun Jul 5 2009
10.1.50.41               10:22:08 Pacific Fri Jul 3 2009
10.1.50.10               06:21:03 Pacific Fri Jul 3 2009
10.1.50.29               21:17:39 Pacific Fri Jul 2 2009
```

Syntax: **show sntp server-mode**

Table 7 Output from the show sntp server-mode command

Field	Description
status	The operational state of the SNTP server. “Up” means that the SNTP port is open; “down” means that the SNTP port is closed. (If sntp server-mode is disabled, the show sntp server-mode command will display the message “SNTP server is not operational.)
stratum	Stratum number of this server. The range is from 1 through 15. If the device is synchronized to an upstream SNTP server, this will show that server’s stratum number +1. If the device is unsynchronized and using the use-local-clock option, this will show the user-specified stratum number (or the default value of “1” if no stratum has been configured).
authentication	Authentication key used. If authentication has been configured successfully, this displays “md5.” If not, it displays “none.”
clock source	The source of the reference time. When the reference source is an upstream SNTP server, this will show the IP address of the upstream server. When the internal clock of the device is being used as the reference, this will show “local-clock.”
last upstream sync	The last upstream time-server synchronization, displayed in timestamp format. This field is not displayed if the time source is the local clock.
last responses sent to clients	The last responses sent to downstream clients (maximum of five unique clients), displayed in reverse chronological order. Each entry shows the IP address of the client and the timestamp sent.

Enabling broadcast mode for an SNTP client

The Brocade device can be configured as an SNTP client. You can enable an SNTP client to function in a broadcast mode when the NTP server is within the same LAN, and the expected delay in response to calibrate the system clock is minimal. In a broadcast mode, the SNTP client will not send queries to the NTP server. The SNTP client will listen to any number of NTP servers on the network until the last message is received from the system clock. To update the system clock with the last message received,

you can enable the SNTP client to either listen to all NTP broadcast servers on any interface, or enable the SNTP client to listen to only one specific NTP broadcast server.

To enable an SNTP client in a broadcast mode to listen to all NTP servers on any interface, enter the **sntp broadcast client** command.

```
Brocade(config)#sntp broadcast client
```

Syntax: **sntp broadcast client**

The **sntp broadcast client** command enables an SNTP client to listen to all NTP servers, and update the client's clock with the last message received from any NTP server.

To enable an SNTP client to listen to only one specific IPv4 NTP broadcast server, enter the following commands.

```
Brocade(config)#sntp broadcast client
Brocade(config)#sntp broadcast server 1.1.1.1
```

To enable an SNTP client to listen to only one specific IPv6 NTP broadcast server, enter the following commands.

```
Brocade(config)#sntp broadcast client
Brocade(config)#sntp broadcast server ipv6 2001:179:2:1::1
```

Syntax: **sntp broadcast server** [<*ip-address*> | **ipv6** <*ipv6-address*>]

The **sntp broadcast client** command must be configured with the **sntp broadcast server** command to allow for an SNTP client to listen to only one specific NTP server.

When both unicast and broadcast modes are enabled for an SNTP client, the priority by which the NTP server is used to update the client's clock is as follows.

- The last responsive unicast server.
- The broadcast server on any interface.

qd commands on FGS and FLS devices

Information on configurable descriptor and configurable buffer for qd commands for FGS and FLS devices in the configuration guide is incorrect.

- The maximum configurable descriptors using the qd-descriptor command is 3999.
- The maximum configurable buffer using the qd-buffer command is 2904.

Flow control on SuperX devices

The *FastIron Configuration Guide* states that all FastIron devices support *asymmetric* flow control, meaning they can receive PAUSE frames but cannot transmit them. This is true for FastIron devices with the exception of SuperX devices; *symmetric* flow control is turned on by default on SuperX devices.

SSH key generation time

The authentication and encryption algorithms have changed to be more secure. The increased security affects SSH key generation time. The new SSH key generation time ranges apply only to initial key generation. Refer to the following table for initial SSH key generation time ranges.

Device	Lowest SSH key generation time (in seconds)	Highest SSH key generation time (in seconds)	Average SSH key generation time (in seconds)
FCX devices	29 seconds	63 seconds	40 seconds
FSX devices	24 seconds	186 seconds	124 seconds
FESX devices	23 seconds	412 seconds	190 seconds
FWS devices	683 seconds (approximately 11 minutes and 23 seconds)	1242 seconds (20 minutes and 42 seconds)	960 seconds (16 minutes)

VRRP show command output

In some of the VRRP show command outputs in the *FastIron Configuration Guide*, Hello-Interval and Dead-Interval timers are displayed in seconds instead of milliseconds.

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 07.2.02.

New limit for IPv4 system-max ip-cache

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 07.2.02 and if your configuration has an ip-cache value greater than 32768, it will be automatically reduced to 32768.

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, SuperX, and FSX devices

High CPU utilization will occur when IGMP Snooping and PIM/DVMRP routing are enabled simultaneously on a FESX, SuperX, or FSX 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 8 characters, the port name will be truncated in the output of the **show interface brief** command.

ICMP redirect messages

In software release 07.2.02, ICMP redirect messages are *disabled* by default, whereas in releases prior to 07.2.02, ICMP redirect messages are *enabled* by default.

- If ICMP redirect messages were enabled prior to upgrading to release 07.2.02, you will need to re-enable this feature after upgrading to 07.2.02. 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 07.2.02, the configuration (**no ip icmp redirect)** will be removed from the configuration file after upgrading to 07.2.02, 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 Layer 3 device, the interface is assigned a leased IP address. To disable DHCP-client service on an interface on a FSX Base Layer 3 device, and assign a new IP address, enter the following commands.

1. Disable DHCP-client on the interface. For example, enter a command such as the following.

   ```
   FastIron(config-if-e1000-3/1)# no ip dhcp-client enable
   ```

   Syntax: no ip dhcp-client enable

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 Layer 3 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 Layer 3 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 Layer 3 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 8 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 8 Supported management features

Category and description	FESX SuperX 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	Yes	Yes	Yes	Yes	Yes
DHCP server	Yes	Yes	Yes	Yes	Yes
Disabling TFTP access	Yes	No	No	No	Yes
Hitless management: • Hitless switchover • Hitless failover	Yes (FSX 800 and	No	No	No	See next line item

Category and description	FESX SuperX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
• Hitless OS upgrade	FSX 1600 only)				
Hitless stacking management: • Hitless stacking switchover • Hitless stacking failover	No	No	No	No	Yes
Hitless support for: • PBR • GRE Tunnels • IPv6 to IPv4 Tunnels	Yes (FSX 800 and FSX 1600 only)	No	No	No	Yes (PBR only)
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 SuperX 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 9 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 9 Supported security features

Category and description	FESX SuperX 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 SuperX 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
• DHCP snooping with dynamic ACLs	Yes	No	No	No	No

Category and description	FESX SuperX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
• 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 10 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 10 Supported system-level features

Category and description	FESX SuperX 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
32,000 MAC addresses per switch (when flow-based MAC learning is enabled)	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

Category and description	FESX SuperX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
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
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

Category and description	FESX SuperX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
Port mirroring and monitoring (mirroring of both inbound and outbound traffic on individual ports)	Yes	Yes	Yes	Yes	Yes
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)
PoE firmware upgrade via CLI	Yes	No	No	No	Yes
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
User-configurable scheduler profile	No	Yes	No	No	Yes
User-configurable buffer profile	No	Yes	No	No	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 11.

Table 11 Supported Layer 2 features

Category and description	FESX SuperX 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
Interpacket Gap (IPG) adjustment	Yes	Yes	Yes	Yes	Yes
IP MTU (individual port setting)	Yes	No	No	No	Yes

Category and description	FESX SuperX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
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
Super Aggregated VLANs	Yes	Yes	Yes	Yes	Yes
Trunk groups: • Trunk threshold for static trunk groups	Yes	Yes	Yes	Yes	Yes

Category and description	FESX SuperX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
• Flexible trunk group membership • Option to include Layer 2 in trunk hash calculation (FGS, FLS, FWS only)					
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 • Multi-range 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
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 12.

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 12 Supported base Layer 3 features

Category and description	FESX SuperX 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 13.

NOTE: Edge Layer 3 images are supported in the FastIron (hardware) models listed in Table 13. These features are also supported with software-based licensing. For details, refer to the chapter "Software-based Licensing" in the *FastIron Configuration Guide*.

Table 13 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 14 .

NOTE: Full Layer 3 features are supported in the FastIron (hardware) models listed in Table 14. These features are also supported with software-based licensing. For details, refer to the chapter "Software-based Licensing" in the *FastIron Configuration Guide*.

Table 14 Supported full Layer 3 features

Category and description	FESX-PREM SuperX-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 SuperX-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 SuperX-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 15 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 15 Supported IPv6 management features

Category and description	FESX SuperX 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
DNS server name resolution	Yes	Yes	Yes	Yes	Yes

Category and description	FESX SuperX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
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 16 lists the features that are not supported on the FastIron devices. If required, these features are available on other Brocade devices.

Table 16 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
• VLAN-based priority

System-level features not supported
Layer 3 features not supported
• AppleTalk routing
• 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 R07.2.02r

Table 17 lists the software image files that are available for IronWare Release 07.2.02r.

Table 17 Software image files

Device	Boot Image	Flash Image
FESX SuperX FSX 800 FSX 1600	sxz07200.bin	SXS07202r.bin (Layer 2) or SXL07202r.bin (base Layer 3) or SXR07202r.bin (full Layer 3)
FGS FLS FWS	fgz05000.bin	FGS07202r.bin (Layer 2) or FGSL07202r.bin (base Layer 3) or FGSR07202r.bin (edge Layer 3)
FGS-STK FLS-STK	fgz05000.bin	FGS07202r.bin (Layer 2) or FGSL07202r.bin (base Layer 3)
FCX	grz07100.bin	FCXS07202r.bin (Layer 2) or FCXR07202r.bin (Layer 3)

Factory pre-loaded software

Table 18 lists the software that is factory-loaded into the primary and secondary flash areas on the device.

NOTE: Devices with 8MB of flash memory, including FGS, FLS and FESX devices, can only store a primary image. FCX and SX devices can store one Full Layer 3 image or two Layer 2 or Base Layer 3 images.

Table 18 Factory pre-loaded software

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

PoE Firmware files

Table 19 lists the PoE firmware file types supported for IronWare Release 07.2.02r. The firmware files are specific to their devices and are not interchangeable. For example, you cannot load FCX PoE firmware on a FSX device.

Table 19 PoE Firmware files

Device	POE Firmware Version	PoE Firmware Filenames
FESX SuperX FSX 800 FSX 1600	6.0.6	fsx_poe_06.0.6.fw
FSX 800 with SX-FI648PP module FSX 1600 with SX-FI648PP module	02.1.0	fsx_poeplus_02.1.0.fw
FCX	02.1.0	fcx_poeplus_02.1.0.fw

NOTE: The PoE circuitry includes a microcontroller pre-programmed at Brocade factory. In the past, a copy of the current microcontroller code was embedded as part of the FastIron software releases and was used for upgrades if necessary. Two different types of PoE controller code sets were included for PoE and POE+ subsystems. That is no longer the case, and the software has been enhanced so that it can be loaded as an external file. The microcontroller code has not changed in this release, so there is no current need for an upgrade.

Should a new version of POE code be released, Brocade will notify its customers of the needed code upgrade. Finally, in the remote case that a failure occurs during an upgrade process, the switch would

still be functional but without PoE circuitry. Should you encounter such an issue, please contact Brocade Technical Support for servicing.

Upgrading the software

Use the procedures in this section to upgrade the software.

Important notes about upgrading or downgrading the software

Note the following when upgrading to software release 07.2.02r:

- If you are performing an upgrade on a device that has an XFP optic that is not working properly and the device is running a software release prior to 07.2.02r, you must remove the XFP optic from the port after the upgrade, then re-insert it into the port.
- To upgrade an FWS device running software version 04.3.00 to version 07.2.02r, you must first upgrade to release 04.3.02 before upgrading to 07.2.02r. 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 07.2.02r 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 07.2.02r 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 07.2.02r:

- 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 07.2.02r 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 07.2.02r compared to releases 07.0.01b and 07.0.01c. Therefore, if an FCX is downgraded from software release 07.2.02r 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 07.2.02r 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 07.2.02r 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 07.2.02r.

Before upgrading the software on the device, first read Important notes about upgrading or downgrading the software.

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. If the device has 8 MB of flash memory or if you want to install a Full Layer 3 image on an SuperX or SX device, you must delete the primary and secondary image
3. 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.

   ```
   FastIron 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.

4. 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.

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

Upgrading the flash code

NOTE: You must delete the current primary and secondary images before completing the upgrade steps. Devices with 8MB of flash memory can only hold one complete image.

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. If the device has 8MB of flash memory or if you want to install a Full Layer 3 image on an FWS, SuperX or FSX device, you must delete the primary and secondary images before upgrading the image. To delete images from the flash, enter the following commands:

```
FastIron Router# erase flash primary
FastIron Router# erase flash secondary
```

NOTE: If the primary flash contains additional files not related to the software update, it is recommended that you also delete these files.

3. 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.

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

4. 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 5, otherwise, go back to step 1.

5. 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
```

6. 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.

NOTE: This example output may not exactly match the output from your system. Output examples do not necessarily reflect all components installed in a system.

```
FastIron Router# show version
Copyright (c) 1996-2010 Brocade Communications Systems, Inc.
    UNIT 1: compiled on Jan 10 2011 at 22:07:22 labeled as FCXR07202
                (6007035 bytes) from Secondary FCXR07202.bin
        SW: Version 07.2.02T7f3
    UNIT 2: compiled on Jan 10 2011 at 22:07:22 labeled as FCXR07202
                (6007035 bytes) from Secondary FCXR07202.bin
        SW: Version 07.2.02T7f3
    UNIT 3: compiled on Jan 10 2011 at 22:07:22 labeled as FCXR07202
                (6007035 bytes) from Secondary FCXR07202.bin
        SW: Version 07.2.02T7f3
    UNIT 4: compiled on Jan 10 2011 at 22:07:22 labeled as FCXR07202
                (6007035 bytes) from Secondary FCXR07202.bin
        SW: Version 07.2.02T7f3
    UNIT 5: compiled on Jan 10 2011 at 22:07:22 labeled as FCXR07202
                    (6007035 bytes) from Secondary FCXR07202.bin
            SW: Version 07.2.02T7f3
      Boot-Monitor Image size = 369292, Version:07.1.00T7f5 (grz07100)
      HW: Stackable FCX648S-PREM (PROM-TYPE FCX-ADV-U)
    ==========================================================================
    UNIT 1: SL 1: FCX-48GS 48-port Management Module
             License: FCX_ADV_ROUTER_SOFT_PACKAGE   (LID: )
             P-ENGINE  0: type DB90, rev 01
             P-ENGINE  1: type DB90, rev 01
    ==========================================================================
    UNIT 1: SL 2: FCX-2XGC 2-port 16G Module (2-CX4)
    ==========================================================================
    UNIT 1: SL 3: FCX-2XG 2-port 10G Module (2-XFP)
    ==========================================================================
    UNIT 2: SL 1: FCX-48GS POE 48-port Management Module
             License: FCX_ADV_ROUTER_SOFT_PACKAGE   (LID: )
             P-ENGINE  0: type DB90, rev 01
             P-ENGINE  1: type DB90, rev 01
    ==========================================================================
    UNIT 2: SL 2: FCX-2XGC 2-port 16G Module (2-CX4)
    ==========================================================================
    UNIT 2: SL 3: FCX-2XG 2-port 10G Module (2-XFP)
    ==========================================================================
```

```
UNIT 3: SL 1: FCX-24GS POE 24-port Management Module
         Serial  #: BCW22926209
         License: FCX_ADV_ROUTER_SOFT_PACKAGE   (LID: )
         P-ENGINE  0: type DB90, rev 01
========================================================================
UNIT 3: SL 2: FCX-2XGC 2-port 16G Module (2-CX4)
========================================================================
UNIT 3: SL 3: FCX-2XG 2-port 10G Module (2-XFP)
========================================================================
UNIT 4: SL 1: FCX-24GS 24-port Management Module
         Serial  #: BCV2223F001
         License: FCX_ADV_ROUTER_SOFT_PACKAGE   (LID: )
         P-ENGINE  0: type DB90, rev 01
========================================================================
UNIT 4: SL 2: FCX-2XGC 2-port 16G Module (2-CX4)
========================================================================
UNIT 5: SL 1: FCX-24GS 24-port Management Module
         Serial  #: BCV2223F022
         License: FCX_ADV_ROUTER_SOFT_PACKAGE   (LID: )
         P-ENGINE  0: type DB90, rev 01
========================================================================
UNIT 5: SL 2: FCX-2XGC 2-port 16G Module (2-CX4)
========================================================================
  800 MHz Power PC processor 8544E (version 33/0022) 400 MHz bus
65536 KB flash memory
  256 MB DRAM
Monitor Option is on
STACKID 1  system uptime is 1 minutes 54 seconds
STACKID 2  system uptime is 1 minutes 54 seconds
STACKID 3  system uptime is 1 minutes 54 seconds
STACKID 4  system uptime is 1 minutes 54 seconds
STACKID 5  system uptime is 1 minutes 54 seconds
The system started at 09:07:46 GMT+09 Tue Feb 08 2011
The system : started=warm start  reloaded=by "reload"
My stack unit ID = 1, bootup role = active
telnet@fcx648s-upper#
```

NOTE: If any unit in the IronStack is running an incorrect version of the software, it 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 section "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

E-mail and telephone access

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

Go to http://www.brocade.com to obtain the latest version of the user guides.

Reporting document errors

Send an email to documentation@brocade.com to report errors you find in the user guides.

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 *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)*	Describes the hardware as shipped. Provides installation instructions, hardware maintenance procedures, hardware specifications, and 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 R07.2.02r

Defect ID: DEFECT000563656	
Technical Severity: Low	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** System
Reported In Release: FI 07.2.02	**Technology:** System
Symptom: Slow memory leak on the device.	
Condition: This issue is seen on all platforms running FI 7.2.02n or previous releases with HTTPs session login/logout.	
Recovery: Reload of device	

Defect ID: DEFECT000564926	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 07.2.02	**Technology:** HTTP/HTTPS
Symptom: Memory leak on FGS device.	
Condition: This issue can be seen in a FGS device running FI 7.2.02n or previous releases and HTTPs enabled.	
Recovery: Reload of device.	

Customer reported defects closed with code in Release R07.2.02q

Defect ID: DEFECT000564199	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 3 Routing/Network Layer
Reported In Release: FI 07.2.02	**Technology Area:** VRRPv2 - Virtual Router Redundancy Protocol Version 2
Symptom: After deletion of a VLAN that contains a virtual interface with VRRPE VIP, the device continues to respond to pings addressed to the VIP.	
Condition: This issue occurs when a VLAN is configured with a ve, the ve is configured with a VRRPE VIP and the VLAN is removed.	
Workaround: This issue can be prevented by disabling the VRRPE VRID before removing the VLAN.	
Recovery: After this issue has occurred, it can be resolved by configuring the VRRPE VIP as a /32 IP address on a previously unused loopback interface and then removing the loopback interface.	

Customer reported defects closed with code in Release R07.2.02p

Defect ID: DEFECT000558263	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Security
Reported In Release: FI 07.2.02	**Technology Area:** 802.1x Port Security
Symptom: When DOT1X client is authorized with a VLAN, the port is moved dynamically to the RADIUS assigned VLAN. After disabling the port, the DOT1X client is cleared but the port remains in RADIUS assigned VLAN instead of moving to original (configured) VLAN.	
Condition: DOT1X is enabled on the port. The DOT1X client is authorized by RADIUS with dynamic VLAN, session-timeout and termination-action as RADIUS-Request.	

Customer reported defects closed with code in Release R07.2.02n

Defect ID: DEFECT000545987	
Technical Severity: Medium	Probability: High
Product: IronWare	Technology: Security
Reported In Release: FI 07.2.02	Technology Area: FIPS
Symptom: Establish HTTPS connection through SSL3.0 version is vulnerable. Reference: CVE-2014-3566 (POODLE): http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566	
Condition: Establish HTTPS connection through SSL3.0 version is vulnerable.	

Customer reported defects closed with code in Release R07.2.02m

Defect ID: DEFECT000389221	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Other
Reported In Release: FI 07.2.02	**Technology Area:** Other
Symptom: When the "dm ps-device 1|2 show all" command is issued, the device stops functioning and has to be restarted manually.	
Condition: When "dm ps-device 1|2 show all" command is issued the device stops functioning and requires manual intervention to reboot.	

Defect ID: DEFECT000389491	
Technical Severity: High	**Probability:** Low
Product: IronWare	**Technology:** Management
Reported In Release: FI 07.1.00	**Technology Area:** SCP - Secure Copy
Symptom: The firmware image update using SCP fails in FastIron device and the image does not get upgraded.	
Condition: When the firmware is updated using SCP in FastIron device, flash corruption is observed resulting in unsuccessful image upgrade.	

Defect ID: DEFECT000485242	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 07.4.00	**Technology Area:** IEEE 802.1w RSTP
Symptom: TCN BPDUs flood the network when the FI devices are connected in a multi-access section (Hub) topology.	
Condition: When several FI devices are connected to a multi-access section (Hub), running 802.1d or PVST, TCN will not terminate resulting in network flooding.	

Defect ID: DEFECT000486788	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 07.2.02	**Technology Area:** IPv4/IPv6 Host Management
Symptom: DHCP DECLINE messages will get dropped by FastIron device when DHCP snooping is enabled for a particular VLAN.	
Condition: When DHCP snooping is enabled on a particular VLAN the FastIron device relay agent would drop the DHCP DECLINE messages.	

Defect ID: DEFECT000512397	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 07.2.02	**Technology Area:** OSPF (IPv4)
Symptom: OSPF routes learnt on interface id 0 (that is, interface 1/1) will not get installed in routing table of FI device resulting in traffic loss.	
Condition: When OSPF routes are learnt on interface 1/1 the routes would not get installed in the IP routing table of the FI device.	

Defect ID: DEFECT000517795	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Other
Reported In Release: FI 07.2.02	**Technology Area:** Other
Symptom: Random logging host configurations are observed in the FI device after cold reboot.	
Condition: When the FI device is cold rebooted with "logging persistence" enabled in the CLI, random logging host entries are observed in the configuration.	

Customer reported defects closed with code in Release R07.2.02k

Defect ID: DEFECT000396271	**Technical Severity:** High
Summary: [CDP-TLV] For certain voice-vlan numbers, checksum for CDP packets is failing	
Symptom: For certain voice-vlan numbers, checksum for CDP packets is failing.	
Probability: Low	**Risk of Fix:** Medium
Feature: FI Platform Specific features	**Function:** PoE/PoE+
Reported In Release: FI 07.3.00	**Service Request ID:** ,1179888

Defect ID: DEFECT000407488	**Technical Severity:** Medium
Summary: Get-next request for OID .1.3.6.1.2.1.17.7.1.4.2.1.3.0 might skip to the next object instead of getting the next value on the same tabular object.	
Symptom: SNMP Get-next request for OID .1.3.6.1.2.1.17.7.1.4.2.1.3.0 skips to .1.3.6.1.2.1.17.7.1.4.2.1.4.0.1 instead of -3.0.1.	
Probability: Medium	
Feature: FCX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 07.2.02	**Service Request ID:** 721281

Defect ID: DEFECT000415181	**Technical Severity:** Medium
Summary: Multicast packets are duplicated to 224.0.0.x across ICX 6610 Layer 2.	
Symptom: Multicast packets are duplicated to 224.0.0.x across ICX 6610 Layer 2.	
Probability: High	**Risk of Fix:** Medium
Feature: L2 Forwarding	**Function:** Other
Reported In Release: FI 07.4.00	**Service Request ID:** 737715

Defect ID: DEFECT000425958	**Technical Severity:** Medium
Summary: Switch unexpectedly reload after executing 'ip dhcp snooping vlan x' command.	
Symptom: Switch may unexpectedly reload after executing 'ip dhcp snooping vlan' command in SX.	
Probability: High	**Risk of Fix:** Medium
Feature: FI ACL	**Function:** DHCP Snooping functionality
Reported In Release: FI 07.4.00	**Service Request ID:** 1060660, 1042423

Defect ID: DEFECT000427550	**Technical Severity:** Medium
Summary: VRRP Standby may encounter port flap with multiple VLANs and VRIDs configuration.	
Symptom: Intermittent flaps on the VRRP standby may occur for multiple VRIDs in multiple VLANs configuration. Flap occurs only on the VRRP Standby and not on the VRRP Owner.	
Probability: Medium	**Risk of Fix:** Low
Feature: Layer3 Control Protocols	**Function:** VRRP/VRRP-E and slow-start timer-VRRP-E timer scale
Reported In Release: FI 07.3.00	**Service Request ID:** 1101971

Defect ID: DEFECT000429808	**Technical Severity:** Medium
Summary: SX switch may perform an unexpected reload when processing CPU packets.	
Symptom: SX switch may perform an unexpected reload when processing CPU packets.	
Probability: Medium	**Risk of Fix:** Low
Feature: FI Infrastructure	**Function:** Packet Scheduling/Marking/Buffering
Reported In Release: FI 07.3.00	**Service Request ID:** 1077158

Defect ID: DEFECT000450766	**Technical Severity:** Medium
Summary: Disabling sFlow at a global configuration level can cause high CPU usage.	
Symptom: When sFlow is disabled at a global CLI configuration level, the CPU utilization may go up to 99%.	
Workaround: Correct the port setting for sFlow usage by entering "sflow enable" and then "no sflow enable" at the global CLI configuration level.	
Probability: Low	**Risk of Fix:** Low
Feature: SX Network Management	**Function:** sFlow
Reported In Release: FI 07.3.00	**Service Request ID:** 1129051

Defect ID: DEFECT000451637	**Technical Severity:** Medium
Summary: Configuring sFlow may cause FastIron device to unexpectedly reload.	
Symptom: Configuring sFlow may cause FastIron device to unexpectedly reload.	
Probability: Low	**Risk of Fix:** Low
Feature: FCX Network Management	**Function:** sFlow
Reported In Release: FI 07.3.00	**Service Request ID:** 1154139

Defect ID: DEFECT000457367	**Technical Severity:** Medium
Summary: When DCHP snooping is enabled, DHCP Discover packets are only forwarded to the helper address but are not broadcast within the local VLAN.	
Symptom: If DHCP Snooping is enabled on a VLAN that has an IP Helper Address configured and a client sends a DHCP Discover packet, the packet is not broadcast within the incoming VLAN.	
Probability: High	**Risk of Fix:** Medium
Feature: FCX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.3.00	**Service Request ID:** 1153147

Defect ID: DEFECT000462469	**Technical Severity:** Medium
Summary: Disabling SNMP traps for link-down/link-up also disables Syslog messages for interface down/up events	
Symptom: Issuing "no snmp-server enable traps <link-down | link-up>" disables Syslog messages for interface down/up events.	
Probability: High	
Feature: FCX Management Functionality	**Function:** CLI and parser
Reported In Release: FI 07.2.02	**Service Request ID:** 1187496

Defect ID: DEFECT000464243	**Technical Severity:** High
Summary: In an ICX 6610 stack, host is intermittently unreachable on the member ports.	
Symptom: Host is intermittently unreachable on ports connected to the member units.	
Probability: Low	**Risk of Fix:** Medium
Feature: FI L3 Unicast	**Function:** Control Plane - Other
Reported In Release: FI 08.0.00	**Service Request ID:** 1190036

Defect ID: DEFECT000466801	**Technical Severity:** High
Summary: While running OSPFv2, device's native Router-LSA gets replaced when a fake LSA is sent from a malicious router that uses an LS ID equivalent to the device's router-id	
Symptom: In OSPFv2, FI device's native Router-LSA gets replaced when a fake LSA is sent from a malicious router which uses an LS ID equivalent to the FI device's router-id.	
Probability: High	**Risk of Fix:** Low
Feature: Layer3 Control Protocols	**Function:** OSPFV2 - IPV4
Reported In Release: FI 07.4.00	

Defect ID: DEFECT000470072	**Technical Severity:** Medium
Summary: If the AES encryption string in SNMPv3 user configuration begins with 00, it is not retained after reloads.	
Symptom: In SNMPv3, if the AES encrypted string that is based on SNMP Engine ID and user supplied key, gets generated such that its first two characters are "00", the string does not get read properly when a reboot or switchover occurs.	
Probability: Low	**Risk of Fix:** Medium
Feature: FI Embedded Management	**Function:** SNMP v1/v2/v3
Reported In Release: FI 07.4.00	**Service Request ID:** 1208892

Defect ID: DEFECT000472837	**Technical Severity:** High
Summary: Multicast traffic is duplicated when we add uplink-switch.	
Symptom: Multicast traffic is duplicated when we add uplink-switch X/Y/Z in a VLAN.	
Probability: Medium	**Risk of Fix:** Low
Feature: FI L3 Multicast	**Function:** Forwarding - TI L3 Multicast
Reported In Release: FI 08.0.00	**Service Request ID:** 1219638

Defect ID: DEFECT000475964	**Technical Severity:** High
Summary: FGS devices sends two IPv6 nd packets every second	
Symptom: Duplicate ICMPv6 neighbor solicitations are sent.	
Probability: Medium	**Risk of Fix:** Low
Feature: FI L3 Unicast	**Function:** Control Plane - ND ICMPv6
Reported In Release: FI 08.0.01	**Service Request ID:** 1219638

Customer reported defects closed with code in Release R07.2.02j

Defect ID: DEFECT000338448	**Technical Severity:** Medium
Summary: CLI throws error message when SSH is accessed through the NMS system.	
Symptom: An error string “fips_hash_Update failed with 0x000000B3, CKR_SESSION_HANDLE_INVALID” appears on the CLI when SSH is accessed through the NMS system.	
Probability: High	**Risk of Fix:** Medium
Feature: FI Embedded Management	**Function:** SSHV2/SCP
Reported In Release: FI 07.3.00	**Service Request ID:** 1112368

Defect ID: DEFECT000389216	**Technical Severity:** Medium
Summary: OSPF adjacency may not form on data ports of the Standby Management module.	
Symptom: OSPF adjacency fails to form on data ports of the Standby Management module although the ARP cache and IP routes are OK.	
Workaround: Disabling and re-enabling the router interface may get the OSPF adjacency to form. Downgrading to release 7.2.00 or prior should also resolve this issue.	
Probability: Medium	
Feature: OSPF	**Function:** OSPF
Reported In Release: FI 07.2.02	**Service Request ID:** 708908, 712545

Defect ID: DEFECT000406403	**Technical Severity:** Medium
Summary: DHCP may fail in VLAN 1 when using dual-mode interface and IP helper.	
Symptom: The switch drops DHCP packets that come on VLAN 1 when dual-mode and IP helper are enabled.	
Probability: High	
Feature: SX L2 Forwarding	**Function:** DHCP assist
Reported In Release: FI 07.2.02	**Service Request ID:** 732333

Defect ID: DEFECT000408520	**Technical Severity:** Medium
Summary: [Web] GUI does not permit applying a MAC filter to the port on FLS.	
Symptom: GUI does not permit applying a MAC filter to the port on FLS.	
Probability: Medium	
Feature: SX Management Functionality	**Function:** HTTPs/HTTP
Reported In Release: FI 07.2.02	**Service Request ID:** 747359

Defect ID: DEFECT000410498	**Technical Severity:** Medium
Summary: First VLAN IP subnet name is erased after reload.	
Symptom: When a protocol-based VLAN is configured in the VLAN, first VLAN IP subnet name is erased. After a reboot of router, dynamic IPv6 protocol VLAN membership that is disabled (using the "ipv6-proto" and dynamic port is disabled) becomes enabled.	
Feature: SX L2 Forwarding	**Function:** Protocol VLAN
Reported In Release: FI 07.2.02	**Service Request ID:** 751033

Defect ID: DEFECT000412264	**Technical Severity:** Medium
Summary: [SX] Error message is printed while loading boot image for 7202X code.	
Symptom: Error message is printed while loading boot image for 7202X code.	
Feature: SX_SYSTEM	**Function:** UNDETERMINED
Reported In Release: FI 07.2.02	**Service Request ID:** 1095368

Defect ID: DEFECT000414072	**Technical Severity:** Medium
Summary: Unable to reload the switches using IPv6 SNMP.	
Symptom: Unable to reload the switches using IPv6 SNMP.	
Probability: High	**Risk of Fix:** Medium
Feature: FCX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 07.3.00	**Service Request ID:** 760347

Defect ID: DEFECT000422319	**Technical Severity:** Medium
Summary: The "ip tcp keepalive" command may not work for IPv6.	
Symptom: The "ip tcp keepalive" command for IPv6 may not work and it may not show in running configuration.	
Probability: High	
Feature: FCX Layer 3 Forwarding - IPV6	**Function:** Data Forwarding (IPV6)
Reported In Release: FI 07.2.02	**Service Request ID:** 1085918

Defect ID: DEFECT000428623	**Technical Severity:** Medium
Summary: CDP packet from a Brocade device has one missing field, and one wrong field.	
Symptom: You are unable to see the hostname in the CDP packet for the location services.	
Probability: High	**Risk of Fix:** Medium
Feature: FI Embedded Management	**Function:** LLDP
Reported In Release: FI 07.4.00	

Defect ID: DEFECT000432681	**Technical Severity:** High
Summary: Configured IPv6 addresses are deleted when addresses learned from Router Advertisements expire.	
Symptom: When the lifetime of an IPv6 address that is auto-learned through Router Advertisements expires, then the configured addresses are deleted along with the auto-learned addresses.	
Workaround: Reboot the device. It will recover and the configured address will take effect from the configuration.	
Probability: High	**Risk of Fix:** Low
Feature: FCX Layer 3 Forwarding - IPV6	**Function:** ECMP (IPV6)
Reported In Release: FI 07.3.00	**Service Request ID:** 1111827

Defect ID: DEFECT000443109	**Technical Severity:** Medium
Summary: You are unable to configure parameters for warning temperature on FESX devices running firmware version 7.2.02 and later.	
Symptom: You are unable to configure parameters for warning temperature on FESX devices running firmware version 7.2.02 and later.	
Feature: SX Platform Specific features	**Function:** Chassis/fan/powersupplies/temperature sensors
Reported In Release: FI 07.2.02	**Service Request ID:** 1137834

Defect ID: DEFECT000448413	**Technical Severity:** Medium
Summary: During boot up, a few characters at the start of syslog messages may be omitted.	
Symptom: When the FastIron device is reloaded, some of the initial characters are omitted for the first few Syslog messages. After some period of time, the messages are generated correctly.	
Probability: Medium	**Risk of Fix:** Medium
Feature: FI Embedded Management	**Function:** SYSLOG
Reported In Release: FI 07.3.00	**Service Request ID:** 1135927

Defect ID: DEFECT000448876	**Technical Severity:** Medium
Summary: IP Cache is not updated from DROP to FORWARD after DHCP snooping and ARP are received.	
Symptom: Traffic loss to certain destinations when traffic transits through a VRRP backup device and when DHCP snooping is enabled on the incoming interface.	
Probability: Low	**Risk of Fix:** Medium
Feature: SX L2 Forwarding	**Function:** MAC Table/FDB Manager
Reported In Release: FI 07.2.00	**Service Request ID:** 1105581

Defect ID: DEFECT000452027	**Technical Severity:** Medium
Summary: The "show aaa" command output is not accurate for certain fields.	
Symptom: Certain fields in the “show aaa” command output do not appear to increment or change state in response to user logins. Specifically, the lines “opens=0 closes=0 timeouts=0 errors=0” and “no connection” do not change in response to successful user logins.	
Probability: High	**Risk of Fix:** Medium
Feature: FI Embedded Management	**Function:** AAA RADIUS/TACACS+ V4/V6
Reported In Release: FI 07.4.00	**Service Request ID:** 1154018

Defect ID: DEFECT000455532	**Technical Severity:** High
Summary: Routes that should be matching the default route are instead displaying error message "No info to print".	
Symptom: The “show ip route” command output may have several entries of "No info to print" and “show ip route x.x.x.x” command output for routes that should match the default route are showing "No info to print", which causes traffic loss.	
Feature: SX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.2.02	**Service Request ID:** 1145828

Defect ID: DEFECT000461953	**Technical Severity:** Medium
Summary: SNMPv3 Engine Time is slower than it should be on devices running firmware version 7.2.02h.	
Symptom: SNMPv3 Engine Time is slower than it should be on devices running firmware version 7.2.02h.	
Probability: High	
Feature: FCX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 07.2.02	**Service Request ID:** 1149710

Customer reported defects closed with code in Release R07.2.02h

Defect ID: DEFECT000347917	**Technical Severity:** Medium
Summary: FCX device does not forward ARP broadcast packets when raw packet debugging is enabled.	
Symptom: When the "dm raw packet debugging" command is executed in a Telnet console, the incoming ARP broadcast packets may not be forwarded in FCX devices.	
Workaround: Turn off "dm raw".	
Probability: Medium	
Feature: FCX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.2.02	**Service Request ID:** 266738

Defect ID: DEFECT000351893	**Technical Severity:** High
Summary: Memory usage steadily increases occurs every time a Web Authentication client logs in and logs out using HTTPS.	
Symptom: Memory is constantly depleted every time a Web Authentication client logs in and logs out using HTTPS.	
Workaround: Reboot the device.	
Probability: High	**Risk of Fix:** Medium
Feature: FI - L4/Security	**Function:** Web Authentication
Reported In Release: FI 07.3.00	**Service Request ID:** 700759

Defect ID: DEFECT000361556	**Technical Severity:** Critical
Summary: System unexpectedly reload in ARP function during hitless-failover.	
Symptom: FastIron devices may go for reset during hitless failover sometimes.	
Risk of Fix: Low	
Feature: FI L3 Unicast	**Function:** Forwarding - FX v4
Reported In Release: FI 07.3.00	**Service Request ID:** 745347

Defect ID: DEFECT000402207	**Technical Severity:** Medium
Summary: Switch reports 1 in snmpget for IF-MIB::ifOperStatus when the port is down.	
Symptom: IF-MIB::ifOperStatus when polled by SNMP may return incorrect status for 10G physical port.	
Workaround: Upgrade code	
Probability: Medium	
Feature: SX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 07.2.02	**Service Request ID:** 691215

Defect ID: DEFECT000404397	**Technical Severity:** Medium
Summary: Printing more than 700 lines at a time in buffer logging, causes high CPU. VRRP might not process control packets.	
Symptom: High CPU may be noticed in SX device when the “logging buffer 1000” command is executed and more than 700 lines are to be logged in SYSLOG.	
Workaround: Remove the "logging buffer" from the configuration. Default is 50 lines.	
Probability: High	
Feature: SX Network Management	**Function:** SYSLOG
Reported In Release: FI 07.2.02	**Service Request ID:** 721885

Defect ID: DEFECT000406631	**Technical Severity:** Medium
Summary: Bridge TC Event log is missing on FastIron SX switches from code 07.2.00 and later.	
Symptom: SX device running Multiple Spanning Tree(MSTP) may not log the reception of Bridge TC Event.	
Workaround: Configure edge port on all switch ports where servers and laptops are to be connected.	
Probability: Medium	
Feature: SX L2 Control	**Function:** SpanningTree Protocols
Reported In Release: FI 07.2.02	**Service Request ID:** 733719

Defect ID: DEFECT000408284	**Technical Severity:** Medium
Summary: Some OpenSSH versions are incompatible with the Fastiron devices when using scp.	
Symptom: FCX Devices may not be able to perform secure shell (SSH) login or secure copy (SCP) from client running OpenSSH v5.5.p1 version. Previous versions work properly.	
Workaround: Use an earlier version of OpenSSH.	
Probability: High	
Feature: FCX Network Management	**Function:** SSHv2/SCP V4/V6
Reported In Release: FI 07.2.02	**Service Request ID:** 604551

Defect ID: DEFECT000408747	**Technical Severity:** Medium
Summary: DHCP server not giving IP addresses to some hosts.	
Symptom: SX device running DHCP server may not offer IP addresses to hosts when moved from one subnet to other.	
Probability: Medium	**Risk of Fix:** Medium
Feature: SX DHCP SERVER	**Function:** DHCP
Reported In Release: FI 07.3.00	**Service Request ID:** 1084792, 1085652

Defect ID: DEFECT000408842	**Technical Severity:** Medium
Summary: Single SPAN STP loop may occur if a port is added to VLAN.	
Symptom: A loop may occur when a port is added to a VLAN that has dual mode port members with the same VLAN and default VLAN, even when Single Spanning Tree is enabled.	
Probability: High	**Risk of Fix:** Medium
Feature: FCX L2 Control	**Function:** single spanning-tree
Reported In Release: FI 07.3.00	**Service Request ID:** 737569

Defect ID: DEFECT000410873	**Technical Severity:** Medium
Summary: Flash can get into locked state after performing a "copy flash to flash" operation.	
Symptom: Execution of the “copy flash to flash” command in an SX device may lock the flash resulting in the following error message “Flash access in progress. Please try later” when a write memory operation is initiated.	
Feature: FCX Management Functionality	**Function:** CLI and parser
Reported In Release: FI 07.2.02	**Service Request ID:** 749897

Defect ID: DEFECT000412141	**Technical Severity:** Medium
Summary: sflow does not work for member units of the FGS stack if the uplink is 10G.	
Symptom: sflow does not work for member units of the FGS stack if the uplink is 10G and configured with IPv6 collector.	
Feature: FCX Network Management	**Function:** sFlow
Reported In Release: FI 07.2.02	**Service Request ID:** 716053

Defect ID: DEFECT000415275	**Technical Severity:** Medium
Summary: In some cases hardware route in FESX show as DROP and packets are not forwarded even if default route is configured.	
Symptom: SX router may drop packets matching to the routes configured earlier to drop, but were deleted and default route is configured.	
Workaround: This issue is not seen in 7.3c code and above	
Probability: Low	
Feature: SX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.2.02	**Service Request ID:** 752703

Defect ID: DEFECT000419065	**Technical Severity:** Medium
Summary: FastIron may have issues verifying the ssh signature with certain SSH clients.	
Symptom: FastIron devices may have issues in verifying the SSH signature with SSH-2.0-OpenSSH_4.3 version of SSH clients causing SSH to stop working with the following error “key_verify failed for server_host_key”.	
Probability: Medium	
Feature: FCX Management Functionality	**Function:** IPv4/V6 SSH Service
Reported In Release: FI 07.2.02	**Service Request ID:** 811769

Defect ID: DEFECT000419248	**Technical Severity:** Medium
Summary: Spanning tree blocked the port that is forwarding ARP broadcasts.	
Symptom: In SX device, enabling a redundant link in a VLAN may occasionally cause loop in the network.	
Workaround: Disable and enable the port that is newly added to the vlan.	
Feature: SX L2 Control	**Function:** SpanningTree Protocols
Reported In Release: FI 07.2.02	**Service Request ID:** 841043

Defect ID: DEFECT000419899	**Technical Severity:** Medium
Summary: Erroneous Syslog messages reporting functioning FCX power supply units going down and coming up immediately are generated due to signal noise level.	
Symptom: Erroneous and cosmetic Syslog messages about a Power Supply Unit being powered down and up are displayed continuously even though the PSU functions correctly and provides uninterrupted AC power to the switch/router.	
Probability: Medium	
Feature: FI Platform Specific features	**Function:** Chassis/fan/powersupplies/temperature sensors
Reported In Release: FI 07.2.02	**Service Request ID:** 1080157

Defect ID: DEFECT000423085	**Technical Severity:** Medium
Summary: PoE on SX can get stuck due to power glitch, no providing inline power or show correct info.	
Symptom: SX device may stop providing power to PDs such as access points and phones and PoE Modules showing incorrect inline power allocation, even when no PD is attached.	
Workaround: Re-install the PoE firmware on the PoE controller, or RMA the affected unit if firware installation is not successful.	
Probability: Medium	
Feature: POE FW upgrade	**Function:** POE FW upgrade
Reported In Release: FI 07.2.02	**Service Request ID:** 760185

Defect ID: DEFECT000424399	**Technical Severity:** Medium
Summary: Software might not be able to read optical monitoring values in M-SX optics.	
Symptom: FLS Device may not be able to read Digital Optical Monitoring (DOM) information from Optical Monitoring enabled optics.	
Probability: High	
Feature: DOM	**Function:** DOM
Reported In Release: FI 07.2.02	**Service Request ID:** 1094609

Customer reported defects closed with code in Release R07.2.02g

Defect ID: DEFECT000341140	**Technical Severity:** High
Summary: PoE ports flap on modifying configuration through Web interface	
Symptom: If a port name is configured via the Web interface, the link may flap.	
Probability: High	
Feature: FI Embedded Management	**Function:** Web Management
Reported In Release: FI 07.3.00	**Service Request ID:** 602297

Defect ID: DEFECT000345889	**Technical Severity:** High
Summary: After disabling/re-enabling a module, SX chassis may stop accepting configuration commands.	
Symptom: After disabling/re-enabling a module, SX chassis does not accept any configuration commands and instead prints "Error : HotSwap is in progress , please try again".	
Probability: Low	
Feature: FI Platform Specific features	**Function:** HotSwap
Reported In Release: FI 07.3.00	**Service Request ID:** 727841

Defect ID: DEFECT000347007	**Technical Severity:** Low
Summary: Port may not be displayed in "show vlan" output if Single Spanning-Tree is configured	
Symptom: With Single Spanning-Tree configured, a port that is displayed under the "show running-config" output may not be displayed as a member of the VLAN when "show vlan" is entered.	
Workaround: Recover temporarily by removing and re-adding the port to the VLAN. However, this workaround will not work across system resets.	
Probability: Medium	
Feature: SX L2 Control	**Function:** single spanning-tree
Reported In Release: FI 07.2.00	**Service Request ID:** 588187

Defect ID: DEFECT000347486	**Technical Severity:** Medium
Summary: After Switchover, SX constantly displays code flash error messages on the console	
Symptom: After Switchover, SX keeps displaying error messages such as "code_flash_block_write3: timeout, f4413620:300010" on the console.	
Probability: Low	
Feature: FI Platform	**Function:** Boot code/Flash/Kernel
Reported In Release: FI 07.3.00	**Service Request ID:** 724459

Defect ID: DEFECT000355892	**Technical Severity:** High
Summary: The command “no snmp-server comm Public ro” is not retained after a reload.	
Symptom: When using the command “no snmp-server comm Public ro” the public community will be disabled and the device will no longer respond to SNMP requests using the Public community. However it is not placed in the running config or retained after a reload. Once the Device reloads it will begin to respond to polling and read only operations using this community.	
Probability: Low	
Feature: FI Embedded Management	**Function:** SNMP v1/v2/v3
Reported In Release: FI 07.3.00	**Service Request ID:** 628995

Defect ID: DEFECT000358890	**Technical Severity:** Critical
Summary: SX1600 may reset when launching an SSHv2 session after a hitless reload	
Symptom: SX1600 may reset when launching an SSHv2 session after a hitless reload.	
Probability: High	
Feature: FI Embedded Management	**Function:** SSHV2/SCP
Reported In Release: FI 07.3.00	**Service Request ID:** 728893

Defect ID: DEFECT000364344	**Technical Severity:** Medium
Summary: When downloading an application image via TFTP, the length of the image name plus its directory location cannot exceed 32 characters	
Symptom: When using the "copy tftp flash <IP-address> <Image-file>" command, the directory containing the image file on the TFTP server can be specified. If the length of the directory name plus the image name exceeds 32 characters, the TFTP copy command will fail.	
Workaround: Do not use the directory name in the "copy tftp flash" command.	
Probability: Medium	
Feature: FI Embedded Management	**Function:** CLI and parser
Reported In Release: FI 07.3.00	**Service Request ID:** 686721

Defect ID: DEFECT000382536	**Technical Severity:** Medium
Summary: CPU memory usage increases with repetitive SSH sessions	
Symptom: With continuous creation and deletion of SSH sessions to the device, the memory usage steadily increases and does not recover.	
Probability: Low	
Feature: FI Embedded Management	**Function:** SSH/SCP
Reported In Release: FI 07.4.00	**Service Request ID:** 704159

Defect ID: DEFECT000383069	**Technical Severity:** High
Summary: TCAM entries are not updated on Standby/Member units for a static ECMP Route when there is MAC movement	
Symptom: When MAC movement for a static ECMP route occurs, traffic that is received on Standby or Member unit continues to be forwarded to the old port.	
Probability: High	
Feature: Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.4.00	**Service Request ID:** 697721

Defect ID: DEFECT000388009	**Technical Severity:** Medium
Summary: DNS resolution does not work when multiple DNS domain lists are used	
Symptom: If several domain names are created using the “ip dns domain-list <name>" command and the first domain name fails, the device keeps trying to reach it instead of trying the other configured domain names.	
Probability: High	
Feature: FCX Management Functionality	**Function:** HTTPs/HTTP
Reported In Release: FI 07.2.02	**Service Request ID:** 697877

Defect ID: DEFECT000388082	**Technical Severity:** Medium
Summary: Broadcast traffic (DHCP Discovery) sent by PVLAN community port is duplicated in primary port and other PVLAN community ports.	
Symptom: Two packets may be received instead of one since they are being duplicated.	
Probability: Medium	
Feature: FCX L2 Forwarding	**Function:** Private VLAN
Reported In Release: FI 07.2.02	**Service Request ID:** 680201

Defect ID: DEFECT000390164	**Technical Severity:** Medium
Summary: ICMP packets are not flooded if ICMP Burst protection is configured on a VE interface	
Symptom: If "ip icmp burst" command is configured on a VE interface, ICMP packets are not flooded within the associated VLAN.	
Probability: Medium	
Feature: FI ACL	**Function:** ACL based rate limitting
Reported In Release: FI 07.3.00	**Service Request ID:** 704591

Defect ID: DEFECT000390792	**Technical Severity:** High
Summary: SX800 experiences high CPU utilization when routing IP packets through ve interfaces in subnet VLANs.	
Symptom: SX800 experiences high CPU utilization when routing IP packets through ve interfaces in subnet VLANs as all routed packets are routed in software by the CPU instead of in hardware by ASICs.	
Probability: Low	
Feature: SX L2 Forwarding	**Function:** Subnet VLAN
Reported In Release: FI 07.2.02	**Service Request ID:** 711367

Defect ID: DEFECT000391791	**Technical Severity:** Medium
Summary: If the same VSRP VRID is used in multiple VLANs, then changes made under one VLAN can affect a different VLAN with the same VSRP VRID.	
Symptom: If the same VSRP VRID is used in multiple VLANs, then changes made under one VLAN can affect a different VLAN with the same VSRP VRID.	
Workaround: Do not use the same VSRP VRID in multiple VLANs.	
Probability: Medium	
Feature: FCX L2 Control	**Function:** VSRP(master and aware)
Reported In Release: FI 07.2.02	**Service Request ID:** 713975

Defect ID: DEFECT000392006	**Technical Severity:** Medium
Summary: MIB OID snAgentPoePortWattage does not return the configured value	
Symptom: The power limit on a PoE port can be set via SNMP and the value is configured correctly on the port, but it cannot be read and always displays the power value as 0 using the snAgentPoePortWattage MIB OID.	
Probability: High	
Feature: FCX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 07.3.00	**Service Request ID:** 696861

Defect ID: DEFECT000392506	**Technical Severity:** Medium
Summary: Hardware MAC entries are not properly deleted after aging, increasing the probability of MAC hash collisions	
Symptom: Over a long period of time on a campus network with many mobile users logging in an out constantly, some users lose Layer 2 connectivity as their MAC addresses cannot be learned.	
Workaround: Clearing the ARP cache usually resolves the problem. If it does not, reload the Switch/Router during a maintenance window.	
Probability: Medium	
Feature: FCX L2 Forwarding	**Function:** MAC Table/FDB Manager
Reported In Release: FI 07.2.00	**Service Request ID:** 712255

Defect ID: DEFECT000394040	**Technical Severity:** Medium
Summary: CPU memory usage increases constantly when using OpenNMS tool to poll system IP addresses	
Symptom: If OpenNMS tool is used to poll the IP addresses on a system, it can cause a CPU heap memory leak over time due to terminating multiple SSH connections prematurely.	
Workaround: Use Telnet instead of SSH to access the device.	
Probability: High	
Feature: SX Management Functionality	**Function:** IPv4/V6 SSH Service
Reported In Release: FI 07.2.02	**Service Request ID:** 704159

Defect ID: DEFECT000395770	**Technical Severity:** Medium
Summary: Using the Web Management interface to add ports to VLAN may cause MRP ring-interfaces to be removed from configuration.	
Symptom: MRP ring Interfaces disappear from the configuration when an unrelated port is added to or removed from the VLAN via Web Management interface.	
Workaround: Use the CLI to make the changes.	
Probability: Medium	
Feature: FCX Network Management	**Function:** Web Management
Reported In Release: FI 07.3.00	**Service Request ID:** 722273

Defect ID: DEFECT000396100	**Technical Severity:** Medium
Summary: Switch with no IPv4 address configured generates ARP packets incorrectly when both a Management VLAN and Uplink Switch are configured	
Symptom: Switch with no IPv4 address configured generates ARP packets with Source Address 0.0.0.0 for directed broadcast traffic when both a Management VLAN and Uplink Switch are configured.	
Probability: High	
Feature: SX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.2.02	**Service Request ID:** 722675

Defect ID: DEFECT000396159	**Technical Severity:** Low
Summary: RADIUS IP Address may be displayed incorrectly in the output of “show table-mac-vlan detail” command	
Symptom: In the "show table-mac-vlan detail" display, not enough characters are allocated for the RADIUS IP address column, which can cause trailing characters to be lost for a given IP address.	
Probability: Medium	
Feature: FCX L2 Forwarding	**Function:** MAC- BASED VLAN
Reported In Release: FI 07.2.02	**Service Request ID:** 722235

Defect ID: DEFECT000396545	**Technical Severity:** Medium
Summary: Aggregate VLAN Q-in-Q supports frame sizes of up to 1522 bytes only	
Symptom: With Q-in-Q configured, frame sizes of up to 1522 bytes are supported instead of the expected 1530 bytes. Frames larger than 1522 bytes are dropped.	
Workaround: Configure for Jumbo frame support.	
Probability: High	
Feature: FCX L2 Forwarding	**Function:** Q-in-Q
Reported In Release: FI 07.2.02	**Service Request ID:** 715413

Defect ID: DEFECT000397889	**Technical Severity:** High
Summary: Configuring and then removing Protocol VLAN does not clear the MAC Address Locking settings on port registers	
Symptom: High CPU condition due to data packets being forwarded by the CPU instead of in the hardware.	
Workaround: Issue "dot1x-enable", followed by "no dot1x-enable".	
Probability: Medium	
Feature: SX L2 Forwarding	**Function:** Protocol VLAN
Reported In Release: FI 07.2.02	**Service Request ID:** 725439

Defect ID: DEFECT000398642	**Technical Severity:** High
Summary: Switch may reset when printing debug messages to all destinations under certain conditions	
Symptom: The switch may experience a reset if Telnet password is enabled and the "debug destination all" command is used to send debug output to all connected sessions.	
Probability: High	
Feature: FI Embedded Management	**Function:** CLI Parser
Reported In Release: FI 07.4.00	**Service Request ID:** 724131

Defect ID: DEFECT000399298	**Technical Severity:** Medium
Summary: IP Cache display shows incorrect VLAN Id's for some entries	
Symptom: In rare cases, the output of the "show ip cache" command displays IP Address entries with incorrect VLAN Id's.	
Probability: Low	
Feature: FCX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.2.02	**Service Request ID:** 683131

Defect ID: DEFECT000400771	**Technical Severity:** Medium
Summary: If the usage of TCAM entries reaches near the maximum, a route entry could be overwritten by another route entry	
Symptom: Routed traffic may not be forwarded to directly connected hosts in rare instances if the TCAM usage reaches near its maximum limit.	
Workaround: Clear the ARP cache and MAC table, then disable and re-enable the relevant IP interface.	
Probability: Low	
Feature: FCX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.3.00	**Service Request ID:** 728137

Defect ID: DEFECT000401082	**Technical Severity:** High
Summary: Cannot communicate with Tagged Promiscuous port on Primary VLAN from Isolated VLAN over PVLAN-trunk.	
Symptom: When the Promiscuous port in the Primary VLAN is Tagged, an ARP request may be forwarded with an incorrect VLAN tag.	
Workaround: Use Untagged port on Primary VLAN.	
Probability: Medium	
Feature: FI L2	**Function:** Forwarding - Private VLAN
Reported In Release: FI 07.3.00	**Service Request ID:** 721623

Defect ID: DEFECT000402371	**Technical Severity:** High
Summary: The "system-max hw-ip-route-tcam" CLI command should be blocked for FCX platform	
Symptom: The "system-max hw-ip-route-tcam <number>" command is not relevant for FCX platform but is still accepted. If it is mistakenly configured, it can cause a side-effect where some routes are prevented from being programmed in the TCAM, thereby causing IP connectivity loss.	
Workaround: Remove the "system-max hw-ip-route-tcam <number>" command from FCX configuration, save the configuration and reload the router.	
Probability: Medium	
Feature: FCX Layer1 features	**Function:** System-max parameters
Reported In Release: FI 07.2.02	**Service Request ID:** 733961

Defect ID: DEFECT000403066	**Technical Severity:** Medium
Summary: If a router is upgraded directly from 4.x code version to 7.2, SSH access to the device could result in a system reset	
Symptom: If a router is upgraded directly from version 4.3 to 7.2 or later code without regenerating the SSH key, the system may reset if an SSH access is attempted.	
Workaround: 1. Invoke the "crypto key gen" command to regenerate the key after the upgrade. 2. Upgrade the device first from version 4.x to 7.1, and then upgrade it from 7.1 to 7.2 or later code streams.	
Probability: Medium	
Feature: FI Embedded Management	**Function:** SSHV2/SCP
Reported In Release: FI 07.3.00	**Service Request ID:** 733057

Defect ID: DEFECT000404560	**Technical Severity:** Critical
Summary: FLS may unexpectedly reset when a new MAC address is being learned due to an invalid port index	
Symptom: In a rare instance, FLS may experience an unexpected system reset when a new MAC address is being learned.	
Probability: Low	
Feature: FCX L2 Forwarding	**Function:** MAC Table/FDB Manager
Reported In Release: FI 07.1.00	**Service Request ID:** 738767

Customer reported defects closed with code in Release R07.2.02f

Defect ID: DEFECT000315704	**Technical Severity:** High
Summary: VE interface's line protocol remains up even if interface itself is not	
Symptom: The outputs of "show ip interface" and "show interface ve" display a given VE's line protocol as 'Up' even though the interface is not enabled.	
Probability: High	**Risk of Fix:** Medium
Feature: FCX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Virtual interface (ve) Manager
Reported In Release: FI 07.1.00	**Service Request ID:** 259859

Defect ID: DEFECT000328636	**Technical Severity:** Medium
Summary: Boot code cannot be upgraded when using only an IPv6 address	
Symptom: If an IPv6 address is used for upgrading the boot code, the TFTP request is not sent from the Switch, resulting in a TFTP timeout error. As a result the boot code cannot be upgraded.	
Workaround: Use IPv4 for upgrading the boot code.	
Probability: High	**Risk of Fix:** Low
Feature: SX_SYSTEM	**Function:** UNDETERMINED
Reported In Release: FI 07.2.00	**Service Request ID:** 269493

Defect ID: DEFECT000331756	**Technical Severity:** Medium
Summary: OSPF point-to-point is configurable on a VE even though it is not supported	
Symptom: The command "ip ospf network point-to-point" is accepted for virtual interfaces via CLI even though it is not supported, and yields unpredictable results.	
Probability: High	**Risk of Fix:** Low
Feature: OSPF	**Function:** OSPF
Reported In Release: FI 07.2.00	**Service Request ID:** 269910

Defect ID: DEFECT000333308	**Technical Severity:** High
Summary: Configuring inline power on a port of a non-PoE FGS switch will cause the system to reset	
Symptom: On a non-PoE FGS switch, configuring "inline power" on a port that is disabled or disconnected causes the switch to reset immediately.	
Probability: High	
Feature: Power over Ethernet	**Function:** Power over Ethernet
Reported In Release: FI 07.2.02	**Service Request ID:** 666731 651017 695411

Defect ID: DEFECT000333939	**Technical Severity:** Medium
Summary: Access-list to permit/deny ICMP with certain types doesn't work	
Symptom: Access list does not honor different types of ICMP packets in transit traffic if the access-list also contains filters for TCP ports. All ICMP types will be permitted or denied.	
Workaround: Do not apply filter with TCP ports in addition to ICMP types.	
Probability: Low	**Risk of Fix:** Low
Feature: SX ACL	**Function:** ACL(all aspects of ACLs - IPV4)
Reported In Release: FI 07.2.00	**Service Request ID:** 514363

Defect ID: DEFECT000334383	**Technical Severity:** Medium
Summary: With "delay-link-event" configured to dampen port flapping, unnecessary Syslog messages are generated if a 10G port goes down	
Symptom: With "delay-link-event" configured to dampen port flapping, unnecessary Syslog messages are generated if a 10G port goes down.	
Probability: Low	**Risk of Fix:** Low
Feature: SX Layer1 features	**Function:** port flap dampening
Reported In Release: FI 07.2.00	**Service Request ID:** 624889

Defect ID: DEFECT000336454	**Technical Severity:** Critical
Summary: Reloading an SX system that has a diagnostic error detected on a Line Module causes the Standby Management module to enter a reset cycle	
Symptom: If a line module is detected as having failed a fabric adapter diagnostic test by the Active Management module during system bring up, the Standby module will enter a reset cycle and will fail to come up.	
Workaround: Remove the Standby Management module from the system and issue a reload. Once the Active Management module brings up the system and resolves the diagnostic failure on the given line module, reinsert the Standby module.	
Probability: Low	**Risk of Fix:** Low
Feature: FI Platform Specific features	**Function:** Management module redundancy
Reported In Release: FI 07.3.00	**Service Request ID:** 702371

Defect ID: DEFECT000340287	**Technical Severity:** Low
Summary: "show media" can cause ports configured with UDLD to flap	
Symptom: Issuing "show media" on an SX system can cause UDLD timers to expire and ports that have UDLD configured will flap.	
Workaround: Increase the UDLD timeout values in order to prevent the timers from expiring.	
Probability: Medium	**Risk of Fix:** Low
Feature: FI Embedded Management	**Function:** CLI and parser
Reported In Release: FI 07.3.00	**Service Request ID:** 689327

Defect ID: DEFECT000344548	**Technical Severity:** Medium
Summary: Unexpected Flow Control behavior when negotiation is enabled on one end and flow control is disabled on the other	
Symptom: Flow control operational state on the interface is displayed as being enabled when it should be disabled.	
Workaround: Disable and re-enable one of the ports or disconnect and reconnect the UTP cable.	
Probability: Low	
Feature: FCX Layer1 features	**Function:** Auto Negotiation
Reported In Release: FI 07.2.02	**Service Request ID:** 544899

Defect ID: DEFECT000346395	**Technical Severity:** Critical
Summary: In rare cases, an unexpected reset of the device may be experienced when sFlow is enabled.	
Symptom: In rare cases an unexpected reset of the device may be experienced when sFlow is enabled.	
Workaround: Disable sFlow.	
Probability: Low	**Risk of Fix:** Low
Feature: FCX Network Management	**Function:** sFlow
Reported In Release: FI 07.3.00	**Service Request ID:** 668067

Defect ID: DEFECT000351270	**Technical Severity:** High
Summary: When an FCX stack is reloaded, the Standby unit may reset unexpectedly	
Symptom: When an FCX stack is reloaded or if the power cord to the Active unit is removed while the stack is up, the Standby unit may experience an unexpected reset.	
Probability: Low	**Risk of Fix:** Low
Feature: FCX L2 Forwarding	**Function:** MAC Table/FDB Manager
Reported In Release: FI 07.3.00	**Service Request ID:** 690585

Defect ID: DEFECT000351317	**Technical Severity:** High
Summary: When a switchover is done on SX, trace messages appear on the console as a result of CPU buffers not being freed	
Symptom: When a switchover is done on SX, during Active to Standby management module synchronization, trace messages appear on the console as a result of CPU buffers not being freed.	
Probability: Low	**Risk of Fix:** Low
Feature: FI Infrastructure	**Function:** SX Hitless Failover
Reported In Release: FI 07.3.00	**Service Request ID:** 683651

Defect ID: DEFECT000354876	**Technical Severity:** Low
Summary: "show version" truncates the full binary image name on non-active units	
Symptom: If a long image name or a long TFTP server directory path is used, a truncated rather than full name is shown on the Standby and member units' flash partitions when "show version" is issued.	
Probability: Medium	**Risk of Fix:** Medium
Feature: FCX Management Functionality	**Function:** CLI and parser
Reported In Release: FI 07.3.00	**Service Request ID:** 686721

Defect ID: DEFECT000361448	**Technical Severity:** Medium
Summary: IP Default Route's hardware entry is not updated although the software entry is updated after failover.	
Symptom: If the configured Static Default Route is deleted after a failover and the best default route is now through OSPF, the OSPF route is updated in software but not in hardware.	
Probability: High	**Risk of Fix:** Medium
Feature: FI L3 Unicast	**Function:** Forwarding - SX v4
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000362369	**Technical Severity:** Medium
Summary: Spanning Tree states of ports of a single LACP trunk are different after a hitless failover on FCX stack	
Symptom: If Spanning Tree is disabled on an LACP trunk, after hitless failover on the FCX stack, Spanning Tree state of the primary port is shown correctly as "OFF", but is shown incorrectly as "ON" for all the member ports.	
Workaround: Disable Spanning Tree for the relevant trunk ports inside the VLAN configuration instead of disabling directly on the ports.	
Probability: Medium	
Feature: FCX L2 Control	**Function:** LinkAggregation - LACP/Dynamic
Reported In Release: FI 07.2.02	**Service Request ID:** 645709

Defect ID: DEFECT000362807	**Technical Severity:** Critical
Summary: The newly elected Active Management module may reset after a switchover due to incomplete synchronization of ARP entries	
Symptom: After doing a Switchover on SX, a flood of error messages indicating an invalid next hop entry are seen, followed by the Active Management module experiencing a reset.	
Probability: Medium	**Risk of Fix:** Medium
Feature: FI L3 Unicast	**Function:** Forwarding - SX v4
Reported In Release: FI 07.3.00	**Service Request ID:** 683651

Defect ID: DEFECT000364929	**Technical Severity:** High
Summary: Excessive warning messages about route entries may be seen during switchover on SX	
Symptom: After system bring up and then a switchover on SX, excessive warning messages concerning route prefixes may be seen on the console.	
Probability: Low	**Risk of Fix:** Medium
Feature: FI L3 Unicast	**Function:** Control Plane - Other
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000366482	**Technical Severity:** Medium
Summary: On FCX, broadcast/multicast/unknown-unicast rate limiting is not accurate on 100Mb links	
Symptom: When Broadcast/Multicast/Unknown-Unicast rate limiting is configured on a port that is running at 100Mb speed, there is a large difference between the observed rate and the configured rate on the egress side.	
Probability: High	**Risk of Fix:** Low
Feature: FI Traffic conditioning and Monitoring	**Function:** broadcast/multicast unknown unicast Rate Limiting
Reported In Release: FI 07.3.00	**Service Request ID:** 700647

Defect ID: DEFECT000366740	**Technical Severity:** High
Summary: Standby Management module may reset unexpectedly after hitless failover due to a watchdog reset	
Symptom: Standby Management module may reset unexpectedly after hitless failover due to a watchdog reset when trying to delete an ARP entry and its associated IPv4 Next Hop entry.	
Probability: Low	**Risk of Fix:** Medium
Feature: FI Infrastructure	**Function:** SX Hitless Failover
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000368019	**Technical Severity:** Medium
Summary: FastIron drops ServerIron Hot Standby HA MAC sync PDUs sent or received on ports configured for UDLD.	
Symptom: Configuring UDLD between an FWS or FGS switch and each ADX in a hot standby ServerIron pair leads to the standby ServerIron not being able to learn MAC addresses on the UDLD-configured port.	
Workaround: Disable UDLD on the intermediate FGS/FWS devices in order to prevent UDLD from interfering with the MAC Sync PDU's on ServerIron devices.	
Probability: Medium	
Feature: SX L2 Control	**Function:** UDLD
Reported In Release: FI 07.2.02	**Service Request ID:** 670755

Defect ID: DEFECT000369368	**Technical Severity:** Medium
Summary: SX momentarily forwards packets during boot up process	
Symptom: During boot up process, SX forwards packets on a port for a short time when initializing that port even though it is disabled in the saved configuration.	
Probability: Medium	
Feature: SX Layer1 features	**Function:** link status - speed and duplex status
Reported In Release: FI 07.2.02	**Service Request ID:** 669641

Defect ID: DEFECT000371093	**Technical Severity:** High
Summary: sFlow may not work on member units of an FGS stack	
Symptom: Although sFlow works as expected on FGS standalone units or master units of a stack, it may not work on member units if the sFlow polling interval is not set to Zero.	
Workaround: Set the 'sflow polling-interval' to zero in order to send the sFlow samples.	
Probability: High	
Feature: FCX Network Management	**Function:** sFlow
Reported In Release: FI 07.2.02	

Defect ID: DEFECT000371615	**Technical Severity:** High
Summary: Standby unit of FCX stack may reset after Hitless Failover if OSPFv2 graceful restart is disabled	
Symptom: If RIPv2 and OSPFv2 neighborhoods are formed on the same interface with the OSPF default route chosen as the best route, issuing a "no-graceful restart" and then doing a failover can lead to a reset on the Standby Management module.	
Probability: Low	**Risk of Fix:** Low
Feature: Layer3 Control Protocols	**Function:** RIP(v1-v2) - IPV4
Reported In Release: FI 07.4.00	**Service Request ID:** 695341

Defect ID: DEFECT000374592	**Technical Severity:** Medium
Summary: After a trunk is unconfigured, IP forwarding to ports that were previously part of that trunk may not work.	
Symptom: IP forwarding to ports that were previously part of a trunk may not work after the trunk is deleted.	
Workaround: Reload the system to re-initialize the ports correctly for IP forwarding.	
Probability: Medium	
Feature: SX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.2.02	**Service Request ID:** 681463

Defect ID: DEFECT000375025	**Technical Severity:** Medium
Summary: Packets destined to the VRRP Virtual MAC address are received by the CPU of the VRRP Backup Router	
Symptom: Packets destined to the VRRP Virtual MAC address are received by the CPU of the VRRP Backup Router instead of being switched in HW to the VRRP Master.	
Probability: High	
Feature: SX Layer3 Control Protocols	**Function:** VRRP/VRRP-E and slow-start timer-VRRP-E timer scale
Reported In Release: FI 07.2.02	**Service Request ID:** 674521

Defect ID: DEFECT000375567	**Technical Severity:** Medium
Summary: If hitless OS upgrade between incompatible SW code versions is attempted, a system reset may be experienced.	
Symptom: If hitless OS upgrade between incompatible SW code versions is attempted, a system reset may be experienced.	
Workaround: Issue a regular 'reload' or 'boot system flash primary/secondary' instead of hitless-reload to upgrade.	
Probability: High	**Risk of Fix:** Low
Feature: FI Infrastructure	**Function:** SX Hitless OS upgrade
Reported In Release: FI 07.3.00	**Service Request ID:** 680843

Defect ID: DEFECT000376558	**Technical Severity:** Medium
Summary: Standby unit may reset if the Active stack unit is unplugged from power during hitless failover	
Symptom: When hitless failover is configured and power is disconnected from the Active FCX of a stacked pair running OSPFv2, the other FCX may reset soon afterwards. When it later recovers, all its interfaces will remain down.	
Probability: Low	
Feature: FCX Layer3 Control Protocols	**Function:** OSPFV2 - IPV4
Reported In Release: FI 07.2.02	**Service Request ID:** 682809

Defect ID: DEFECT000377048	**Technical Severity:** Medium
Summary: After stack failover causes preferred RIPv2 route to get deleted, backup Static route does not take over	
Symptom: If only the Active unit has RIP reachability and learns a better route than a configured Static route for a given IP Next Hop, upon disabling power to the Active unit, the ensuing failover does not move up the Static route as the best route on the new Active unit.	
Probability: Medium	
Feature: FCX Layer3 Control Protocols	**Function:** RIP(v1-v2) - IPV4
Reported In Release: FI 07.2.02	**Service Request ID:** 683931

Defect ID: DEFECT000377054	**Technical Severity:** Medium
Summary: FCX "E" type FAN displays erroneous airflow direction in "show chassis" output	
Symptom: The output of "show chassis" on FCX displays the airflow for "E" type fan as Back to Front even though the fan actually provides airflow from the front to the back.	
Probability: Medium	**Risk of Fix:** Low
Feature: FI Platform	**Function:** Power Supply/Temp Sensor/Fan Controller
Reported In Release: FI 07.3.00	**Service Request ID:** 686691

Defect ID: DEFECT000377090	**Technical Severity:** Medium
Summary: MAC table is not updated correctly when client is moved from PVLAN primary to PVLAN community or from PVLAN community to PVLAN primary	
Symptom: MAC table is not updated correctly when client is moved from PVLAN primary to PVLAN community or from PVLAN community to PVLAN primary.	
Probability: High	
Feature: FCX L2 Forwarding	**Function:** Private VLAN
Reported In Release: FI 07.2.02	**Service Request ID:** 687429

Defect ID: DEFECT000377099	**Technical Severity:** Medium
Summary: Interface and Port descriptions for 10/100M ports on some FWS models are incorrectly displayed as 'GigabitEthernet'	
Symptom: On non-Gigabit capable FWS models (FWS624, FWS624-EPREM, FWS624-POE, FWS648, FWS648-EPREM & FWS648-POE), ifDescr and port description for 10/100M ports are displayed as 'GigabitEthernet' instead of 'FastEthernet'.	
Probability: High	**Risk of Fix:** Low
Feature: FCX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 07.2.00	**Service Request ID:** 683989

Defect ID: DEFECT000377535	**Technical Severity:** Medium
Summary: FCX stack with 10G ports breaks when upgraded from 7.2.02d to 7.2.02e	
Symptom: FCX stack with 10G ports breaks when upgraded from 7.2.02d to 7.2.02e	
Probability: High	
Feature: FCX Stacking	**Function:** stack-ports
Reported In Release: FI 07.2.02	**Service Request ID:** 686589

Defect ID: DEFECT000377762	**Technical Severity:** Critical
Summary: SX Standby Management module unexpectedly resets after 231 days	
Symptom: On SX platform, after 231 days of continuous uptime, the Standby Management module unexpectedly resets with a log message "Mgmt CPU1 (slot 10) failed".	
Probability: High	**Risk of Fix:** Low
Feature: SX Platform Specific features	**Function:** Management module redundancy
Reported In Release: FI 07.2.00	**Service Request ID:** 682807

Defect ID: DEFECT000377873	**Technical Severity:** High
Summary: If multiple 0.0.0.0 route updates over RIPv2 with netmasks other than /0 from multiple neighboring routers are received, the device could lock up or reset	
Symptom: Upon receiving multiple 0.0.0.0 route updates over RIPv2 with non-zero netmasks, continuous route updates for 0.0.0.0 will be emitted by the affected system. FCX devices may experience a lockup while FESX/SX devices may experience a reset.	
Probability: High	
Feature: FCX Layer3 Control Protocols	**Function:** RIP(v1-v2) - IPV4
Reported In Release: FI 07.2.02	**Service Request ID:** 685879

Defect ID: DEFECT000378514	**Technical Severity:** Medium
Summary: One ICMP packet is lost every 60 seconds over a cross unit trunk when one switch in a stack of 2 goes down	
Symptom: In a stack of two FCX switches containing a 2-port trunk with one port on each chassis, if one of the switches is powered off, ICMP through the FCX shows one packet is lost every 60 seconds.	
Probability: High	**Risk of Fix:** Low
Feature: FCX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.3.00	**Service Request ID:** 687111

Defect ID: DEFECT000379697	**Technical Severity:** Critical
Summary: ARP age is not refreshed after disabling/enabling a module even though there is constant traffic from/to the host	
Symptom: ARP age is not refreshed after disabling/enabling the module even though there is constant traffic from/to the host	
Probability: High	
Feature: SX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.2.02	**Service Request ID:** 691653

Defect ID: DEFECT000381074	**Technical Severity:** Medium
Summary: Logical VE interface remains UP even though none of its associated physical ports are enabled	
Symptom: With Single Spanning Tree enabled, even if all the physical ports of a VLAN are down, the associated VE interface is displayed as being logically up under "show ip interface".	
Probability: High	
Feature: FCX Layer1 features	**Function:** link status - speed and duplex status
Reported In Release: FI 07.2.02	**Service Request ID:** 675563

Defect ID: DEFECT000382104	**Technical Severity:** Medium
Summary: When the active FCX switch in a stack fails, OSPF routes that had depended on ve interfaces using the failed switch's physical interfaces remain in the routing table with OSPF cost "n/a".	
Symptom: Loss of connectivity lasting 90 seconds in 7.3 and lasting indefinitely in 7.2.02e when the active FCX in a stack goes down.	
Probability: High	
Feature: FCX Layer3 Control Protocols	**Function:** OSPFV2 - IPV4
Reported In Release: FI 07.2.02	**Service Request ID:** 683169

Defect ID: DEFECT000382236	**Technical Severity:** Medium
Summary: SNMP ifOperStatus reports ports in STP Blocking as down even though the ports are physically and administratively up	
Symptom: SNMP ifOperStatus reports ports in STP Blocking as down even though the ports are physically and administratively up.	
Probability: Medium	
Feature: FCX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 07.2.02	**Service Request ID:** 696127

Defect ID: DEFECT000382390	**Technical Severity:** Medium
Summary: New active port of protected-link-group over stacking units does not handle any traffic	
Symptom: With a protected-link group configured over multiple units of a stack, after the Active unit of the Stack is powered off, the new Active unit's port does not handle any traffic even though the interface moves to Forwarding state.	
Workaround: Configure an 'active-port' for the protected link group.	
Probability: Low	
Feature: FCX L2 Forwarding	**Function:** Protected Link group
Reported In Release: FI 07.2.02	**Service Request ID:** 694309

Defect ID: DEFECT000383469	**Technical Severity:** Medium
Summary: A Layer 2 loop may be created if the Native VLAN Id is changed on other vendors' switches	
Symptom: If the Native VLAN Id is changed from the default on other vendors' switches that are connected to a Brocade device, a Layer 2 loop may result due to the Brocade device expecting an IEEE BPDU in the default VLAN 1.	
Workaround: Configure the Native VLAN to default value 1 on the other vendor's switch or configure VLAN 1 on the interface connected to the Brocade device.	
Probability: Low	**Risk of Fix:** Low
Feature: FCX L2 Control	**Function:** PVST/PVST+/ PVRST
Reported In Release: FI 07.3.00	**Service Request ID:** 670195

Defect ID: DEFECT000386563	**Technical Severity:** High
Summary: After the previous Master unit of an FCX stack goes down, the new Master unit may reset when commands related to traffic statistics are executed	
Symptom: After the Master unit of a 2-node FCX stack is powered down, the new Master unit may reset if certain commands like "show statistics traffic-policy" or "show access-list" are issued from CLI.	
Probability: Low	
Feature: FCX Stacking	**Function:** IPC Infrastructure
Reported In Release: FI 07.2.02	**Service Request ID:** 705189

Defect ID: DEFECT000386695	**Technical Severity:** Medium
Summary: Standby port of a protected-link group on new Active stack controller does not discard any packets	
Symptom: Standby port of a protected-link group on new Active stack controller does not discard any packet	
Probability: High	
Feature: FCX L2 Control	**Function:** LinkAggregation - LACP/Dynamic
Reported In Release: FI 07.2.02	**Service Request ID:** 705187

Defect ID: DEFECT000387044	**Technical Severity:** High
Summary: FCX E/I shows PSU 2 as normal when inserted without power	
Symptom: 2nd PSU without power shows as normal and plugged in. Occurs in 7.202a, 7202f, and 7.3.	
Probability: High	**Risk of Fix:** Low
Feature: FI Platform Specific features	**Function:** Chassis/fan/powersupplies/temperature sensors
Reported In Release: FI 07.3.00	**Service Request ID:** 707887

Defect ID: DEFECT000387141	**Technical Severity:** Medium
Summary: Port status changes to Blocking although Protected-link-status is Active after Stack Failover/Switchover	
Symptom: After the active ports of a cross-unit protected link group on an FCX stack are flapped a few times and a failover or switchover is then done, the expected Active port of the protected link group is shown to be in Blocked state.	
Probability: High	
Feature: FCX L2 Control	**Function:** LinkAggregation - LACP/Dynamic
Reported In Release: FI 07.2.02	**Service Request ID:** 705571

Customer reported defects closed with code in Release R07.2.02e

Defect ID: DEFECT000330146	**Technical Severity:** High
Summary: Newly inserted Management Module may have invalid LID displayed, after which the module cannot be upgraded via SW Licensing.	
Symptom: On the Standby module, the LID value is displayed as ÿÿÿÿÿÿÿÿÿÿ. After a failover, the new Active will have this same LID and thus cannot be upgraded.	
Probability: High	
Feature: SX Management Functionality	**Function:** CLI and parser
Reported In Release: FI 07.2.02	**Service Request ID:** 595349

Defect ID: DEFECT000338861	**Technical Severity:** High
Summary: Device unexpectedly reloads when using SHA to verify sanctity of flash images.	
Symptom: Device unexpectedly reloads when "verify sha <primary/secondary>" command is executed.	
Probability: High	
Feature: FI Embedded Management	**Function:** CLI and parser
Reported In Release: FI 07.3.00	**Service Request ID:** 642003

Defect ID: DEFECT000338864	**Technical Severity:** Medium
Summary: Verification of flash images using MD5 gives incorrect and unpredictable results.	
Symptom: When “verify md5 <primary/secondary>” is issued, the first run after a reboot returns all zeros. Subsequent runs will show incorrect file size and MD5 hash.	
Probability: High	
Feature: FI Embedded Management	**Function:** CLI and parser
Reported In Release: FI 07.3.00	**Service Request ID:** 642003, 645141

Defect ID: DEFECT000343157	**Technical Severity:** Medium
Summary: 2500W PoE power supply is misidentified as a 1250W power supply.	
Symptom: 2500W power supply can allocate only half its capacity and is displayed incorrectly as 1350W or 1250W in the output of "show inline power detail" and "show power" commands.	
Probability: High	
Feature: FI Platform Specific features	**Function:** Chassis/fan/power supplies/temperature sensors
Reported In Release: FI 07.3.00	**Service Request ID:** 641069

Defect ID: DEFECT000344380	**Technical Severity:** Medium
Summary: FCX IP traffic goes to the CPU if it ingresses an IP Subnet VE interface.	
Symptom: IP traffic goes to CPU with a VE interface configured on an IP Subnet VLAN, or if the VE is created first before adding ports to the VLAN.	
Probability: High	
Feature: FI L2	**Function:** Forwarding - VLAN Manager
Reported In Release: FI 07.3.00	**Service Request ID:** 646619

Defect ID: DEFECT000345298	**Technical Severity:** High
Summary: IPv6 functionality is dependent only on HW EPROM licensing even if the system is upgraded via SW Licensing.	
Symptom: Although IPv6 commands are configurable on a system that is upgraded via SW Licensing, a directly connected IPv6 neighbor is not reachable.	
Probability: High	
Feature: SX Layer 3 Forwarding - IPV6	**Function:** Host Networking stack (IPV6)
Reported In Release: FI 07.3.00	**Service Request ID:** 640715

Defect ID: DEFECT000347484	**Technical Severity:** High
Summary: Memory leak may be observed when Policy Based Routing is configured.	
Symptom: When Policy Based Routing is dynamically configured or removed from the configuration, the memory consumption may increase continuously, eventually leading to a system reset.	
Probability: High	
Feature: FI L3 Unicast	**Function:** Forwarding – PBR
Reported In Release: FI 07.3.00	**Service Request ID:** 672437

Defect ID: DEFECT000353729	**Technical Severity:** Medium
Summary: FastIron switches may not respond to ICMPv6 echo request.	
Symptom: FESX, FCX and FGS switches may fail to reply to ICMPv6 echo request sent by router or IPV6 server (Linux) that is directly connected to the switch.	
Probability: High	
Feature: FCX Layer 3 Forwarding - IPV6	**Function:** Data Forwarding (IPV6)
Reported In Release: FI 07.2.02	**Service Request ID:** 611321

Defect ID: DEFECT000354169	**Technical Severity:** Medium
Summary: A system memory leak may be seen on devices configured with PIM Routing.	
Symptom: Stack trace messages are printed on the console while the "show memory" output shows a rapid increase in memory consumption, eventually leading to a system reload.	
Probability: Medium	
Feature: SX L2/L3 Multicast Features	**Function:** PIM Sparse
Reported In Release: FI 07.3.00	**Service Request ID:** 670015

Defect ID: DEFECT000355497	**Technical Severity:** Medium
Summary: FCX cannot process ARP Requests at a high rate.	
Symptom: FCX does not process more than 256 ARP Request packets per second.	
Probability: High	
Feature: FCX Layer 3 Forwarding - IPV4	**Function:** Host Networking stack (IPV4)
Reported In Release: FI 07.2.02	**Service Request ID:** 625975, 653983

Defect ID: DEFECT000355653	**Technical Severity:** Medium
Summary: FWS does not allow Port-based Mirroring and VLAN-based Mirroring on the same port to be configured.	
Symptom: Port-based Mirroring and VLAN-based Mirroring is not permitted simultaneously on the same port on FWS platform, even though it is supported on FCX platform.	
Probability: Medium	
Feature: FI Traffic conditioning and Monitoring	**Function:** port mirroring/monitoring
Reported In Release: FI 07.2.02	**Service Request ID:** 614459

Defect ID: DEFECT000356155	**Technical Severity:** Medium
Summary: After the Master unit in a stack goes down, OSPF routes that used this disabled unit's ports can remain in the routing table indefinitely.	
Symptom: After the Master unit in an FCX stack goes down, OSPF routes that used this disabled unit's ports will remain in the routing table indefinitely.	
Workaround: Disable OSPF graceful restart by configuring "no graceful-restart" under "router ospf" on the stacked FCX before the active FCX goes down. With graceful restart disabled, loss of connectivity is reduced from 120 seconds to about 45 seconds.	
Probability: High	
Feature: OSPF	**Function:** OSPF
Reported In Release: FI 07.2.02	**Service Request ID:** 632283

Defect ID: DEFECT000356415	**Technical Severity:** Critical
Summary: System unexpectedly resets after becoming unresponsive.	
Symptom: Device displays LID message, then freezes and is unresponsive even from console.	
Probability: Low	
Feature: Sw licensing	**Function:** Licensing All
Reported In Release: FI 07.3.00	**Service Request ID:** 642829

Defect ID: DEFECT000357491	**Technical Severity:** Medium
Summary: Rare error during baseline synchronization between Active and Standby Management modules may lead to unexpected system reset.	
Symptom: In very rare cases during baseline synchronization stage, an error may occur that can lead to unexpected system reset.	
Probability: Low	
Feature: SX Platform Specific features	**Function:** Management module redundancy
Reported In Release: FI 07.2.00	**Service Request ID:** 266664

Defect ID: DEFECT000357789	**Technical Severity:** Medium
Summary: After reload, CRC errors are seen on the link partner of member trunk ports.	
Symptom: If a trunk is configured with member ports on two or more units and the ports used are default stacking ports, on reload of the stack, the link partner of the trunk member ports will observe CRC errors.	
Workaround: Delete the trunk configuration, configure long-preamble on the trunk interfaces and then re-deploy the trunk.	
Probability: Medium	
Feature: FCX Stacking	**Function:** stack-ports
Reported In Release: FI 07.2.02	**Service Request ID:** 633009

Defect ID: DEFECT000358149	**Technical Severity:** High
Summary: Watchdog reset may occur during system bring-up.	
Symptom: During reboot, system may become unresponsive and reload unexpectedly.	
Probability: Low	
Feature: FI Platform Specific features	**Function:** system bringup
Reported In Release: FI 07.3.00	**Service Request ID:** 642829

Defect ID: DEFECT000359744	**Technical Severity:** Medium
Summary: FESX code flash memory size is displayed incorrectly.	
Symptom: FESX code flash memory is displayed as 16MB even if it is only 8MB in size.	
Probability: High	
Feature: SX Management Functionality	**Function:** CLI and parser
Reported In Release: FI 07.2.02	**Service Request ID:** 640449

Defect ID: DEFECT000360173	**Technical Severity:** High
Summary: After enabling Single Spanning-Tree and reloading the device, the first port of the system may be removed from VLAN 1.	
Symptom: After 'spanning-tree single' is configured on the device and it is reloaded, Eth1 may be removed from VLAN1.	
Probability: High	
Feature: SX L2 Control	**Function:** single spanning-tree
Reported In Release: FI 07.2.02	**Service Request ID:** 643797

Defect ID: DEFECT000361466	**Technical Severity:** Medium
Summary: Cannot communicate between Primary and Isolated Private VLANs.	
Symptom: It is not possible to communicate between Primary and Isolated VLAN when Private VLANs are configured.	
Probability: High	
Feature: SX L2 Forwarding	**Function:** Private VLAN
Reported In Release: FI 07.2.02	**Service Request ID:** 636621, 650833

Defect ID: DEFECT000362478	**Technical Severity:** Medium
Summary: When CPU intensive tasks like repeated TFTP uploads are done, it may lead to loss of heartbeat from Active to Standby Management modules, resulting in a switchover.	
Symptom: When repeated TFTP uploads are done via INM, a switchover may be observed.	
Probability: Low	
Feature: SX Platform Specific features	**Function:** Management module redundancy
Reported In Release: FI 07.2.02	**Service Request ID:** 592699

Defect ID: DEFECT000364076	**Technical Severity:** High
Summary: ARP request is not forward between Primary and Isolated VLANs.	
Symptom: When Private VLANs are configured, an ARP request is not forward between the Primary and Isolated VLANs.	
Probability: High	
Feature: FCX L2 Forwarding	**Function:** Private VLAN
Reported In Release: FI 07.2.02	**Service Request ID:** 650833

Defect ID: DEFECT000364534	**Technical Severity:** Medium
Summary: When the Master unit of a stack is powered off, the ARP entries that are bound to ports on that unit are not updated even though the MAC entries are updated correctly.	
Symptom: FCX fails to transmit L3 routing packet when the stack's Master unit is powered off. 'show arp' shows a port on the old Master unit which is now inactive.	
Workaround: 1) Issue clear arp. 2) Do a switchover between Active and Standby by CLI and then power off the new Standby (old Active).	
Probability: High	
Feature: FCX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.2.02	**Service Request ID:** 658785

Defect ID: DEFECT000365673	**Technical Severity:** Medium
Summary: ARP request is not received from host directly connected to a 48 port line module.	
Symptom: Cannot ping SX router from a PC that is directly connected to a 48 port line card.	
Probability: High	
Feature: SX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.2.02	**Service Request ID:** 646649

Defect ID: DEFECT000365696	**Technical Severity:** High
Summary: A Layer 2 Multicast Client may not be able to receive a multicast stream when PIM Dense Mode is configured.	
Symptom: When FCX is running PIM Dense Mode, some Layer 2 receivers may not receive the data.	
Probability: Medium	
Feature: FCX L2/L3 Multicast Features	**Function:** PIM Dense
Reported In Release: FI 07.2.02	

Defect ID: DEFECT000366413	**Technical Severity:** Critical
Summary: Static default route does not get updated after the master unit of the stack goes down.	
Symptom: If there are multiple static default routes from both master and non-master units, the default route from the master unit is correctly displayed in the routing table. But if the master unit is powered down, this route will still be displayed instead of the route from the non-master unit.	
Probability: High	
Feature: FCX Layer 3 Forwarding - IPV4	**Function:** STATIC ROUTES (IPV4)
Reported In Release: FI 07.2.02	**Service Request ID:** 665605

Defect ID: DEFECT000366766	**Technical Severity:** High
Summary: OSPFv2 Type4 ASBR Summary LSA is removed if the neighbor ASBR's interface in the same area is deleted.	
Symptom: ASBR route is not advertised properly and subsequently, redistributed routes are not installed in the routing table.	
Probability: High	
Feature: FI L3 Unicast	**Function:** Control Plane - OSPF/OSPFv3
Reported In Release: FI 07.3.00	**Service Request ID:** 642515

Defect ID: DEFECT000368465	**Technical Severity:** High
Summary: When the sFlow collector is configured on a VE, FCX member units may reload unexpectedly.	
Symptom: When adding/removing RSTP config from the VLAN, member units may reload if sFlow is configured on the VE for that VLAN.	
Workaround: Disable sFlow or configure the collector on a physical interface instead of on the VE.	
Probability: High	
Feature: FCX Network Management	**Function:** sFlow
Reported In Release: FI 07.2.02	**Service Request ID:** 669137

Defect ID: DEFECT000368913	**Technical Severity:** Medium
Summary: Memory tracking debug command may not work for all cases.	
Symptom: Some memory leak conditions may not be detected using the “dm mem-leak” tool.	
Probability: Low	
Feature: SX_SYSTEM	**Function:** UNDETERMINED
Reported In Release: FI 07.2.02	

Defect ID: DEFECT000369317	**Technical Severity:** Medium
Summary: Layer 3 connectivity is lost and ARP error messages are displayed on the console.	
Symptom: Messages such as "pp_find_arp_entry failed to create ARP entry" are seen on the console, while connectivity to the Internet is lost.	
Probability: High	
Feature: FCX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.2.02	**Service Request ID:** 671567

Open defects in Release 07.2.02e

The following table lists the defect that is open in release 07.2.02e.

Defect ID: DEFECT000344548	**Technical Severity**: Medium	
Summary: Unexpected Flow Control behavior when negotiation is enabled on one end and flow control is disabled on the other		
Symptom: Flow control operational state on the interface is displayed as being enabled when it should be disabled.		
Workaround: Disable and re-enable one of the ports or disconnect and reconnect the UTP cable.		
Feature: FCX Layer1 features	**Function**: Auto Negotiation	**Probability**: Low
Found in Release: FI 07.2.02	**Service Request ID**: 544899	

Defect ID: DEFECT000371093	**Technical Severity**: High	
Summary: sFlow may not work on member units of an FGS stack		
Symptom: Although sFlow works as expected on FGS standalone units or master units of a stack, it may not work on member units if the sFlow polling interval is not set to Zero.		
Workaround: Set the 'sflow polling-interval' to zero in order to send the sFlow samples.		
Feature: FCX Network Management	**Function**: sFlow	**Probability**: High
Found in Release: FI 07.2.02		

Customer reported defects closed with code in Release R07.2.02

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

Defect ID: DEFECT000298350	**Technical Severity:** Low
Summary: The FCX allows configuration of optical monitoring on SFPs that do not support optical monitoring.	
Probability: High	
Feature: FCX Layer1 features	**Function:** Digital Optical Monitoring
Reported In Release: FI 07.0.01	**Service Request ID:** 244736F

Defect ID: DEFECT000301831	**Technical Severity:** High
Summary: When strict priority is configured on the FGS624P, QoS priority 7 traffic dropped in preference to QoS priority 0 traffic.	
Feature: FCX Quality Of Service	**Function:** TOS/QOS
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000302513	**Technical Severity:** Medium
Summary: Following OSPF area configuration change, type4 LSA may be incorrectly advertized.	
Feature: SX Layer3 Control Protocols	**Function:** OSPFV2 - IPV4
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000309026	**Technical Severity:** Medium
Summary: CLI is not taking more than one monitor command on the link-aggregate interface configuration	
Feature: SX Traffic conditioning and Monitoring	**Function:** port mirroring/monitoring
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000309344	**Technical Severity:** Medium
Summary: A 10G port flapped (down/up) when another port in the same module was manually disabled or re-enabled.	
Feature: SX Layer1 features	**Function:** Auto Negotiation
Reported In Release: FI 07.1.00	

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. It can be ignored 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: DEFECT000321932	**Technical Severity:** High
Summary: SX router performed a system reset during system bringup and layer 3 protocol convergence along with reload of neighboring router.	
Probability: Low	
Feature: SX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Data Forwarding
Reported In Release: FI 07.2.00	

Defect ID: DEFECT000321950	**Technical Severity:** High
Summary: A 48-port FWS or FGS can be made to continuously flood known unicast frames out of all ports.	
Symptom: A 48-port FWS or FGS can be made to continuously flood known unicast frames out of multiple ports. Even though a MAC address appears in output of "show mac" command, frames addressed to that MAC address are flooded out of multiple ports.	
Workaround: Execute "clear mac <address>" against the specific destination MAC address of the flooded frames.	
Probability: High	
Feature: FCX L2 Forwarding	**Function:** MAC Table/FDB Manager
Reported In Release: FI 07.2.00	**Service Request ID:** 258207

Defect ID: DEFECT000322572	**Technical Severity:** Medium
Summary: Setting port speed to 100-full will not take effect unless the switch is reloaded (FESXHF Only)	
Probability: High	
Feature: SX Layer1 features	**Function:** Auto Negotiation
Reported In Release: FI 07.2.00	**Service Request ID:** 263600

Defect ID: DEFECT000324371	**Technical Severity:** Medium
Summary: FCX management port does not reply to IPv6 neighbor advertisement.	
Symptom: Unable to ping FCX IPv6 address after issuing the 'clear ipv6 neighbor' CLI command.	
Workaround: FCX needs to initiate the pingv6 command to other device.	
Probability: High	
Feature: FCX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Data Forwarding
Reported In Release: FI 07.2.00	**Service Request ID:** 266516

Defect ID: DEFECT000324507	**Technical Severity:** Medium
Summary: Router cannot install a router LSA with more than 8304 bytes LSA size and generate a checksum error resulting in the OSPF neighbor staying in LOADING state.	
Probability: Medium	
Feature: OSPF	**Function:** OSPF
Reported In Release: FI 07.2.00	**Service Request ID:** 265202

Defect ID: DEFECT000326611	**Technical Severity:** High
Summary: Executing "dm pp-interrupts counters" command with any device number causes an FESX to reload.	
Workaround: This is a diagnostic command not to be used under normal operating conditions.	
Probability: High	
Feature: SX_SYSTEM	**Function:** UNDETERMINED
Reported In Release: FI 07.2.00	**Service Request ID:** 268470

Defect ID: DEFECT000327840	**Technical Severity:** High
Summary: CPU usage is high due to the next-hop-ip running out of resources.	
Feature: SX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Data Forwarding
Reported In Release: FI 07.1.00	

Defect ID: DEFECT000328563	**Technical Severity:** Medium
Summary: After increasing the system max parameter “system-max hw-ip-route-tcam”, the error message “There is insufficient hardware resource for binding the ACL 100 to interface v1” may be displayed when trying to rebind an ACL.	
Probability: Medium	
Feature: FCX ACL	**Function:** ACL(all aspects of ACLs - IPV4)
Reported In Release: FI 07.2.00	

Defect ID: DEFECT000328635	**Technical Severity:** Medium
Summary: 802.1x per-user ACL cannot be installed if enable password is set and serial console CLI is not in privileged mode	
Symptom: If enable super-user password is configured on the FWS, and also the serial console CLI is not in privileged mode, the switch cannot install the per-user ACL that was received from the RADIUS server in an access-accept message.	
Probability: Medium	
Feature: FCX ACL	**Function:** 802.1x userbased dynamic policies
Reported In Release: FI FGS 04.3.03	**Service Request ID:** 00268592

Defect ID: DEFECT000328640	**Technical Severity:** Medium
Summary: The error "Internal error! var_tree_get_one_entry_prefer_end() no entry but avail=57" is displayed when IP address is created or removed on a virtual interface.	
Symptom: Error message "Internal error! var_tree_get_one_entry_prefer_end() no entry but avail=57" is displayed when the IP address is created or removed on a virtual interface.	
Probability: Low	
Feature: FCX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Virtual interface (ve) Manager
Reported In Release: FI 07.0.01	**Service Request ID:** 268797

Defect ID: DEFECT000331021	**Technical Severity:** Critical
Summary: High CPU condition may occur due to a Next Hop memory leak.	
Symptom: After running out of next hop resource, CPU usage became high because the device failed to allocate the nexthop for hardware routes entries. CPU usage still remained high (96%) even when all interfaces are disabled.	
Probability: Medium	
Feature: SX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Data Forwarding
Reported In Release: FI 07.2.00	**Service Request ID:** 270255

Defect ID: DEFECT000331527	**Technical Severity:** Medium
Summary: Default dead-interval should be 3500 msec and current dead-interval should be 3500 msec" for default timer values.	
Feature: SX Layer3 Control Protocols	**Function:** VRRP/VRRP-E and slow-start timer-VRRP-E timer scale
Reported In Release: FI 07.2.02	

Defect ID: DEFECT000332671	**Technical Severity:** Medium
Summary: Stackable FCX routes packets with the source MAC address of a physical port rather than those with a MAC address of the VE interface.	
Symptom: FCX is not sending the source MAC of the VE Interface.	
Probability: High	
Feature: FCX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Host Networking stack (IPV4 and IPV6)
Reported In Release: FI 07.0.00	**Service Request ID:** 270088F

Customer reported defects closed without code in Release R07.2.02

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

Defect ID: DEFECT000333601	**Technical Severity:** High
Summary: Receiving one RADIUS packet with an erroneous, unparsable attribute breaks the switch's ability to receive RADIUS packets until after the next reload.	
Reason Code: Already Fixed in Release	**Probability:** High
Feature: FCX L2 Forwarding	**Function:** MAC- BASED VLAN
Reported In Release: FI FGS 04.3.03	**Service Request ID:** 508319

Defect ID: DEFECT000323514	**Technical Severity:** Medium
Summary: FCX displays optics alarms although the reading was normal	
Reason Code: Already Fixed in Release	**Probability:** High
Feature: Optics	**Function:** OPTICS
Reported In Release: FI 07.2.00	**Service Request ID:** 264237

Open defects in Release 07.2.02

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

Defect ID: DEFECT000319118	**Technical Severity:** High
Summary: EOP/SOP drop occurs when FESX receives high volume of Priority7 PIM packets.	
Symptom: IP multicast traffic packet loss	
Workaround: Apply an ACL to block the PIM packets	
Feature: SX L2/L3 Multicast Features	**Function:** IGMP snooping and variants

Reported In Release:	FI 07.1.00	**Probability:**	Medium