IronWare Software Release R07.3.00c for Brocade FCX, FESX (IPv6 Models), FSX, FWS, ICX 6610, and TurboIron 24X Switches

Release Notes v4.0

October 18, 2012

Document History

Document Title	Summary of Changes	Publication Date
IronWare Software Release R07.3.00c for Brocade FCX, FESX (IPv6 Models), FSX, FWS, ICX 6610, and TurboIron 24X Switches Release Notes v1.0	Initial release	04/30/2012
IronWare Software Release R07.3.00c for Brocade FCX, FESX (IPv6 Models), FSX, FWS, ICX 6610, and TurboIron 24X Switches Release Notes v2.0	Updated defect list with correct list	05/01/2012
IronWare Software Release R07.3.00c for Brocade FCX, FESX (IPv6 Models), FSX, FWS, ICX 6610, and TurboIron 24X Switches Release Notes v3.0	Updated Symptom information for DEFECT000348267 and DEFECT000377762	06/18/2012
IronWare Software Release R07.3.00c for Brocade FCX, FESX (IPv6 Models), FSX, FWS, ICX 6610, and TurboIron 24X Switches Release Notes v4.0	Corrected POE firmware file names and VCT support	10/18/2012

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

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

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

Contents

Supported devices

The **07.3.00c** software release applies only to the following Brocade products:

- FCX Series (FCX)
- FastIron X Series:
  - FastIron Edge Switch X Series, (IPv6 models) (FESX6)
  - FastIron SX 800 and 1600 (FSX 800 and FSX 1600)
- FastIron WS Series (FWS)
- ICX 6610 Series (ICX 6610)
- TurboIron 24X (TI24X)

Manageability

This 07.3.00c software releases are supported by Brocade Network Advisor 11.2. Any earlier versions of Network Advisor, as well as any version of IronView Network Manager (INM) are not compatible with this release or its supported hardware platforms (see Supported Devices). Network Advisor 11.2 is generally available for download on my.brocade.com. It is strongly recommended that customers upgarde to Network Advisor 11.2, as part of their upgrade to this 07.3.00 software release.

Brocade will continue to address customer issues on INM (unrelated to this 07.3.00b release).

Summary of enhancements

Summary of enhancements in IronWare release R07.3.00c

This release adds support for DHCPv6 relay agent to devices that support IPv6.With DHCPv6 relay agent, you can have interfaces on a device access services from a DHCP Server that doesn't belong to the same network segment. You can configure up to 16 DHCPv6 relay agents on an interface.

Summary of enhancements in IronWare release R07.3.00b

There are no enhancements in software release R07.3.00b.

Summary of enhancements in IronWare release R07.3.00a

There are no enhancements in software release R07.3.00a.

Summary of enhancements in IronWare release R07.3.00

This section describes the enhancements in software release R07.3.00.

New hardware

This release introduces the new ICX 6610 Series of stackable switches.

This release also introduces the following new FastIron SX interface modules:

- 24-port Gigabit Ethernet copper interface module
- 24-port Gigabit Ethernet fiber interface module
- 2-port 10-Gigabit Ethernet interface module
- 8-port 10-Gigabit Ethernet interface module

Summary of enhancements in FCX R07.3.00

Table 1 lists the enhancements in software release 07.3.00 for FCX and ICX 6610 devices.

Table 1 Enhancements in FCX R07.3.00

Feature	Description	See the *FastIron Configuration Guide*, section entitled…
DHCPv6 Relay Agent	Support for DHCPv6 relay agent on IPv6 interfaces enable DHCP functionality of devices that don't share the same network segment as the DHCP Server.	*Documentation Updates* section in this document.
802.1X guest VLAN per port	You can configure 802.1X guest VLAN on each port individually.	"Specifying the authentication-failure action"
DHCP Option 66	You can configure the DHCP TFTP server option by specifying the TFTP server name.	"Configure the TFTP server"
IPv4 Egress ACL support	Access Control Lists (ACLs) for filtering outbound traffic.	Chapter "Configuring Rule-Based IP Access Control Lists (ACLs)" Chapter "Configuring IPv6 Access Control Lists (ACLs)"
GRE support (FCX ONLY)	IPv4 point-to-point GRE tunnels are now supported. Hitless management for IPv6-over-IPv4 tunnels is supported for GRE tunnels. Hitless management for IPv6-over-IPv4 tunnels is not supported for IP tunnels.	"IPv4 point-to-point GRE tunnels"
IPSec for OSPFv3	IPSec can be applied to an interface, area, or virtual link that is using OSPFv3, to provide security.	• "IPsec for OSPFv3" • "Configuring IPsec for OSPFv3"
IPv4 & IPv6 Ingress ACL support	Access Control Lists (ACLs) can now be used to filter both IPv4 and IPv6 traffic on FCX and ICX 6610 devices.	Chapter "Configuring Rule-Based IP Access Control Lists (ACLs)" Chapter "Configuring IPv6 Access Control Lists (ACLs)"

Feature	Description	See the *FastIron Configuration Guide*, section entitled…
IPv6 routing enhancements	This release adds IPv6 routing enhancements: • Router advertisement and solicitation • IPv6 static routes • IPv6 over IPv4 tunnels • ECMP load sharing • IPv6 ICMP • IPv6 routing protocols • ICMP redirect messages • IPv6 neighbor discovery • IPv6 Layer 3 forwarding • IPv6 redistribution • IPv6 MTU • Static neighbor entries • Hop limit for IPv6 packets • Clear IPv6 global information FCX devices also allow you to configure how TCAM space is used to store routing information and GRE tunnel information. The following are NOT supported: • OSPFv6 • RIPng • BGPv4+ • PIMv6	• "Configuring IPv6 on FastIron X, FCX, and ICX 6610 Series Switches" chapter • "Configuring TCAM space on FCX and ICX 6610 devices"
IPv6 source routing security enhancements	As a security measure, source-routed IPv6 traffic is deprecated.	"IPv6 source routing security enhancements"
IPv6 Support for VRRP and VRRPE	IPv6 VRRP version 3 (v3) and IPv6 VRRP-E (v3) is now supported on devices with IPv6 routing support. You can configure a VRRP or a VRRPE instance on an IPv6 interface under the IPv6 VRRP or VRRPE router mode.	"Configuring VRRP and VRRPE" chapter
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…
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*
Ports on Demand	Licensing for Ports on Demand (POD) is introduced on the ICX 6610 devices. By default, the ICX 6610 device has eight active 1 Gb uplink ports. To upgrade the ICX 6610 10 Gb ports from 1 Gb to 10 Gb port speed, use the ICX6610-10G-LIC-POD license. To increase the uplink capacity of four ports from 1 Gb to 10 Gb port speed, purchase a single ICX 661010G-LIC-POD license. To increase the uplink capacity of all eight ports from 1 Gb to 10 Gb port speed, purchase a second ICX 6610-10G-LIC-POD license.	"Licensed features and part numbers" "Licensing for Ports on Demand for ICX 6610 devices"
SNTP Server Support	SNTP server support allows you to enable SNTP server and serve SNTP clients	"Configuring the device as an SNTP server"
SNTP Broadcast Support	SNTP broadcast support allows you to 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.	"Specifying a Simple Network Time Protocol (SNTP) server"
SNTP MD5 Authentication	To configure an authentication key for communication with the SNTP server, use the **authentication-key** option. You can also configure the device to function as an SNTP server to its downstream clients.	• "Specifying a Simple Network Time Protocol (SNTP) server" • "Configuring the device as an SNTP server"
SNTP Show Association	The **show sntp associations details** command displays detailed information about SNTP associations.	"Specifying a Simple Network Time Protocol (SNTP) server"

Feature	Description	See the *FastIron Configuration Guide*, section entitled…
Software-based Licensing	Software-based licensing is introduced on ICX 6610 devices. The ICX 6610 Premium license, Advance license, and Upgrade license (from Premium to Advance license) are introduced to support routing functionality. New features are also added to the FCX Advance license. The behavior for running software-based licensing in a stack with different licenses (Premium, Advance, or Upgrade licenses) is the same for FCX and ICX 6610 devices. Commands for adding, deleting, or displaying a license are also introduced for FCX and ICX 6610 devices only.	"Non-licensed features" "Licensed features and part numbers" "FCX and ICX 6610 devices" "Using TFTP to copy a license file on FCX and ICX devices" "Deleting a license on FCX and ICX devices" "Viewing information about software licenses"
SSHv2 Client	SSHv2 client allows you to connect to SSHv2 servers while logged onto the device.	"Configuring and using SSH2 client"
SSHv2 Server RSA 2048 key authentication	SSHv2 server supports authentication using RSA keys of up to 2048 bits in length.	"Configuring SSH2 and SCP" chapter
VRRP-E MD5 authentication	VRRP-E supports MD5 for authentication of VRRP-E traffic.	"Configuring VRRP and VRRPE" chapter

Summary of enhancements in FSX R07.3.00

Table 1 lists the enhancements in software release 07.3.00 for FESX6 and SX devices.

Table 2 Enhancements in FSX R07.3.00

Feature	Description	See the *FastIron Configuration Guide*, section entitled…
New hardware	This release introduces the following new FastIron SX third generation interface modules: • SX-FI-24GPP - 24-port Gigabit Ethernet copper third generation interface module • SX-FI-24HF - 24-port Gigabit Ethernet 100/1000 Mbps SFP fiber third generation interface module • SX-FI-2XG - 2-port 10-Gigabit Ethernet SFP+ third generation interface module • SX-FI-8XG - 8-port 10-Gigabit Ethernet SFP+ thrird generation interface module	
802.1X guest VLAN per port	You can configure 802.1X guest VLAN on each port individually.	"Specifying the authentication-failure action"
DHCP Option 66	You can configure the DHCP TFTP server option by specifying the TFTP server name.	"Configure the TFTP server"
IPv4 Egress ACL support (*Supported only on SX 800 and SX 1600 new 1Gb and 10Gb modules*)	Access Control Lists (ACLs) for filtering outbound traffic.	Chapter "Configuring Rule-Based IP Access Control Lists (ACLs)" Chapter "Configuring IPv6 Access Control Lists (ACLs)"
IPSec for OSPFv3	IPSec can be applied to an interface, area, or virtual link that is using OSPFv3, to provide security.	• "IPsec for OSPFv3" • "Configuring IPsec for OSPFv3"
IPv6 source routing security enhancements	As a security measure, source-routed IPv6 traffic is deprecated.	"IPv6 source routing security enhancements"
IPv6 Support for VRRP and VRRPE	IPv6 VRRP version 3 (v3) and IPv6 VRRP-E (v3) is now supported on devices with IPv6 routing support. You can configure a VRRP or a VRRPE instance on an IPv6 interface under the IPv6 VRRP or VRRPE router mode.	"Configuring VRRP and VRRPE" chapter

Feature	Description	See 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"
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*
SNTP Server Support	SNTP server support allows you to enable SNTP server and serve SNTP clients	"Configuring the device as an SNTP server"
SNTP Broadcast Support	SNTP broadcast support allows you to 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.	"Specifying a Simple Network Time Protocol (SNTP) server"
SNTP MD5 Authentication	To configure an authentication key for communication with the SNTP server, use the **authentication-key** option. You can also configure the device to function as an SNTP server to its downstream clients.	● "Specifying a Simple Network Time Protocol (SNTP) server" ● "Configuring the device as an SNTP server"
SNTP Show Association	The **show sntp associations details** command displays detailed information about SNTP associations.	"Specifying a Simple Network Time Protocol (SNTP) server"
SSHv2 Client	SSHv2 client allows you to connect to SSHv2 servers while logged onto the device.	"Configuring and using SSH2 client"
SSHv2 Server RSA 2048 key authentication	SSHv2 server supports authentication using RSA keys of up to 2048 bits in length.	"Configuring SSH2 and SCP" chapter
VRRP-E MD5 authentication	VRRP-E supports MD5 for authentication of VRRP-E traffic.	"Configuring VRRP and VRRPE" chapter

Summary of enhancements in FWS R07.3.00

Table 1 lists the enhancements in software release 07.3.00 for FWS devices.

Table 3 Enhancements in FWS R07.3.00

Feature	Description	See the *FastIron Configuration Guide*, section entitled...
FIPS Software Compliance (certification pending)	Includes commands to enable FIPS-related security policy settings and commands to alter the level of protection. See "Appendix D: Federal Information Processing Standard" in the *Brocade FastIron Configuration Guide*.	"Federal Information Processing Standards" appendix
Multi-range VLANs	The multi-range VLAN feature allows you to use a single command to create and configure multiple VLANs.	"Multi-range VLAN"
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 TurboIron 24X R07.3.00

Feature	Description	See the *TurboIron 24X Configuration Guide*, section entitled...
AES in SNMP v3	TurboIron supports AES Encryption for SNMP v3	Chapter 48: Securing SNMP Access Defining an SNMP group
Symmetric Flow Control	In addition to asymmetric flow control, TurboIron devices support symmetric flow control, meaning they can both receive and transmit 802.3x PAUSE frames.	Chapter 3: Configuring Basic Software Features
Inter-domain Multicast	Support for the validation of inter-domain multicasting BGP	Chapter 20: Configuring IP Multicast Protocols Multicast Source Discovery Protocol (MSDP)

Feature	Description	See the *TurboIron 24X Configuration Guide*, section entitled…
New SNMP MIBs	TurboIron now supports the Unified IP MIB. 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)	*Unified IP MIB Reference Guide*

Deprecated commands

The CLI command **flash** is deprecated. You cannot change the default block size for TFTP file transfers.

Configuration Notes and feature limitations

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

Additional notes on trunk group rules

The following additional considerations apply to forming trunk groups:

- Legacy ports and 48 Gbps copper ports cannot be members of the same trunk group in hardware configurations such as the following:
- 48-port 10/100/1000 Mbps (RJ45) Ethernet PoE interface module (SX-FI48GPP) and IPv4/IPv6 interface modules or management modules with user ports.

Combination of different generations of ports cannot be members of the same trunk group under the following hardware configurations:

- 24-port fiber and copper Ethernet PoE/Fiber interfaces (SX-FI24GPP, SX-FI24GF) and IPv4/IPv6 interface modules or management modules with user ports
- 2-port 10G and 8-port 10G interfaces (SX-FI8XG, SX-FI2XG) and the IPv4/IPv6 interface modules or management modules with user ports

SNTP version configuration during upgrade

Starting with release 7.3.00, the default SNTP version is 4. In previous releases, the default SNTP version was

1. When you upgrade to release 7.3.00, the SNTP version gets set automatically to 4, unless a different SNTP version is specified in the device startup configuration.

ICMP redirect messages

In software release 07.2.02 and later, 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 and later, you will need to re-enable this feature after upgrading to 07.2.02 and later. 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 and later, the configuration (**no ip icmp redirect**) will be removed from the configuration file after upgrading to 07.2.02 and later, since this feature is now disabled by default. In this case, ICMP redirect messages will not be sent and no further action is required.

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

Documentation updates

This section contains updates to the documentation for this release.

DHCPv6 relay agent

A client locates a DHCP server using a reserved, link-scoped multicast address. Direct communication between the client and server requires that they are attached by the same link. In some situations where ease-of-management, economy, and scalability are concerns, you can allow a DHCPv6 client to send a message to a DHCP server using a DHCPv6 relay agent.

A DHCPv6 relay agent, which may reside on the client link, but is transparent to the client, relays messages between the client and the server. Multiple DHCPv6 relay agents can exist between the client and server. DHCPv6 relay agents can also receive relay-forward messages from other relay agents; these messages are forwarded to the DHCP server specified as the destination.

When the relay agent receives a message, it creates a new relay-forward message, inserts the original DHCPv6 message, and sends the relay-forward message as the DHCP server.

Configuring the DHCPv6 relay agent

To enable the DHCPv6 relay agent function and specify the relay destination (the DHCP server) address on an interface, enter the following command at the interface level:

```
Brocade(config-if-e1000-2/3)#ipv6 dhcp-relay destination 2001::2
```

Syntax: [no] ipv6 dhcp-relay destination <ipv6-address>

Specify the <ipv6-address> as a destination address to which client messages are forwarded and which enables DHCPv6 relay service on the interface. You can configure up to 16 relay destination addresses on an interface.

Use the **[no]** version of the command to remove a DHCPv6 relay agent from the interface.

Displaying DHCPv6 relay agents

The **show ipv6 dhcp-relay** command displays the DHCPv6 relay agents configured on the device:

```
Brocade(config)# show ipv6 dhcp-relay

Current DHCPv6 relay agent state: Enabled

State: Enabled       RCV 0 packets,       TX 0 packets

DHCPv6 destinations on Ethernet 1:

         ab::cb

         11::22

DHCPv6 destinations on Ethernet 2:

         FE02::1

         11::22

DHCPv6 relay agent Total RCV 22 packets, TX 20 packets

Received packets: RELAY_FORWARD: 5, RELAY_REPLY: 5

OtherServertoClient: 15, OtherClinettoServer: 15
```

Displaying debug options

To display debug information related to DHCPv6 relay agent, use the following commands:

Display the DCHPv6 debug status

Enter the following command:

```
Brocade# debug ipv6 dhcp all
          DHCP6:  all debugging is on
```

Syntax: debug upv6 dhcp all

Display the DHCP trace debugging status

Enter the following command:

```
Brocade# debug ipv6 dhcp trace
          DHCP6:  trace debugging is on
```

Syntax: debug ipv6 dhcp trace

Display the DHCPv6 statistics

Enter the following command:

```
Brocade# show ipv6 dhcp-relay debug
DHCP6 Error Counters:
   rx_packet_dropped_dhcp6_relay_disabled: 0
   rx_packet_dropped_no_relay_option: 0
   rx_packet_dropped_no_buffer: 0
   send_packet_fail_no_address: 0
   send_packet_fail_no_buffer: 0
   send_packet_fail_udp: 0
DHCP6 Other Counters:
   dhcp6_relay_enabled_cnt: 1
```

Syntax: show ipv6 dhcp-relay debug

Enabling the detection of PoE power requirements advertised through CDP

The dynamic configuration of a PoE powered device such as a wireless access point (AP) or a VoIP device uses an initial discovery process. Upon installation, and sometimes periodically, a device will query the Brocade device for available power information and will advertise information about itself, such as, device ID, port ID, and power request. When the Brocade device receives the query, it sends the power available in a reply packet back to the device. The device then configures itself to draw power up to the power level available to it.

SNTP authentication key configuration

The **authentication-key** <*key-ID*> <*key-string*> option is used to configure an authentication key for communication with the SNTP server. If the <*key-string*> variable consists of only numerical characters, you must enclose the numerical characters in double quotes.

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

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

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 L3 device by entering the following command:

```
FastIron# reload
```

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

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

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

   ```
   FastIron(config-if-e1000-3/1)# no ip address 192.0.2.0/24
   ```

   Syntax: no ip address <ip-address>

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

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

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

```
FastIron# reload
```

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

Supported FSX modules

This release supports the following modules on the FSX 800 and FSX 1600 devices.

First generation modules	Second generation modules	Third generation modules
SX-FI2XGMR4	SX-FI2XGMR6	SX-FI48GPP
SX-FI2XGMR4-PREM	SX-FI2XGMR6-PREM	SX-FI-2XG
SX-FI424100FX	SX-FI2XGMR6-PREM6	SX-FI-8XG
SX-FI42XG-BNDL-2CX4	SX-FI624100FX	SX-FI-24HF
SX-FI424C	SX-FI624C	SX-FI-24GPP
SX-FI424P	SX-FI624HF	
SX-FI424F	SX-FI624P	
SX-FI424HF	SX-FI62XG	
SX-FI42XG		

In addition, the SX-FIZMR, SX-FIZMR-PREM, SX-FIZMR-6-PREM and SX-FIZMR-6-PREM6, which do not have packet processors, are supported in this release.

Feature support

Feature support for FCX, FESX6, ICX 6610, SX, and FWS

These release notes include a list of supported features in IronWare software for FCX, FESX6, ICX 6610, SX, and FWS devices supported in this release. For more information about supported features, refer to the manuals listed in Additional resources.

Supported management features

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

Table 4 Supported management features

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610
802.1X accounting	Yes	Yes	Yes	Yes
AAA support for console commands	Yes	No	Yes	Yes
Access Control Lists (ACLs) for controlling management access	Yes	Yes	Yes	Yes
Alias command	Yes	Yes	Yes	Yes
Combined DSCP and internal marking in one ACL rule	Yes	No	No	No
Single source address for the following packet types: ● Telnet ● TFTP ● Syslog ● SNTP ● TACACS/TACACS+ ● RADIUS ● SSH ● SNMP	Yes	No	No	No
DHCP client-based auto-configuration	Yes	Yes	Yes	Yes
DHCP server	Yes	Yes	Yes	Yes
Disabling TFTP access	Yes	No	Yes	Yes

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610
Brocade Network Advisor 11.2	Yes	Yes	Yes	Yes
Hitless management: ● Hitless switchover ● Hitless failover ● Hitless OS upgrade	Yes (FSX 800 and FSX 1600 only)	No	See next line item	See next line item
Hitless stacking management: ● Hitless stacking switchover ● Hitless stacking failover	No	No	Yes	Yes
Hitless support for: ● PBR ● GRE Tunnels ● Ipv6 to Ipv4 Tunnels	Yes (FSX 800 and FSX 1600 only)	No	Yes (PBR and GRE only)	Yes (PBR only)
Brocade Network Advisor 11.2	Yes	Yes	Yes	Yes
Remote monitoring (RMON)	Yes	Yes	Yes	Yes
Retaining Syslog messages after a soft reboot	Yes	Yes	Yes	Yes
sFlow support for IPv6 packets	Yes	Yes	Yes	Yes
DHCP Client	Yes	Yes	Yes	Yes
SNTP Server	Yes	Yes	Yes	Yes
SNTP Client (Broadcast & Unicast)	Yes	No	Yes	Yes
Flexible Port On Demand Licensing	No	No	No	Yes
sFlow version 2	Yes	Yes	Yes	Yes
sFlow version 5 (default)	Yes	Yes	Yes	Yes
Industry-standard Command Line Interface (CLI), including support for: ● Serial and Telnet access	Yes	Yes	Yes	Yes

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610
● Alias command ● On-line help ● Command completion ● Scroll control ● Line editing ● Searching and filtering output ● Special characters				
Show log on all terminals	Yes	Yes	Yes	Yes
SNMP v1, v2, v3	Yes	Yes	Yes	Yes
SNMP V3 traps	Yes	Yes	Yes	Yes
Specifying the maximum number of entries allowed in the RMON Control Table	Yes	No	Yes	Yes
Specifying which IP address will be included in a DHCP/BOOTP reply packet	Yes	No	Yes	Yes
Traffic counters for outbound traffic	Yes	No	No	No
Web-based GUI	Yes	Yes	Yes	Yes
Web-based management HTTPS/SSL	Yes	Yes	Yes	Yes

Supported security features

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

Table 5 Supported security features

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610
802.1X port security	Yes	Yes	Yes	Yes
802.1X authentication RADIUS timeout action	Yes	Yes	Yes	Yes

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610
802.1X dynamic assignment for ACL, MAC filter, and VLAN	Yes	Yes	Yes	Yes
Access Control Lists (ACLs) for filtering transit traffic ● Support for inbound ACLs. ● Support Outbound ACLs (*SX 800 and SX1600 on third generation modules only)	Yes Yes *	Yes No	Yes Yes	Yes Yes
Address locking (for MAC addresses)	Yes	Yes	Yes	Yes
AES Encryption for SNMP v3	Yes	Yes	Yes	Yes
AES Encryption for SSH v2	Yes	Yes	Yes	Yes
Authentication, Authorization and Accounting (AAA): ● RADIUS ● TACACS/TACACS+	Yes	Yes	Yes	Yes
Denial of Service (DoS) attack protection: ● Smurf (ICMP) attacks ● TCP SYN attacks	Yes	Yes	Yes	Yes
DHCP Snooping	Yes	Yes	Yes	Yes
Dynamic ARP Inspection	Yes	Yes	Yes	Yes
EAP Pass-through Support	Yes	Yes	Yes	Yes
HTTPS	Yes	Yes	Yes	Yes
IP Source Guard	Yes	Yes	Yes	Yes
Local passwords	Yes	Yes	Yes	Yes
MAC address filter override of 802.1X	Yes	Yes	Yes	Yes
MAC address filtering (filtering on source and destination MAC addresses)	Yes	Yes	Yes	Yes
Ability to disable MAC learning	Yes	Yes	Yes	Yes

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610
Flow-based MAC address learning	Yes	No	Yes	Yes
MAC port security	Yes	Yes	Yes	Yes
Multi-device port authentication	Yes	Yes	Yes	Yes
Support for Multi-Device Port Authentication together with:				
● Dynamic VLAN assignment	Yes	Yes	Yes	Yes
● Dynamic ACLs	Yes	Yes	Yes	Yes
● 802.1X	Yes	Yes	Yes	Yes
● Dynamic ARP inspection with dynamic ACLs	Yes	No	No	No
● DHCP snooping with dynamic ACLs	Yes	No	No	No
● Denial of Service (DoS) attack protection	Yes	No	Yes	Yes
● Source guard protection	Yes	Yes	Yes	Yes
● ACL-per-port-per-VLAN	Yes	Yes	Yes	Yes
Multi-device port authentication password override	Yes	Yes	Yes	Yes
Multi-device port authentication RADIUS timeout action	Yes	Yes	Yes	Yes
Secure Copy (SCP)	Yes	Yes	Yes	Yes
Secure Shell (SSH) v2	Yes	Yes	Yes	Yes
Packet filtering on TCP Flags	No	Yes	Yes	Yes
DHCP Relay Agent information (DHCP Option 82)	Yes	Yes	Yes	Yes
Web Authentication	Yes	Yes	Yes	Yes

Supported system-level features

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

Table 6 Supported system-level features

Category and description	FESX6 FSX FSX 800 FSX 1600	FWS	FCX	ICX 6610
10/100/1000 port speed	Yes	Yes	Yes	Yes
16,000 MAC addresses per switch (FastIron devices)	Yes	Yes	Yes	Yes
32,000 MAC addresses per switch	Yes	No	Yes	Yes
ACL-based mirroring	Yes	Yes	Yes	Yes
ACL-based fixed rate limiting	Yes	Yes	Yes	Yes
ACL-based adaptive rate limiting	Yes	No	Yes	Yes
ACL filtering based on VLAN membership or VE port membership	Yes	Yes	Yes	Yes
ACL logging of denied packets (IPv4)	Yes	Yes	Yes	Yes
ACL statistics	Yes	Yes	Yes	Yes
ACLs to filter ARP packets	Yes	Yes	Yes	Yes
Auto MDI/MDIX detection	Yes	Yes	Yes	Yes
Auto-negotiation	Yes	Yes	Yes	Yes
Automatic removal of Dynamic VLAN for 802.1X ports	Yes	Yes	Yes	Yes
Automatic removal of Dynamic VLAN for MAC authenticated ports	Yes	No	No	No
Byte-based broadcast, multicast, and unknown-unicast rate limits	Yes	No	No	No
Packet-based broadcast, multicast, and unknown-unicast rate limits	Yes	Yes	Yes	Yes
DiffServ support	Yes	Yes	Yes	Yes
Digital Optical Monitoring	Yes	Yes	Yes	Yes
Displaying interface names in Syslog messages	Yes	Yes	Yes	Yes

Category and description	FESX6 FSX FSX 800 FSX 1600	FWS	FCX	ICX 6610
Displaying TCP and UDP port numbers in Syslog messages	Yes	Yes	Yes	Yes
Dynamic buffer allocation for QoS priorities	Yes	Yes	Yes	Yes
Flow control: ● Responds to flow control packets, but does not generate them	Yes	Yes	Yes	Yes
Inbound rate limiting (port-based fixed rate limiting on inbound ports)	Yes	Yes	Yes	Yes
Foundry Discovery Protocol (FDP) / Cisco Discovery Protocol (CDP)	Yes	Yes	Yes	Yes
Generic buffer profile	No	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
LLDP	Yes	Yes	Yes	Yes
LLDP-MED	Yes	Yes	Yes	Yes
MAC address filter-based mirroring	No	Yes	Yes	Yes
Multi-port static MAC address	Yes	Yes	Yes	Yes
Multiple Syslog server logging (up to six Syslog servers)	Yes	Yes	Yes	Yes
Outbound rate limiting (port-based and port- and priority-based rate limiting on outbound ports)	No	Yes	No	No
Outbound rate shaping	Yes	No	Yes	Yes
Path MTU Discovery	Yes	No	Yes	Yes
Port flap dampening	Yes	Yes	Yes	Yes

Category and description	FESX6 FSX FSX 800 FSX 1600	FWS	FCX	ICX 6610
Port mirroring and monitoring (mirroring of both inbound and outbound traffic on individual ports)	Yes	Yes	Yes	Yes
Power over Ethernet (POE)	Yes (POE-enabled Interface modules with POE power supply)	Yes (FWS-POE and FWS-G-POE only)	Yes (FCX-S-POE+ only)	Yes - ICX 6610-24P and ICX 6610-48P
High Power over Ethernet (POE)+	Yes (SX-FI48GPP SX-FI-24GPP module only)	No	Yes (FCX-S-POE+ only)	Yes - ICX 6610-24P and ICX 6610-48P
PoE firmware upgrade via CLI	Yes	No	Yes	Yes
Priority mapping using ACLs	Yes	Yes	Yes	Yes
Protected link groups	Yes	Yes	Yes	Yes
Layer 2 stacking rapid failover and switchover	No	No	Yes	Yes
Static MAC entries with option to set traffic priority	Yes	Yes	Yes	Yes
Symmetric flow control ● Can transmit and receive 802.1x PAUSE frames	No	No	Yes	Yes
System time using a Simple Network Time Protocol (SNTP) server or local system counter	Yes	Yes	Yes	Yes
User-configurable scheduler profile	No	No	Yes	Yes
User-configurable buffer profile	No	No	Yes	Yes

Category and description	FESX6 FSX FSX 800 FSX 1600	FWS	FCX	ICX 6610
Virtual Cable Testing (VCT) technology	Not on third generation modules	Yes	Yes	No

Supported Layer 2 features

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

Table 7 Supported Layer 2 features

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610
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
802.1p Quality of Service (QoS): ● Strict Priority (SP) ● Weighted Round Robin (WRR) ● Combined SP and WRR ● 8 priority queues	Yes	Yes	Yes	Yes
802.1s Multiple Spanning Tree	Yes	Yes	Yes	Yes
802.1W Rapid Spanning Tree (RSTP)	Yes	Yes	Yes	Yes
802.3ad link aggregation (dynamic trunk groups)	Yes	Yes	Yes	Yes
ACL-based rate limiting QoS	Yes	Yes	Yes	Yes
BPDU Guard	Yes	Yes	Yes	Yes
Dynamic Host Configuration Protocol (DHCP) Assist	Yes	Yes	Yes	Yes
IGMP v1/v2 Snooping Global	Yes	Yes	Yes	Yes

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610
IGMP v3 Snooping Global	Yes (*,G)	Yes (S,G)	Yes (S,G)	Yes (S,G)
IGMP v1/v2/v3 Snooping per VLAN	Yes	Yes	Yes	Yes
IGMP v2/v3 Fast Leave (membership tracking)	Yes	Yes	Yes	Yes
Interpacket Gap (IPG) adjustment	Yes	Yes	Yes	Yes
IP MTU (individual port setting)	Yes	No	Yes	Yes
Jumbo frames: ● Up to 10240 bytes, or ● Up to 10232 bytes in an IronStack	Yes	Yes	Yes	Yes
Link Aggregation Control Protocol (LACP)	Yes	Yes	Yes	Yes
Link Fault Signaling (LFS) for 10G	Yes	Yes	Yes	Yes
MAC-Based VLANs, including support for dynamic MAC-Based VLAN activation	No	Yes	Yes	Yes
Metro Ring Protocol 1 (MRP 1)	Yes	Yes	Yes	Yes
Metro Ring Protocol 2 (MRP 2)	Yes	Yes	Yes	Yes
Extended MRP ring IDs from 1 – 1023	Yes	No	Yes	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
Multicast static group traffic filtering (for snooping scenarios)	No	Yes	Yes	Yes
PIM-SM V2 Snooping	Yes	Yes	Yes	Yes
PVST/PVST+ compatibility	Yes	Yes	Yes	Yes
PVRST+ compatibility	Yes	Yes	Yes	Yes

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610
Remote Fault Notification (RFN) for 1 G fiber	Yes	Yes	Yes	Yes
Root Guard	Yes	Yes	Yes	Yes
Single link LACP	Yes	Yes	Yes	Yes
Super Aggregated VLANs	Yes	Yes	Yes	Yes
Trunk groups: ● Trunk threshold for static trunk groups ● Flexible trunk group membership ● Option to include Layer 2 in trunk hash calculation (FGS, FLS, FWS only)	Yes	Yes	Yes	Yes
Topology groups	Yes	Yes	Yes	Yes
Uni-directional Link Detection (UDLD) (Link keepalive)	Yes	Yes	Yes	Yes
Uplink Ports within a Port-Based VLAN	Yes	Yes	Yes	Yes
VLAN Support: ● 4096 maximum VLANs ● 802.1Q with tagging ● 802.1ad 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

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610
VLAN-based mirroring	No	Yes	Yes	Yes
VoIP Autoconfiguration and CDP	Yes	Yes	Yes	Yes
Virtual Switch Redundancy Protocol (VSRP)	Yes	Yes	Yes	Yes
VSRP-Aware security features	Yes	Yes	Yes	Yes
VSRP and MRP signaling	Yes	Yes	Yes	Yes
VSRP Fast Start	Yes	Yes	Yes	Yes
VSRP timer scaling	Yes	Yes	Yes	Yes

Supported base Layer 3 features

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

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

Table 8 Supported base Layer 3 features

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610
BootP/DHCP Relay	Yes	Yes	Yes	Yes
Equal Cost Multi Path (ECMP) load sharing	Yes	Yes	Yes	Yes
IP helper	Yes	Yes	Yes	Yes
RIP V1 and V2 (advertising only)	Yes	Yes	Yes	Yes
Routing for directly connected IP subnets	Yes	Yes	Yes	Yes
Static IP routing	Yes	Yes	Yes	Yes
Virtual Interfaces (up to 512)	Yes	Yes	Yes	Yes
Virtual Router Redundancy Protocol (VRRP)	Yes	Yes	Yes	Yes

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610
VRRP timer scaling	Yes	Yes	Yes	Yes

Supported edge Layer 3 features

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

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

Table 9 Supported edge Layer 3 features

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

Supported full Layer 3 features

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

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

Table 10 Supported full Layer 3 features

Category and description	FESX-PREM FSX 800-PREM FSX 1600-PREM	FCX	ICX 6610
Active host routes	Yes (6,000)	Yes (16,000)	Yes (16,000)

Category and description	FESX-PREM FSX 800-PREM FSX 1600-PREM	FCX	ICX 6610
Anycast RP	Yes	No	No
IPv6 BGP/BGP4+	No	No	No
BGP4 graceful restart	Yes (FSX 800 and FSX 1600 only)	Yes (ADV models in a stack)	Yes (ADV models in a stack)
BGP4	Yes	Yes (ADV models)	Yes (ADV models)
Distance Vector Multicast Routing Protocol (DVMRP) V2 (RFC 1075)	Yes	No	No
Internet Group Management Protocol (IGMP) V1, V2, and V3 (for multicast routing scenarios)	Yes	Yes	Yes
ICMP Redirect messages	Yes	Yes	Yes
IGMP V3 fast leave (for routing)	Yes	Yes	Yes
IPv4 point-to-point GRE IP tunnels	Yes (IPv6 devices only and 3rd gen modules)	No	No
IPv6 Layer 3 forwarding[1]	Yes	Yes	Yes
IPv6 over IPv4 tunnels in hardware[1]	Yes	Yes	Yes
IPv6 Redistribution[1]	Yes	Yes	Yes
IPv6 Static Routes[1]	Yes	Yes	Yes
Multiprotocol Source Discovery Protocol (MSDP)	Yes	Yes	Yes
OSPF graceful restart	Yes (FSX 800 and FSX 1600 only)	Yes	Yes
OSPF V2	Yes	Yes	Yes

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

Category and description	FESX-PREM FSX 800-PREM FSX 1600-PREM	FCX	ICX 6610
OSPF V3 (IPv6)[1]	Yes	Yes	Yes
Protocol Independent Multicast Dense mode (PIM-DM) V1 (draft-ietf-pim-dm-05) and V2 (draft-ietf-pim-v2-dm-03)	Yes	Yes	Yes
Protocol Independent Multicast Sparse mode (PIM-SM) V2 (RFC 2362)	Yes	Yes	Yes
PIM passive	Yes	Yes	Yes
Policy-Based Routing (PBR)	Yes	Yes	Yes
RIPng (IPv6)[1]	Yes	Yes	Yes
Route-only support (Global CONFIG level and Interface level)	Yes	Yes	Yes
Route redistribution (including BGP4)	Yes	Yes (BGP4 supported on ADV models only)	Yes (BGP4 supported on ADV models only)
Routes in hardware maximum: • FESX6 – up to 256K routes • FESX6-E – up to 512K routes • FSX – up to 512K routes • FCX – up to 16K routes • ICX – up to 15K Ipv4 routes and 2800 IPv6 routes	Yes	Yes	Yes
Static ARP entries	Yes (up to 6,000)	Yes (up to 1,000)	Yes (up to 1,000)
VRRP-E	Yes	Yes	Yes
VRRP-E slow start timer	Yes	Yes	Yes
VRRP-E timer scale	Yes	Yes	Yes

Supported IPv6 management features

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

Table 11 Supported IPv6 management features

Category and description	FESX6 FSX 800 FSX 1600	FWS	FCX	ICX 6610
Link-Local IPv6 Address	Yes	Yes	Yes	Yes
IPv6 Access List (management ACLs)	Yes	Yes	Yes	Yes
IPv6 copy	Yes	Yes	Yes	Yes
IPv6 ncopy	Yes	Yes	Yes	Yes
IPv6 debug	Yes	Yes	Yes	Yes
IPv6 ping	Yes	Yes	Yes	Yes
IPv6 traceroute	Yes	Yes	Yes	Yes
DNS server name resolution	Yes	Yes	Yes	Yes
HTTP/HTTPS	Yes	Yes	Yes	Yes
Logging (Syslog)	Yes	Yes	Yes	Yes
RADIUS	Yes	Yes	Yes	Yes
SCP	Yes	Yes	Yes	Yes
SSH	Yes	Yes	Yes	Yes
SNMP	Yes	Yes	Yes	Yes
SNMP traps	Yes	Yes	Yes	Yes
SNTP	Yes	Yes	Yes	Yes
TACACS/TACACS+	Yes	Yes	Yes	Yes
Telnet	Yes	Yes	Yes	Yes
TFTP	Yes	Yes	Yes	Yes

Unsupported features

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

Table 12 Unsupported features

System-level features not supported
● ACL logging of permitted packets
● Broadcast and multicast MAC filters
● Outbound ACLs on FWS, and 1st or 2nd generation of FSX modules.
Layer 2 features not supported
● SuperSpan
● VLAN-based priority
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)

TurboIron 24X Feature Support

This section describes the feature highlights in this release. Features or options not listed in this section or documented in the *FastIron and TurboIron 24X Configuration Guide* are not supported.

Supported Management Features

This release supports the following management features.

Supported Management Features Category, Description, and Configuration Notes	Supported on TurboIron
802.1X accounting	No

Supported Management Features Category, Description, and Configuration Notes	Supported on TurboIron
AAA support for console commands	Yes
Access Control Lists (ACLs) for controlling management access	Yes
Alias Command	Yes
Combined DSCP and internal marking in one ACL rule	Yes
Configuring an interface as the source for all TFTP, Syslog, and SNTP packets	No
DHCP Client-Based Auto-Configuration	No
DHCP Server	No
Disabling TFTP Access	Yes
Brocade Network Advisor 11.2	Yes
P-Bridge and Q-Bridge MIBs	Yes
Remote monitoring (RMON)	Yes
Retaining Syslog messages after a soft reboot	No
sFlow For inbound traffic only 802.1X username export support for encrypted and non-encrypted EAP types	Yes
sFlow support for IPv6 packets	Yes
sFlow Version 5	No
Serial and Telnet access to industry-standard Command Line Interface (CLI)	Yes
Show log on all terminals	Yes
SNMP v1, v2, v3	Yes
SNMP V3 traps	Yes
Specifying the maximum number of entries allowed in the RMON Control Table	Yes
Specifying which IP address will be included in a DHCP/BOOTP reply packet	No
Traffic counters for outbound traffic	Yes
Web-based GUI	No
Web-based management HTTPS/SSL	No

Supported IPv6 Management Features

This release supports the following IPv6 management features.

Supported IPv6 Management Features Category, Description, and Configuration Notes	Supported on TurboIron
Link-Local IPv6 Address	Yes
IPv6 Access List	No
IPv6 copy	Yes
IPv6 ncopy	Yes
IPv6 debug	Yes
IPv6 ping	Yes
IPv6 traceroute	Yes
DNS server name resolution	Yes

Supported IPv6 Management Features Category, Description, and Configuration Notes	Supported on TurboIron
HTTP/HTTPS	No
Logging (syslog)	Yes
RADIUS	Yes
SCP	Yes
SSH	Yes
SNMP v1, v2, v3	Yes
SNTP	Yes
Syslog	Yes
TACACS/TACACS+	Yes
Telnet	Yes
TFTP	Yes
Traps	Yes

Supported Security Features

This release supports the following security features.

Supported Security Features Category, Description, and Configuration Notes	Supported on TurboIron
802.1X port security	Yes
802.1X authentication RADIUS timeout action	Yes
802.1X dynamic assignment for ACL, MAC filter, and VLAN	Yes
Access Control Lists (ACLs) for filtering transit traffic Support for inbound ACLs only. These devices do not support outbound ACLs.	Yes
Address locking (for MAC addresses)	Yes
AES Encryption for SNMP v3	Yes
AES Encryption for SSH v2	Yes
Authentication, Authorization and Accounting (AAA) RADIUS, TACACS/TACACS+	Yes
Denial of Service (DoS) protection TCP SYN Attacks and ICMP Attacks	Yes
DHCP Snooping	No
Dynamic ARP Inspection	No

Supported Security Features Category, Description, and Configuration Notes	Supported on TurboIron
EAP Pass-through Support	Yes
Enhancements to username and password	Yes
HTTPS	No
IP Source Guard	No
Local passwords	Yes
MAC filter override of 802.1X	Yes
MAC filtering Filtering on source and destination MAC addresses	Yes
Ability to disable MAC Learning	Yes
Flow-based MAC learning	No
MAC port security	Yes
Multi-device port authentication	Yes
Multi-device port Authentication with dynamic ACLs	Yes
Multi-device port authentication with dynamic VLAN assignment	Yes
Multi-device port authentication password override	Yes
Multi-device port authentication RADIUS timeout action	Yes
Secure Copy (SCP)	Yes
Secure Shell (SSH) v2 Server	Yes
Packet filtering on TCP Flags	Yes
DHCP Relay Agent information (DHCP Option 82) for DHCP snooping	No
Web Authentication	No

Supported System-Level Features

This release supports the following system-level features.

Supported System –Level Features Category, Description, and Configuration Notes	Supported on TurboIron
10/100/1000 port speed	Yes
1 Gbps and 10 Gbps configurable port speed on fiber ports	Yes
32,000 MAC addresses per switch	Yes
ACL-Based Mirroring	Yes
ACL-Based Rate Limiting	Yes

Supported System –Level Features Category, Description, and Configuration Notes	Supported on TurboIron
ACL-based fixed and adaptive rate limiting on inbound ports	
ACL filtering based on VLAN membership or VE port membership	Yes
ACL logging of denied packets ACL logging is supported for denied packets, which are sent to the CPU for logging ACL logging is not supported for permitted packets Packets that are denied by ACL filters are logged in the Syslog based on a sample time-period.	Yes
ACL statistics	Yes
ACLs to filter ARP packets	Yes
Asymmetric flow control Responds to flow control packets, but does not generate them	Yes
Auto MDI/MDIX	Yes
Auto-negotiation	Yes
Automatic removal of Dynamic VLAN for 802.1X ports	No
Automatic removal of Dynamic VLAN for MAC authenticated ports	No
Broadcast, multicast, and unknown-unicast rate limiting	Yes
Boot and reload after 5 minutes at or above shutdown temperature	Yes
Cut-through switching	Yes
DiffServ support	Yes
Digital Optical Monitoring	Yes
Displaying interface names in Syslog	Yes
Displaying TCP/UDP port numbers in Syslog messages	Yes
DSCP Mapping for values 1 through 8	Yes
Dynamic buffer allocation	Yes
Egress buffer thresholds	Yes
Fixed rate limiting Port-based rate limiting on inbound ports. Fixed rate limiting is supported on 1 Gbps and 10 Gbps Ethernet ports. Fixed rate limiting is not supported on tagged ports in the full Layer 3 router image.	Yes
Foundry Discovery Protocol (FDP) / Cisco Discovery Protocol (CDP)	Yes
Generic buffer profile	No
High Availability Layer 2 hitless switchover Layer 2 hitless Operating System (OS) upgrade	No

Supported System –Level Features Category, Description, and Configuration Notes	Supported on TurboIron
LLDP	Yes
LLDP-MED	No
MAC filter-based mirroring	Yes
Multi-port static MAC address	Yes
Multiple Syslog server logging Up to six Syslog servers	Yes
Negative temperature setting	Yes
Outbound rate limiting	No
Outbound rate shaping	Yes
Path MTU Discovery support	No
Port flap dampening	Yes
Port mirroring and monitoring Mirroring of both inbound and outbound traffic on individual ports is supported.	Yes
Power over Ethernet	No
Priority mapping using ACLs	Yes
Protected link groups	No
Specifying a Simple Network Time Protocol (SNTP) Server	Yes
Specifying the minimum number of ports in a trunk group	Yes
Static MAC entries with option to set traffic priority	Yes
Virtual Cable Testing (VCT) technology Uses Time Domain Reflectometry (TDR) technology to detect and report cable statistics such as; local and remote link pair, cable length, and link status.	No

Supported Layer 2 Features

This release supports the following Layer 2 features.

Supported Layer 2 Features Category, Description, and Configuration Notes	Supported on TurboIron
802.1D Spanning Tree Support Enhanced IronSpan support includes Fast Port Span and Single-instance Span TurboIron switches support up to 255 spanning tree instances for VLANs.	Yes
802.1p Quality of Service (QoS) Strict Priority (SP) Weighted Round Robin (WRR)	Yes

Supported Layer 2 Features Category, Description, and Configuration Notes	Supported on TurboIron
Combined SP and WRR 8 priority queues	
802.1s Multiple Spanning Tree	Yes
802.1W Rapid Spanning Tree (RSTP) 802.1W RSTP support allows for sub-second convergence (both final standard and draft 3 supported)	Yes
802.3ad link aggregation (dynamic trunk groups) Brocade ports enabled for link aggregation follow the same rules as ports configured for trunk groups.	Yes
ACL-based rate limiting QoS	Yes
BPDU Guard	Yes
Dynamic Host Configuration Protocol (DHCP) Assist	Yes
IGMP v1/v2 Snooping Global	Yes
IGMP v3 Snooping Global	Yes (*,G and S,G)
IGMP v1/v2/v3 Snooping per VLAN	Yes
IGMP Proxy	Yes
IGMP v2/v3 Fast Leave (membership tracking)	Yes
IGMP Filters	Yes
Interpacket Gap (IPG) adjustment	Yes
Jumbo frames 10/100/1000 and 10-Gigabit Ethernet ports Up to 9216 bytes	Yes
LACP LACP trunk group ports follow the same configuration rules as for statically configured trunk group ports. Support for single link LACP	Yes
Link Fault Signaling (LFS) for 10-Gigabit Ethernet ports	Yes
MAC-Based VLANs Dynamic MAC-Based VLAN Activation	No
Metro Ring Protocol 1 (MRP 1)	Yes
Metro Ring Protocol 2 (MRP 2)	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	No

Supported Layer 2 Features Category, Description, and Configuration Notes	Supported on TurboIron
Multicast static group traffic filtering (for snooping scenarios)	No
PIM-SM V2 Snooping	Yes
PVST/PVST+ compatibility	Yes
PVRST+ compatibility	Yes
Remote Fault Notification (RFN) for 10-Gigabit Ethernet ports	No
Root Guard	Yes
Super Aggregated VLANs	Yes
Trunk groups Trunk threshold for static trunk groups Flexible trunk group membership	Yes
Topology groups	Yes
Uni-directional Link Detection (UDLD) (Link keepalive)	Yes
Uplink Ports Within a Port-Based VLAN	Yes
VLAN Support on TurboIron Devices: 4096 maximum VLANs Dual-mode VLANs 802.1Q with tagging Port-based VLANs VLAN groups Private VLANs	Yes
802.1ad Tagging (tag-type 8100 over 8100 encapsulation)	Yes
VLAN-based mirroring	No
VoIP Auto-configuration and CDP	No
Virtual Switch Redundancy Protocol (VSRP)	Yes
VSRP-Aware security features	Yes
VSRP and MRP signaling	Yes
VSRP Fast Start	Yes
VSRP timer scaling	Yes

Supported Layer 3 Features

This release supports the following Layer 3 features.

Supported Layer 3 Features Category, Description, and Configuration Notes	Supported on TurboIron
Anycast RP	Yes
BGP	Yes
IGMP V1, V2, and V3	Yes
IP helper	Yes
IP multicast routing protocols: PIM-SM and PIM-DM DVMRP is not supported	Yes
ICMP Redirect messages	Yes
Multiprotocol Source Discovery Protocol (MSDP)	Yes
OSPF V2 (IPv4)	Yes
RIP V1 and V2	Yes
Route-only support Disabling Layer 2 Switching at the CLI Interface level as well as the Global CONFIG level. This feature is not supported on virtual interfaces.	Yes
Routing for directly connected IP subnets	Yes
Static IP Routing	Yes
Virtual Interfaces Up to 255 virtual interfaces	Yes
VRRP	Yes
VRRP-E	Yes

Note: Layer 3 features not listed under “Layer 3 Features” are not supported.

Upgrading software for FSX and FESX6

Use the procedures in this section to upgrade the software for FSX and FESX6.

Important notes about upgrading or downgrading the software

Note the following when upgrading to software release R07.3.00c:

- FSX devices can store two Full Layer 3 image or two Layer 2 or Base Layer 3 images.
- FESX6 can store one Full Layer 3 image or two Layer 2 or Base Layer 3 images
- The image for IronWare R07.2.00a and later uses different Interprocessor Communications (IPC) versions for FCX devices; however, units in a stack must run the same IPC version to communicate. After upgrading from IronWare R07.2.00 or earlier to IronWare R07.3.00c, you must verify that the same image downloaded to every unit in the stack before reloading the entire stack. To verify the images, you can enter the **show flash** command at any level of the CLI. A stack cannot be built and will not operate if one or more units has different software images.

Note the following when downgrading from software release R07.3.00c:

- 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.

Standard upgrade procedure

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

Software image file for IronWare release R07.3.00c

Table 13 lists the software image file that is available for IronWare Release R07.3.00c.

Table 13 Software image file

Device	Boot Image	Flash Image
FESX6 FSX 800 FSX 1600	sxz07200.bin	SXS07300c.bin (Layer 2) or SXL07300c.bin (base Layer 3) or SXR07300c.bin (full Layer 3)
FWS	fgz05000.bin	FWS07300c.bin (Layer 2) FWSR07300c.bin (Layer 3) FWSL07300c.bin (base Layer 3)
FCX ICX 6610	grz07302.bin	FCXS07300c.bin (Layer 2) FCXR07300c.bin (Layer 3)

Factory pre-loaded software

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

NOTE: Devices with 8MB of flash memory, including FESX6 devices, can only store a primary image. FCX, ICX, and SX devices can store one Full Layer 3 image or two Layer 2 or Base Layer 3 images.

Table 14 Factory pre-loaded software

Model	Software Images	
	Primary Flash	Secondary Flash
FESX6 FSX 800 FSX 1600	Layer 2	Base Layer 3
FESX6 PREM FSX 800 PREM FSX 1600 PREM	Full Layer 3	Layer 2
ICX 6610	Full Layer 3	Layer 2

PoE Firmware files

Table 15 lists the PoE firmware file types supported for IronWare Release R07.3.00c. The firmware files are specific to their devices and are not interchangeable. For example, you cannot load FCX PoE firmware on a FSX device.

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. Brocade is still on the initial release of the microcontroller code, so there is no current need for an upgrade. The PoE firmware version string will be kept updated to match the corresponding FastIron software version; however, this is only a cosmetic change and the firmware itself remains unchanged. Should a new version of the 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.

Table 15 PoE Firmware files

Device	PoE Firmware
FESX6 FSX 800 FSX 1600	fsx_poe_07300c.fw
FSX 800 with SX-FI648PP or SX-FI-24GPP module FSX 1600 with SX-FI648PP or SX-FI-24GPP module	fsx_poeplus_07300c.fw and fsx_poeplus_07300c.fw

Upgrading the boot code

If you need 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 FCX or FSX 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.

   ```
   Device# 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 FCX device, you must delete the primary and secondary images before upgrading the image. To delete images from the flash, enter the following commands:

   ```
   Device# erase flash primary

   Device# 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.

   ```
   Device# 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.

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

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.

```
Device# show version

  Copyright (c) 1996-2011 Brocade Communications Systems, Inc.
    UNIT 3: compiled on Sep 26 2011 at 21:15:14 labeled as FCXR07300
                (6801867 bytes) from Primary fcxr07300.bin
        SW: Version 07.3.00T7f3
    UNIT 1: compiled on Sep 26 2011 at 21:15:14 labeled as FCXR07300
                (6801867 bytes) from Primary fcxr07300.bin
        SW: Version 07.3.00T7f3
    UNIT 2: compiled on Sep 26 2011 at 21:15:14 labeled as FCXR07300
                (6801867 bytes) from Primary fcxr07300.bin
        SW: Version 07.3.00T7f3
    UNIT 4: compiled on Sep 26 2011 at 21:15:14 labeled as FCXR07300
                (6801867 bytes) from Primary fcxr07300.bin
        SW: Version 07.3.00T7f3
    UNIT 5: compiled on Sep 26 2011 at 21:15:14 labeled as FCXR07300
                (6801867 bytes) from Primary fcxr07300.bin
        SW: Version 07.3.00T7f3
    UNIT 6: compiled on Sep 26 2011 at 21:15:14 labeled as FCXR07300
                (6801867 bytes) from Primary fcxr07300.bin
        SW: Version 07.3.00T7f3
    UNIT 7: compiled on Sep 26 2011 at 21:15:14 labeled as FCXR07300
                (6801867 bytes) from Primary fcxr07300.bin
        SW: Version 07.3.00T7f3
    UNIT 8: compiled on Sep 26 2011 at 21:15:14 labeled as FCXR07300
                (6801867 bytes) from Primary fcxr07300.bin
        SW: Version 07.3.00T7f3
  Boot-Monitor Image size = 369321, Version:07.3.00T7f5 (grz07300)
  HW: Stackable FCX648S-PREM (PROM-TYPE FCX-ADV-U)
==========================================================================
UNIT 1: SL 1: FCX-24GS 24-port Management Module
         License: FCX_ADV_ROUTER_SOFT_PACKAGE   (LID: )
         P-ENGINE  0: type DB90, rev 01
```

```
         PROM-TYPE: FCX-ADV-U
==========================================================================
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
         PROM-TYPE: FCX-ADV-U
==========================================================================
UNIT 2: SL 2: FCX-2XGC 2-port 16G Module (2-CX4)
==========================================================================
UNIT 3: 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
         PROM-TYPE: FCX-ADV-U
==========================================================================
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-F 24-port Management Module
         Serial  #: BFC2239E03J
         License: FCX_ADV_ROUTER_SOFT_PACKAGE   (LID: dheHHIOgFIl)
         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  #: BCV2218F091
         License: FCX_ADV_ROUTER_SOFT_PACKAGE   (LID: dexHHGNhFOG)
         P-ENGINE  0: type DB90, rev 01
==========================================================================
UNIT 5: SL 2: FCX-2XGC 2-port 16G Module (2-CX4)
==========================================================================
UNIT 6: SL 1: FCX-24GS 24-port Management Module
         Serial  #: BCV2218F0BX
         License: FCX_ADV_ROUTER_SOFT_PACKAGE   (LID: dexHHGNhFdz)
         P-ENGINE  0: type DB90, rev 01
==========================================================================
UNIT 6: SL 2: FCX-2XGC 2-port 16G Module (2-CX4)
==========================================================================
UNIT 7: SL 1: FCX-24GS 24-port Management Module
         Serial  #: BCV2218F099
         License: FCX_ADV_ROUTER_SOFT_PACKAGE   (LID: dexHHGNhFOO)
         P-ENGINE  0: type DB90, rev 01
==========================================================================
UNIT 7: SL 2: FCX-2XGC 2-port 16G Module (2-CX4)
==========================================================================
UNIT 8: SL 1: FCX-24GS 24-port Management Module
         Serial  #: BCV2218F0B7
         License: FCX_ADV_ROUTER_SOFT_PACKAGE   (LID: dexHHGNhFdM)
         P-ENGINE  0: type DB90, rev 01
==========================================================================
UNIT 8: SL 2: FCX-2XGC 2-port 16G Module (2-CX4)
==========================================================================
     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 "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.

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 FCX Series Hardware Installation Guide *Brocade FastIron WS Series Hardware Installation Guide* *Brocade FastIron X Series Chassis Hardware Installation Guide* *Brocade FastIron Edge X-Series Switch Hardware Installation guide* *Brocade ICX 6610 Series Hardware Installation Guide*	Describes the hardware as shipped. Provides installation instructions, hardware maintenance procedures, hardware specifications, and compliance information.
Unified IP MIB Reference	Simple Network Management Protocol (SNMP) Management Information Base (MIB) objects.

Document Title	Contents
Brocade FCX, Brocade FastIron SX, Brocade ICX 6610 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.
Brocade FCX and Brocade ICX 6610 Debug Guide	Documents debug commands for debugging devices.
TurboIron 24X Configuration Guide	Provides configuration procedures for system-level features, enterprise routing protocols, and security features for TurboIron 24X.
Brocade TurboIron 24X Series Hardware Installation Guide	Describes the TurboIron 24X hardware as shipped. Provides installation instructions, hardware maintenance procedures, hardware specifications, and compliance information.

Go to http://www.brocade.com/ethernetproducts to obtain the latest version of the guides. To report errors in the guide, send an email to documentation@brocade.com.

Closed Defects in IronWare Software Release 07.3.00c

Defect ID: DEFECT000333027	**Technical Severity:** Medium
Summary: Unicast DHCP offer packets are intermittently dropped	
Symptom: DHCP Client sometimes does not get the DHCP offer packet from the Server when connecting directly through TurboIron in the same VLAN.	
Probability: High	
Feature: TI IPv4 Forwarding	**Function:** DHCP Snooping
Reported In Release: FI TI 04.2.00	**Service Request ID:** 511501

Defect ID: DEFECT000346307	**Technical Severity:** Medium
Summary: “dm diag” causes the switch to get stuck in the diagnostic mode, making it unusable.	
Symptom: “dm diag” causes the switch to get stuck in the diagnostic mode, making it unusable	
Probability: High	
Feature: FI Platform Specific features	**Function:** system bringup
Reported In Release: FI 07.2.02	**Service Request ID:** 590679

Defect ID: DEFECT000346422	**Technical Severity:** High
Summary: After failing to copy 7.2.02a router image due to lack of flash space, user unable to write anything to the flash.	
Symptom: Get "Flash access in progress. Please try later" errors when trying to copy image from TFTP server or when saving the running configuration.	
Probability: High	
Feature: SX Network Management	**Function:** TFTP Configuration- Software V4/V6
Reported In Release: FI 07.2.02	**Service Request ID:** 592067

Defect ID: DEFECT000348065	**Technical Severity:** Critical
Summary: Traffic going through valid default route gets dropped.	
Symptom: All traffic that uses the default route is dropped if the default route is learned from OSPF, when Active/Standby Management Modules are present.	
Probability: High	
Feature: SX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.2.02	**Service Request ID:** 568471

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: DEFECT000355892	**Technical Severity:** High
Summary: SNMP: All Plat: the command “no snmp-server comm Public ro” is not retained after a reload. Once the Device reloads it will begin to respond to polling and read only operations using this community	
Symptom: Synopsis: the command when you use the command “no snmp-server comm Public ro” the public community will be disabled and our 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	

Defect ID: DEFECT000359994	**Technical Severity:** High
Summary: System continuously reloads with "Error: flash_get_fresh_block: no space."after upgrading to 7.2.02D Router code	
Symptom: Customer system continuously reloads after upgrading to 7202D.	
Feature: FCX Platform Specific features	**Function:** system bringup
Reported In Release: FI 07.2.02	**Service Request ID:** 643927

Defect ID: DEFECT000365448	**Technical Severity:** Medium
Summary: Private VLAN does not work as expected	
Symptom: When Private VLAN's are used, the "show mac" output is not consistent.	
Workaround: Downgrade code to version 7.1.00a.	
Probability: High	
Feature: FCX L2 Forwarding	**Function:** Private VLAN
Reported In Release: FI 07.2.02	**Service Request ID:** 660501

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.	
Probability: Medium	
Feature: SX L2 Control	**Function:** UDLD
Reported In Release: FI 07.2.02	**Service Request ID:** 670755

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	
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: DEFECT000374604	**Technical Severity:** Medium
Summary: IP forwarding between FCX stack units may fail after switchover with MSTP configuration	
Symptom: With MSTP configuration present, IP forwarding between FCX stack units may fail after doing a switchover.	
Workaround: Reload the whole stack again.	
Probability: Medium	
Feature: FCX L2 Control	**Function:** SpanningTree Protocols
Reported In Release: FI 07.3.00	**Service Request ID:** 681225

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: 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	
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: DEFECT000377562	**Technical Severity:** Medium
Summary: Q-in-Q removes the original customer's 802.1q tag for broadcast packets	
Symptom: Broadcast packets do not get forwarded at all in Q-in-Q environment.	
Probability: Medium	
Feature: FCX L2 Forwarding	**Function:** Q-in-Q
Reported In Release: FI 07.3.00	**Service Request ID:** 682505

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: DEFECT000379038	**Technical Severity:** Critical
Summary: High CPU condition when non-POE devices connect to POE-enabled ports	
Symptom: CPU usage rate goes high when non-POE devices are connected to POE-enabled ports.	
Workaround: Disable legacy POE detection by configuring the following command at the global level: "no legacy -inline-power <slot#>"	
Probability: High	
Feature: Power over Ethernet	**Function:** Power over Ethernet
Reported In Release: FI 07.3.00	**Service Request ID:** 680137

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: DEFECT000380312	**Technical Severity:** Medium
Summary: Unexpected reset may occur when dm command is issued in a VLAN that contains no ports.	
Symptom: Debug CLI command "dm 802-1w bridge vlan <ID>" may cause an unexpected reset of the device.	
Workaround: Add ports to the VLAN. Do not run the command.	
Probability: High	
Feature: FI Debug support	**Function:** dm commands - L2
Reported In Release: FI 07.3.00	**Service Request ID:** 689965

Defect ID: DEFECT000380727	**Technical Severity:** High
Summary: System Diagnostic feature not functioning on TI products	
Symptom: "dm diag" command is accepted on TI24 but upon resetting the device, it goes into application code without running diagnostics.	
Probability: High	
Feature: Platform	**Function:** Dm commands
Reported In Release: FI 07.4.00	**Service Request ID:** 714763

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: DEFECT000381773	**Technical Severity:** Medium
Summary: LACP may break if FCX stack is reloaded	
Symptom: LACP breaks if FCX stack is reloaded and only the Standby unit comes up.	
Probability: High	
Feature: FCX L2 Forwarding	**Function:** LinkAggregation - Static
Reported In Release: FI 07.3.00	**Service Request ID:** 695251

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:	DEFECT000382316	**Technical Severity:**	Medium
Summary:	FCX ports go into Blocking if both STP and 802.1w are configured after a stack reload		
Symptom:	FCX ports go into Blocking state if both STP and 802.1w are configured after a stack reload.		
Workaround:	Reload the whole FCX stack again.		
Probability:	High		
Feature:	FCX L2 Control	**Function:**	SpanningTree Protocols
Reported In Release:	FI 07.3.00	**Service Request ID:**	691379

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:	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: DEFECT000383004	**Technical Severity:** Medium
Summary: ARP and MAC entries may not be updated correctly on SX when a connected device is removed	
Symptom: With continuous traffic flowing to an attached device that has valid ARP and MAC entries, the ARP and MAC entries are not deleted when that device is disconnected.	
Workaround: After disconnecting the device, stop the continuous traffic meant for that device in order to age the ARP/MAC entries out.	
Probability: High	
Feature: SX L2 Forwarding	**Function:** MAC Table/FDB Manager
Reported In Release: FI 07.3.00	**Service Request ID:** 695827

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: 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	
Feature: FCX L2 Control	**Function:** PVST/PVST+/ PVRST
Reported In Release: FI 07.3.00	**Service Request ID:** 670195

Defect ID: DEFECT000383745	**Technical Severity:** Medium
Summary: Power supply front LEDs not working correctly	
Symptom: When the power supply unit is unplugged, the LED turns amber. But when it is plugged in again, the LED stays in amber and does not move to green.	
Probability: High	
Feature: FI Platform	**Function:** Power Supply/Temp Sensor/Fan Controller
Reported In Release: FI 07.3.00	**Service Request ID:** 696305

Defect ID: DEFECT000384066	**Technical Severity:** Medium
Summary: In PBR, the Secondary Gateway IP Address is not selected when the link to the Primary Gateway goes down	
Symptom: If multiple Next Hop gateways are configured in PBR, when the VLAN associated with the Primary Next Hop goes down, the Secondary Next Hop does not become effective if the Default Route is also configured.	
Probability: Low	
Feature: FCX Layer 3 Forwarding - IPV4	**Function:** PBR
Reported In Release: FI 07.3.00	**Service Request ID:** 697479

Defect ID: DEFECT000384408	**Technical Severity:** High
Summary: ServerIron HA PDUs (EtherType 0x885a) are not switched across VLAN	
Symptom: TI products incorrectly drop ServerIron control packets (Ethertype 0x885a) instead of switching them.	
Probability: Low	
Feature: FI L2	**Function:** Forwarding - Other
Reported In Release: FI 07.3.00	**Service Request ID:** 695053

Defect ID: DEFECT000385534	**Technical Severity:** High
Summary: MAC address being learned on STP Blocking port when DHCP snooping is enabled	
Symptom: If Spanning Tree is configured on a VLAN and DHCP Snooping is enabled on a port that is in Blocking state, a packet that is received on that port incorrectly triggers learning of its Source MAC address on it.	
Probability: High	
Feature: FI ACL	**Function:** DHCP Snooping functionality
Reported In Release: FI 07.4.00	**Service Request ID:** 712523, 712913

Defect ID: DEFECT000385924	**Technical Severity:** Medium
Summary: IPv6 Ping to Virtual IP Address fails after VRRP-E state change to Backup	
Symptom: IPv6 Ping to VRRP-E Virtual IP address times out after failing over from Master to Backup state.	
Workaround: Clear IPv6 cache and fail over VRRP-E again.	
Probability: High	
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:** 700737

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: DEFECT000387044	**Technical Severity:** High
Summary: FCX shows Power Supply Unit as normal even when it is inserted without power	
Symptom: If two PSU's are inserted into an FCX with no power cable plugged into PSU2, both PSU's are displayed as present and OK.	
Probability: High	
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

Defect ID:	DEFECT000388009	**Technical Severity:**	Medium
Summary:	DNS resolution does not work when multiple DNS domain lists are used		
Symptom:	When "ip dns domain-list <name>" command is used to specify more than one domain name, if the first one fails, the device retries for it and times out instead of trying the successive domain names.		
Probability:	High		
Feature:	FCX Management Functionality	**Function:**	HTTPs/HTTP
Reported In Release:	FI 07.2.02	**Service Request ID:**	697877

Defect ID:	DEFECT000388194	**Technical Severity:**	Medium
Summary:	SSH session to device may disconnect due to bad server public DH value		
Symptom:	SSH login attempts to the switch repeatedly fail after several attempts when using the default OpenSSH installation with Ubuntu 10.04 and possibly other versions/distributions.		
Workaround:	Reload the device or use Telnet/Console instead of SSH.		
Probability:	Low		
Feature:	FCX Management Functionality	**Function:**	IPv4/V6 SSH Service
Reported In Release:	FI 07.3.00	**Service Request ID:**	688843, 700589

Defect ID:	DEFECT000388293	**Technical Severity:**	Medium
Summary:	Standby Management module may not come up after upgrading to 7.3 or greater code base due to calibration errors		
Symptom:	Standby Management module does not come up and displays the following message on the console - "Error: valid DFCDL file not found for slot 9 in hal_hw_init()"		
Probability:	Low		
Feature:	FI Platform Specific features	**Function:**	system bringup
Reported In Release:	FI 07.3.00	**Service Request ID:**	704997

Defect ID:	DEFECT000388432	**Technical Severity:**	High
Summary:	Switch may reset when it gets the digital signature from the SSH Client and validates it		
Symptom:	With OpenSSH 5.5p1&Open SSL 0.9.8o, multiple logins to the device can cause the switch to reset.		
Probability:	Medium		
Feature:	FCX Network Management	**Function:**	SSHv2/SCP V4/V6
Reported In Release:	FI 07.3.00	**Service Request ID:**	709277

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 mitigate the issue.	
Probability: Medium	
Feature: OSPF	**Function:** OSPF
Reported In Release: FI 07.2.02	**Service Request ID:** 708908, 712545

Defect ID: DEFECT000389267	**Technical Severity:** Low
Summary: Username could get overwritten due to changes in other usernames in the configuration	
Symptom: If the first username is changed many times, the successive usernames may get overwritten and are displayed with unexpected characters.	
Probability: Medium	
Feature: SX Network Management	**Function:** AAA RADIUS/TACACS+ V4/V6
Reported In Release: FI 07.2.02	**Service Request ID:** 710445

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" 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: DEFECT000390166	**Technical Severity:** Medium
Summary: Brocade Web GUI shows VLAN 0 for all ports on FCX	
Symptom: All ports are displayed incorrectly as being in VLAN 0 via the Brocade Web GUI.	
Probability: Medium	
Feature: FCX Management Functionality	**Function:** HTTPs/HTTP
Reported In Release: FI 07.3.00	**Service Request ID:** 712561

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.	
Workaround: Use 5.1.00f instead of anything in the 7 range.	
Probability: Low	
Feature: SX L2 Forwarding	**Function:** Subnet VLAN
Reported In Release: FI 07.2.02	**Service Request ID:** 711367

Defect ID: DEFECT000391366	**Technical Severity:** Medium
Summary: "Version Number" field is not correctly displayed in the "show pid" command output	
Symptom: On TI24X running 7.3.00 or later, "show pid" command returns error for "Version Number".	
Probability: Low	
Feature: FI Platform	**Function:** EEPROM - serial number/LID/etc
Reported In Release: FI 07.3.00	**Service Request ID:** 714305

Defect ID: DEFECT000391539	**Technical Severity:** Medium
Summary: Cisco AP using proprietory TLV may not work after Brocade switch reload	
Symptom: Cisco AP using proprietory TLV may not work after Brocade switch reload	
Probability: High	
Feature: Power over Ethernet	**Function:** Power over Ethernet
Reported In Release: FI 07.3.00	**Service Request ID:** 674465

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.	
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: reload the switch/router during manintenance window to clear.	
Probability: Medium	
Feature: FCX L2 Forwarding	**Function:** MAC Table/FDB Manager
Reported In Release: FI 07.2.00	**Service Request ID:** 712255

Defect ID: DEFECT000392549	**Technical Severity:** Medium
Summary: VRRP-E flaps when ports are added or removed from a VLAN through Web Management interface	
Symptom: VRRP-E flaps when ports are added or removed from a VLAN through Web Management interface.	
Workaround: add or delete ports from CLI	
Probability: Medium	
Feature: FCX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.3.00	**Service Request ID:** 693427

Defect ID: DEFECT000393415	**Technical Severity:** Medium
Summary: IP Follow VE address may be unreachable upon creation when VRRP is enabled on the Master VE	
Symptom: Unable to ping newly-added Virtual Interface IP Address configured with IP Follow feature.	
Workaround: disable/enable master interface OR disable/enable vrrp instance on master interface	
Probability: Low	
Feature: SX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Virtual interface (ve) Manager
Reported In Release: FI 07.2.02	**Service Request ID:** 706005

Defect ID: DEFECT000394040	**Technical Severity:** Medium
Summary: CPU memory usage increases constantly when using OpenNMS tool to poll system's 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	
Probability: High	
Feature: SX Management Functionality	**Function:** IPv4/V6 SSH Service
Reported In Release: FI 07.2.02	**Service Request ID:** 704159

Defect ID:	DEFECT000394590	**Technical Severity:**	Low
Summary:	Flow control packets seen with no traffic on Fiber ports with 1G SFP		
Symptom:	Flow control packets with the pause quanta field set to zero, which do not make the partner stop the traffic, are seen with no traffic on 1G Fiber ports.		
Workaround:	Configure 'no flow control' on the port.		
Probability:	High		
Feature:	FI Infrastructure	**Function:**	Flow Control
Reported In Release:	FI 07.3.00	**Service Request ID:**	724451

Defect ID:	DEFECT000395855	**Technical Severity:**	High
Summary:	SX 2x10G cards may fail to initialize on cold start due to errors when trying to read EEPROM		
Symptom:	If an SX1600 switch is powered off for several hours and then powered on, some of the 2x10G line modules will fail to initialize with the following error: "Unable to read slot 1 EEPROM... please re-insert the line card in slot 1"		
Workaround:	re-enable line modules from CLI using enable/disable command		
Probability:	Low		
Feature:	FI Platform Specific features	**Function:**	system bringup
Reported In Release:	FI 07.3.00	**Service Request ID:**	713675

Defect ID:	DEFECT000396159	**Technical Severity:**	Low
Summary:	Radius IP Address may be displayed incorrectly in the output of “sh table-mac-vlan detail”		
Symptom:	In the "show table-mac-vlan detail" display, not enough characters are allocated for the Radius IP address column, which might 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:	DEFECT000399035	**Technical Severity:**	Medium
Summary:	Routed packets on an FCX/ICX stack may have an incorrect Source MAC address		
Symptom:	When a Stack MAC Address is configured for an FCX/ICX stack, a routed packet that egresses the stack has a Source MAC Address with the first 5 octets identical to the Stack MAC, but may have the last octet overwritten.		
Probability:	High		
Feature:	FCX Layer 3 Forwarding - IPV4	**Function:**	Data Forwarding (IPV4)
Reported In Release:	FI 07.3.00	**Service Request ID:**	720777

Closed Defects in IronWare Software Release 07.3.00b

Defect ID:	DEFECT000303853	**Technical Severity:**	High
Summary:	Unable to configure VRRP in base layer 3 code.		
Symptom:	Unable to configure VRRP in base layer 3 code.		
Probability:	High		
Feature:	SX Layer3 Control Protocols	**Function:**	VRRP/VRRP-E and slow-start timer- VRRP-E timer scale
Reported In Release:	FI 07.1.00	**Service Request ID:**	253547

Defect ID: DEFECT000381441	**Technical Severity:** Medium
Summary: 8 port management card shows all ports UP even without any cable connected	
Symptom: 8 port management card shows all ports UP even without any cable connected	
Feature: FI Platform Specific features	**Function:** Management Port
Reported In Release: FI 07.3.00	**Service Request ID:** 694599

Closed Defects in IronWare Software Release 07.3.00a

The following defects have been closed as part of this release with code changes as of December 21, 2011.

Customer reported defects closed with code in Release 07.3.00a

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of December 16, 2011.

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: 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	
Feature: SX Layer1 features	**Function:** port flap dampening
Reported In Release: FI 07.2.00	**Service Request ID:** 624889

Defect ID: DEFECT000338676	**Technical Severity:** Medium
Summary: Installing a cable in the SFP ports 1/1 to 1/2 causes the LED on the copper combo ports 1/2 to be lit.	
Feature: FCX Layer1 features	**Function:** link status - speed and duplex status
Reported In Release: FI 07.2.00	**Service Request ID:** 548131

Defect ID: DEFECT000348267	**Technical Severity:** Medium
Summary: Unable to set POE via SNMPSET on FWS	
Symptom: Can read the POE value using snmpwalk command but cannot set using snmpset command. Sytem responds: Error in packet. Reason: undoFailed	
Workaround: Set the POE via the CLI	
Feature: POE MIBS	**Function:** POE MIBS
Reported In Release: FI 07.2.02	**Service Request ID:** 578485

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: 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:** 650833,660501

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: DEFECT000368973	**Technical Severity:** High
Summary: If inline power is configured through SNMP on FWS, device allocates only 1W to the port	
Symptom: On configuring inline power through SNMP, power devices may not come up	
Workaround: Please use Command Line Interface to configure inline power	
Probability: Low	
Feature: FI Embedded Management	**Function:** SNMP
Reported In Release: FI 07.3.00	

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: DEFECT000369547	**Technical Severity:** Medium
Summary: DHCP Client - SX device connected via another DUT to server is not getting IP address	
Symptom: Customer may see the issue.	

Probability: Medium	
Feature: SX DHCP CLIENT	**Function:** DHCP
Reported In Release: FI 07.3.00	**Service Request ID:** 694027 694027

Defect ID: DEFECT000370080	**Technical Severity:** High
Summary: DSCP tag values for VRRPv2, VRRPv3, and ICMPv6-Router Advertisements(RA) packets are 0	
Symptom: The current priority field values for VRRPv2, VRRPv3, and ICMPv6-RA are set to zero	
Probability: High	
Feature: Layer3 Control Protocols	**Function:** VRRP/VRRP-E and slow-start timer- VRRP-E timer scale
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000371312	**Technical Severity:** High
Summary: Port LED does not glow when E1MG-TX optics is plugged into the 1G ports on ICX6610-24F and the speed is set to 100 full	
Symptom: Port LED does not glow when E1MG-TX optics is plugged into the 1G ports on ICX6610-24F and the speed is set to 100 full	
Probability: Low	
Feature: Optics	**Function:** OPTICS
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000374288	**Technical Severity:** High
Summary: On Production ICX 24P Fiber Units, Links don't come up when E1MG-TX optics are plugged in	
Symptom: [ICX] If copper GBIC is used in 1G SFP port, link may not come up	
Workaround: no	
Probability: Medium	
Feature: FI Platform	**Function:** 1G Link
Reported In Release: FI 07.3.00	

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: DEFECT000375146	**Technical Severity:** High
Summary: A very long CLI string may be truncated in the running-configuration	
Symptom: A very long CLI string may be truncated in the running-configuration	
Probability: Medium	
Feature: SX Management Functionality	**Function:** CLI and parser
Reported In Release: FI 05.1.00	**Service Request ID:** 683689

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	
Feature: FI Infrastructure	**Function:** SX Hitless OS upgrade
Reported In Release: FI 07.3.00	**Service Request ID:** 680843

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	
Feature: FI Platform	**Function:** Power Supply/Temp Sensor/Fan Controller
Reported In Release: FI 07.3.00	**Service Request ID:** 686691

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	
Feature: SX Platform Specific features	**Function:** Management module redundancy
Reported In Release: FI 07.2.00	**Service Request ID:** 682807

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	
Feature: FCX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.3.00	**Service Request ID:** 687111

Defect ID: DEFECT000381053	**Technical Severity:** Medium
Summary: DHCP does not work with SX-FI-24 GPP cards	
Symptom: DHCP does not work with SX-FI-24 GPP cards on superx	
Probability: High	
Feature: SX DHCP CLIENT	**Function:** DHCP
Reported In Release: FI 07.3.00	**Service Request ID:** 694027

Closed Defects in IronWare Software Release 07.3.00

The following defects have been closed as part of this release.

Customer reported defects closed with code in Release 07.3.00

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of October 13, 2011.

Defect ID: DEFECT000335488	**Technical Severity:** Critical
Summary: A fully loaded SX1600 will not synchronize with the redundant management module	
Symptom: Active and Standby module with be out of sync and Standby module will crash	
Probability: High	
Feature: SX Platform Specific Features	**Function:** Management Module Redundancy
Reported In Release: FI 07.2.00	**Service Request ID**: 509075

Defect ID: DEFECT000318624	**Technical Severity:** High
Summary: On FSX platform, v4 and v6 license is shown as "invalid"	
Symptom: V4 ADV software license is shown as invalid on both v4 and v6 chassis	
Probability: High	
Feature: FCX SW License	**Function:** Licensing
Reported In Release: FI 07.2.00	**Service Request ID**:

Defect ID: DEFECT000320370	**Technical Severity:** Medium
Summary: FGS Buffer depletion when running multiple instances of a looped SNMP Bulk get Script	
Symptom: Device runs out of memory	
Probability: Medium	
Feature: FCX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 07.2.00	

Defect ID: DEFECT000325993	**Technical Severity:** Low
Summary: "show inline power detail" display is inconsistent between active and standby units	
Symptom: Standby unit displaying wrong POE firmware version for active unit	
Probability: Low	
Feature: FCX Stacking	**Function:** PoE/PoE+
Reported In Release: FI 07.2.00	

Defect ID: DEFECT000326814	**Technical Severity:** Medium
Summary: LED remains green after removing PoE Powered Device from a port.	
Symptom: If a PoE PD is removed from a port, the LED for that port still remains green as if it was still plugged in.	
Probability: High	
Feature: FCX Layer1 features	**Function:** PoE/PoE+
Reported In Release: FI 07.2.00	

Defect ID: DEFECT000329490	**Technical Severity:** High
Summary: SX system reloads due to running out of Multicast next hop entries	
Symptom: SX system may reload after continuously displaying error messages due to next hop entries not being available for Multicast route programming	
Probability: Low	
Feature: SX L2/L3 Multicast Features	**Function:** PIM Sparse
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000332429	**Technical Severity:** Low
Summary: When a standby module is inserted into an SX chassis, it does not display a License ID	
Symptom: Newly inserted management module will display a blank entry for the License.	
Workaround: Set the active management module to the new one and reload the device.	
Probability: High	
Feature: FCX SW License	**Function:** Licensing
Reported In Release: FI 07.2.02	**Service Request ID:** 595349

Defect ID: DEFECT000334142	**Technical Severity:** Medium
Summary: Cannot open web authentication login page after moving from one port to another.	
Symptom: If a client first logs in using web authentication on one port, and then moves to another port of the switch, the client will not be able to reopen the web authentication login page.	
Probability: Low	
Feature: FCX Network Management	**Function:** Web Management
Reported In Release: FI 07.2.00	**Service Request ID:** 504247

Defect ID: DEFECT000335182	**Technical Severity:** Medium
Summary: Incorrect display in ipCidrRouteTable MIB	
Symptom: While executing an snmpwalk on a FESX 424-PREM system using ipCidrRouteDest MIB 1.3.6.1.2.1.4.24.4.1.1, the result shows incorrect subnet mask and route destination values	
Probability: High	
Feature: SX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 07.2.00	**Service Request ID:** 505491

Defect ID: DEFECT000335749	**Technical Severity:** Medium
Summary: Error message displayed when configuring port mirroring if sFlow is enabled.	
Symptom: Error message displayed when configuring inbound port mirroring and monitoring if sFlow is also enabled on that port."	
Workaround: Remove sFlow temporarily from the port(s). Configure the monitoring, then add sFlow back.	
Probability: Medium	
Feature: SX Management Functionality	**Function:** CLI and parser
Reported In Release: FI 07.2.00	**Service Request ID:** 524679

Defect ID: DEFECT000336328	**Technical Severity:** Medium
Summary: ACL dynamically applied does not take effect on the multi-chassis trunk link on the standby stack unit	
Symptom: ACL dynamically applied does not take effect on the multi-chassis trunk link on the standby stack unit	
Probability: High	
Feature: FCX Stacking	**Function:** IPC Sync messages
Reported In Release: FI 07.2.00	**Service Request ID:** 506901

Defect ID: DEFECT000338071	**Technical Severity:** High
Summary: In an MCT configuration, all members of a LAG on FCX get disabled when one of the connected MCT devices is reset, even though the other MCT device is still up.	
Symptom: With an FCX connected to two MCT devices using a single Link Aggregation Group, if one of the MCT devies is reset, all link members the LAG on FCX get disabled.	
Probability: High	
Feature: FCX L2 Control	**Function:** LinkAggregation - LACP/Dynamic
Reported In Release: FI 07.2.00	**Service Request ID:** 543693

Defect ID: DEFECT000338822	**Technical Severity:** Medium
Summary: Trunk goes down forever if Master switch in FCX stack goes down for 2 minutes	
Symptom: When the Master FCX switch in a stack is brought down and then restarted after 2 minutes, the trunk does not get re-established.	
Workaround: Reload the master and standby switches again.	
Probability: High	
Feature: SX L2 Control	**Function:** LinkAggregation - LACP/Dynamic
Reported In Release: FI 07.2.00	**Service Request ID:** 530331

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: DEFECT000339214	**Technical Severity:** Medium
Summary: If a user is authenticated by 802.1x via an IP ACL, the ACL may affect another user on the same port that was not authenticated with the ACL.	
Symptom: If there are two users on a given port, one authenticated by an IP ACL and one authenticated without an IP ACL, reconnecting the former will cause the ACL to affect the latter user.	
Probability: High	
Feature: FCX ACL	**Function:** 802.1x authentication
Reported In Release: FI 07.2.00	**Service Request ID:** 550451

Defect ID: DEFECT000340240	**Technical Severity:** Medium
Summary: SX devices could reload due to a memory leak when running Multicast traffic	
Symptom: With Multicast data traffic running, the CPU memory could run out, causing the device to reload.	
Probability: Medium	
Feature: SX L2/L3 Multicast Features	**Function:** PIM Sparse
Reported In Release: FI 07.2.00	**Service Request ID:** 528867

Defect ID: DEFECT000340947	**Technical Severity:** Medium
Summary: IP route may not be programmed to TCAM although it is added to the IP route table when OSPF route takes over from a static route.	
Symptom: When a static route gets deleted due to the link to the next hop going down, and OSPF takes over for that route, the route gets added to the IP routing table, but a packet destined to the route is dropped.	
Workaround: Issue "clear ip route".	
Probability: High	
Feature: FCX Layer3 Control Protocols	**Function:** OSPFV2 - IPV4
Reported In Release: FI 07.2.00	**Service Request ID:** 558807

Defect ID: DEFECT000341364	**Technical Severity:** Medium
Summary: Optical-monitor caused bogus syslog messages	
Symptom: Syslog messages SYSTEM: Optic is not Brocade qualified (port 1/1/1) is logged although port 1/1/1 is a copper port	
Probability: High	
Feature: FCX Layer1 features	**Function:** Digital Optical Monitoring
Reported In Release: FI 07.2.02	**Service Request ID:** 547677

Defect ID: DEFECT000342071	**Technical Severity:** Medium
Summary: PIM Dense forwarding cache entry gets removed even while active stream is present.	
Symptom: Continuity errors are seen every few minutes when continuous PIM traffic is being forwarded.	
Probability: High	
Feature: SX L2/L3 Multicast Features	**Function:** PIM Dense
Reported In Release: FI 07.2.02	**Service Request ID:** 559053

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/powersupplies/temperature sensors
Reported In Release: FI 07.3.00	**Service Request ID:** 641069

Defect ID: DEFECT000343165	**Technical Severity:** Medium
Summary: Fully loaded SuperX CPU goes to 18% without any configuration.	
Symptom: After upgrading from 5.1.00d to 7.2.02a, CPU utilization increases from 1% to 18%.	
Probability: High	
Feature: SX_SYSTEM	**Function:** UNDETERMINED
Reported In Release: FI 07.2.02	**Service Request ID:** 578549

Defect ID: DEFECT000343288	**Technical Severity:** Medium
Summary: ACL dynamically applied from the Active FCX stack unit does not take effect on the Standby unit	
Symptom: ACL dynamically applied from the Active FCX stack unit does not take effect on the Standby unit if "enable acl-per-port-per-vlan" is not configured	
Probability: High	
Feature: FCX ACL	**Function:** ACL(all aspects of ACLs - IPV4)
Reported In Release: FI 07.2.02	**Service Request ID:** 578523

Defect ID: DEFECT000344224	**Technical Severity:** Medium
Summary: Uplink-switch fails to limit the formation of IPv6 neighbor relationships.	
Symptom: If you enable uplink-switch in a VLAN, the FWS will successfully prevent ARP request broadcasts from being forwarded between non-uplink ports, but the FWS will fail to prevent IPv6 neighbor relationships from being formed between non-uplink ports.	
Probability: High	
Feature: SX L2 Forwarding	**Function:** Uplink-Switch
Reported In Release: FI 07.2.02	**Service Request ID:** 583307

Defect ID: DEFECT000344380	**Technical Severity:** Medium
Summary: FCX IP traffic goes to cpu with 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: DEFECT000345082	**Technical Severity:** Medium
Summary: Trunk interface goes into Blocked state if spanning tree is disabled on interface	
Symptom: Issuing “no spanning-tree” on a Trunk port causes it to go into Blocking state.	
Probability: High	
Feature: FCX L2 Control	**Function:** LinkAggregation - LACP/Dynamic
Reported In Release: FI 07.2.00	**Service Request ID:** 582937

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 neigbor 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: DEFECT000346307	**Technical Severity:** Medium
Summary: “dm diag” causes the switch to get stuck in the diagnostic mode, making it unusable.	
Symptom: “dm diag” causes the switch to get stuck in the diagnostic mode, making it unusable	
Probability: High	
Feature: FI Platform Specific features	**Function:** system bringup
Reported In Release: FI 07.2.02	**Service Request ID:** 590679

Defect ID: DEFECT000346568	**Technical Severity:** Medium
Summary: Interface level command “dhcp snooping client-learning disable” missing in 7.2 code.	
Symptom: Interface level command “dhcp snooping client-learning disable” present in 7.0.01 code but missing in 7.2 code.	
Probability: High	
Feature: FCX DHCP	**Function:** Client
Reported In Release: FI 07.2.00	**Service Request ID:** 591879

Defect ID: DEFECT000346882	**Technical Severity:** High
Summary: SNMPv3 configuration sometimes gets corrupted.	
Symptom: If multiple SNMP groups and users are configured, removed and re-added, the running configuration could show corrupted values.	
Probability: Medium	
Feature: FI Embedded Management	**Function:** CLI and parser
Reported In Release: FI 07.3.00	**Service Request ID:** 608663

Defect ID: DEFECT000347484	**Technical Severity:** High
Summary: Memory leak may be observed when Policy Based Routing is configured	
Symptom: Memory leak may be observed when Policy Based Routing is configured	
Probability: High	
Feature: FI L3 Unicast	**Function:** Forwarding - PBR
Reported In Release: FI 07.3.00	**Service Request ID:** 672437

Defect ID: DEFECT000347677	**Technical Severity:** Medium
Summary: Maximum number of traffic policies changed from 256 in 4.x code to 50 in 7.2.x code.	
Symptom: Cannot configure more than 50 traffic policies in 7.2.02 code.	
Probability: High	
Feature: Traffic Policy	**Function:** Traffic Policy
Reported In Release: FI 07.2.02	**Service Request ID:** 558097

Defect ID: DEFECT000347906	**Technical Severity:** Critical
Summary: Upon loading a new bootcode to the flash, multiple units of an FCX stack can experience a reload.	
Symptom: Some units of an FCX stack can unexpectedly reload when a new bootcode is downloaded to the active unit's flash.	
Probability: Medium	
Feature: FI Platform	**Function:** Boot code/Flash/Kernel
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000348432	**Technical Severity:** Medium
Summary: FWS system fan noise is too high when operating at room temperature.	
Symptom: FWS system fan noise is higher than permissible when operating at room temperature.	
Probability: High	
Feature: FCX Platform Specific features	**Function:** Chassis/fan/powersupplies/temperature sensors
Reported In Release: FI 07.2.02	

Defect ID: DEFECT000349335	**Technical Severity:** High
Summary: Routing data traffic to management network may result in buffer loss	
Symptom: Routing data traffic to out of band management network may result in buffer loss	
Probability: High	
Feature: SX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.2.02	**Service Request ID:** 602867

Defect ID: DEFECT000349416	**Technical Severity:** High
Summary: Debug tool to track CPU buffer usage does not work.	
Symptom: The commands to track buffer leaking: “dm gi-buffer-debug” and “dm track-buffer-show” do not display the used buffers.	
Probability: High	
Feature: FCX Platform Specific features	**Function:** Management Port
Reported In Release: FI 07.2.02	**Service Request ID:** 602867

Defect ID: DEFECT000350084	**Technical Severity:** Medium
Summary: CPU memory usage can continuously increase in 7.2.02, eventually causing the device to reload.	
Symptom: With certain network access controllers, every time a user logs in and logs out, memory usage increases by 1%.	
Probability: High	
Feature: FIPS	**Function:** FIPS
Reported In Release: FI 07.2.02	**Service Request ID:** 571469

Defect ID: DEFECT000350162	**Technical Severity:** Medium
Summary: FCX PoE power allocating 30 watts although the port is down and is not operational .	
Symptom: Under some circumstances, the 'show inline power' displays that the port is allocated 30 Watts even though the port is down and operationally off.	
Probability: Low	
Feature: FCX Layer1 features	**Function:** PoE/PoE+
Reported In Release: FI 07.2.02	**Service Request ID:** 608563

Defect ID: DEFECT000350302	**Technical Severity:** Medium
Summary: On a 2-Unit FCX stack with a trunk configured across the units, traffic doesn’t fall back to the Standby ports when the Active goes down.	
Symptom: After power cycling the master in a 2 unit stack, ARP is not learnt on the trunk port, causing packet loss.	
Probability: High	
Feature: FCX L2 Control	**Function:** LinkAggregation - LACP/Dynamic
Reported In Release: FI 07.2.02	**Service Request ID:** 599545

Defect ID: DEFECT000350592	**Technical Severity:** High
Summary: FWS cannot load router code with license upon erasing the EEPROM.	
Symptom: If EEPROM is erased, FWS with valid license shows error message and does not boot up when trying to load a router image.	
Probability: High	
Feature: SW licensing	**Function:** Licensing All
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000352213	**Technical Severity:** High
Summary: After reloading, ICXs console halts for over 25 minutes to sync up the dhcp_lease_binding.txt file of size 23000 bytes in flash.	
Symptom: ICXs console halts for over 25 minutes	
Probability: Medium	
Feature: FI Embedded Management	**Function:** DHCP IPv4 Client/Server
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000352356	**Technical Severity:** Medium
Summary: Uplink-switch fails to limit the formation of IPv6 neighbor relationships in a VLAN if management-vlan is configured in a separate VLAN.	
Symptom: If you enable management-vlan in one VLAN and then enable uplink-switch in another VLAN, the VLAN with uplink-switch will successfully prevent ARP request broadcasts from being forwarded between non-uplink ports, but it will fail to prevent IPv6 neighbor relationships from being formed between non-uplink ports.	
Probability: High	
Feature: FI L2	**Function:** Forwarding - uplink switch
Reported In Release: FI 07.3.00	**Service Request ID:** 623977

Defect ID: DEFECT000352576	**Technical Severity:** Medium
Summary: CPU Memory leak is not traceable by the memory leak finding tool.	
Symptom: Although “show memory” command detects that CPU memory is depleting, the “dm mem-leak” tool fails to identify it.	
Probability: High	
Feature: FI Debug support	**Function:** dm commands - General
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000353245	**Technical Severity:** High
Summary: System allocates 30W power to a PoE Port even if it detects a non-Powered Device connected to it	
Symptom: Although the System correctly detects the operational state of a port connected to a non-Powered Device as off, it may still allocate 30W to it.	
Probability: High	
Feature: FI Platform Specific features	**Function:** PoE/PoE+
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000353729	**Technical Severity:** Medium
Summary: FCX/FGS switches are not responding to ICMPv6 echo request	
Symptom: FESX6, 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: DEFECT00053823	**Technical Severity:** High
Summary: [SX] Multicast traffic duplicated when the VEs with pim-sparse configured face towards a SWTCH	
Symptom: Duplicate multicast packets are seen on other devices in the network	
Probability: Medium	
Feature: FI L3 Multicast	**Function:** Control Plane - PIM Sparse
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000353828	**Technical Severity:** High
Summary: ZR Optic is not passing traffic after upgrading to 7.2.02.	
Symptom: When upgrading from 7.2.00 to 7.2.02a on FCX platform, 10G-ZR optics send traffic but do not receive traffic.	
Probability: High	
Feature: Optics	**Function:** OPTICS
Reported In Release: FI 07.2.02	**Service Request ID:** 568471

Defect ID: DEFECT000354169	**Technical Severity:** Medium
Summary: A system memory leak may be seen when running 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: High	
Feature: SX L2/L3 Multicast Features	**Function:** PIM Sparse
Reported In Release: FI 07.3.00	**Service Request ID:** 670015

Defect ID: DEFECT000354279	**Technical Severity:** High
Summary: FCX may allocate incorrect wattage to all ports with Powered Devices, regardless of class.	
Symptom: After configuring "inline power power-by-class 1" and then "inline power power-by-class 0", FCX will allocate 30W to all ports with PD.	
Probability: High	
Feature: FI Platform Specific features	**Function:** PoE/PoE+
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000355279	**Technical Severity:** Medium
Summary: DHCP Server-Client binding does not get cleared when "no ip dhcp-client enable" is issued on the client.	
Symptom: A new IP address is not assigned for 5 or more minutes even if the "no ip dhcp-client enable" command is issued to clear the original DHCP Server-Client binding.	
Probability: High	
Feature: FCX DHCP	**Function:** Server
Reported In Release: FI 07.2.02	

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:** Data Forwarding (IPv4)
Reported In Release: FI 07.2.02	**Service Request ID:** 625975

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 a stack goes down, OSPF routes that used this disabled unit's ports will remain in the routing table indefinitely.	
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.	
Feature: Sw licensing	**Function:** Licensing
Probability: Low	
Found in Release: FI 07.3.00	**Service Request ID:** 642829

Defect ID: DEFECT000356978	**Technical Severity:** High
Summary: FCX / STK2: After active unit was removed from the stack, OSPF interfaces on standby or member unit stayed in EXST state	
Symptom: OSPF neighbor relationship is not formed	
Probability: Medium	
Feature: FI L3 Unicast	**Function:** Control Plane - OSPF/OSPFv3
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000357433	**Technical Severity:** High
Summary: Layer 3 traffic sometimes does not get forwarded on an FCX stack.	
Symptom: IP Traffic is not forwarded on an FCX stack's member units.	
Workaround: Clearing the MAC or ARP tables temporarily resolves the problem.	
Probability: Low	
Feature: FCX Layer 3 Forwarding - IPV4	**Function:** Data Forwarding (IPV4)
Reported In Release: FI 07.2.02	**Service Request ID:** 601967

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: 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
Reported In Release: FI 07.3.00	**Service Request ID:** 642829

Defect ID: DEFECT000358969	**Technical Severity:** High
Summary: DHCP Server binding table shows a single IP address bound to multiple MAC addresses	
Symptom: When DHCP Server is enabled, multiple clients sending DHCP requests to a single port may get the same IP address assigned to them.	
Probability: Medium	
Feature: FCX DHCP	**Function:** Server
Reported In Release: FI 07.2.02	

Defect ID: DEFECT000359744	**Technical Severity:** Medium
Summary: FESX6 code flash memory is incorrectly displayed as 16MB	
Symptom: FESX6 code flash memory is displayed 16MB instead of 8MB	
Probability: High	
Feature: SX_SYSTEM	**Function:** UNDETERMINED
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, Eth1 the first port of the system may be removed from the VLAN 1	

Symptom: After enabling Single Spanning-tree and reloading the device, Eth1 the first port of the system may be removed from the VLAN 1	
Probability: High	
Feature: SX L2 Control	**Function:** single spanning-tree
Reported In Release: FI 07.2.02	**Service Request ID:** 643797

Defect ID: DEFECT000363716	**Technical Severity:** Medium
Summary: FCX CPU rate limits broadcast ARP packets to as low as 256 Packets per second	
Symptom: ARP resolution will fail	
Probability: Medium	
Feature: FCX Layer 3 Forwarding - IPV4 and IPV6	**Function:** ARP
Reported In Release: FI 07.2.02	**Service Request ID:** 653983

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: Stacking FCX fails to transmit L3 routing packet when Master unit is powered off. 'show arp' shows a port on the old Master unit which is inactive.	
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: Not able to ping the FSX from directly connected PC on 48 port poe card	
Symptom: Unable to ping the FSX from directly connected PC on 48 port poe 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 master unit 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: Medium	
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.	
Probability: High	
Feature: FCX Network Management	**Function:** sFlow
Reported In Release: FI 07.2.02	**Service Request ID:** 669137

Defect ID: DEFECT000362369	**Technical Severity:** Medium
Summary: Spanning Tree State Not In SYNC with Primary Port of Trunk Port after stack is rebooted.	
Symptom: After hitless failover, Spanning Tree state on the primary port of a trunk shows correctly as "OFF" but shows incorrectly as ON on the member port	
Probability: Medium	
Feature: FCX L2 Control	**Function:** LinkAggregation - LACP/Dynamic
Reported In Release: FI 07.2.02	**Service Request ID:** 645709

Customer reported defects closed without code in Release 07.3.00

This section lists the defects with Critical, High and Medium Technical Severity closed without a code change as of October 13, 2011.

Defect ID:	DEFECT000344733	**Technical Severity:**	Medium
Summary:	Secure copy does not work if done to startup config.		
Symptom:	Secure copy to startup configuration on FCX fails, although secure copy to running configuration works.		
Probability:	Medium		
Feature:	FCX Management Functionality	**Function:**	CLI and parser
Reported In Release:	FI 07.2.02	**Service Request ID:**	585183

Defect ID:	DEFECT000351027	**Technical Severity:**	Medium
Summary:	FCX HPOE products with Advanced License are incorrectly displayed as POE.		
Symptom:	The output of “show version” displays FCX648 and FCX624 HPOE products with Advanced License as “FCX648S-POE-PREM” and “FCX624S-POE-PREM” respectively.		
Probability:	High		
Feature:	FCX Management Functionality	**Function:**	CLI and parser
Reported In Release:	FI 07.2.02		

Defect ID:	DEFECT000363357	**Technical Severity:**	High
Summary:	SXR07300q053 STBY MP continuously reloads after downgrade to SXR07202d		
Symptom:	STBY module resets after downgrade		
Probability:	High		
Feature:	FI Platform Specific features	**Function:**	Management module redundancy
Reported In Release:	FI 07.3.00		

Defect ID:	DEFECT000365719	**Technical Severity:**	Medium
Summary:	dynamic-vlan-discovery is enabled by default		
Symptom:	A customer noted strange traffic similar to udld in ether type and destination mac 0x885a and 00:e0:52:00:00:00		
Workaround:	'no dynamic-vlan-discovery' will disable the feature		
Probability:	High		
Feature:	L2	**Function:**	Dynamic VLAN Discovery
Reported In Release:	FI 07.2.02	**Service Request ID:**	643357

Defect ID:	DEFECT000369317	**Technical Severity:**	Medium
Summary:	Connectivity problem along with ARP error messages that are displayed on the console		
Symptom:	Keep getting "pp_find_arp_entry failed to create ARP" entry on the console while connectivity to the Internet is lost.		
Probability:	High		
Feature:	FCX Layer 3 Forwarding - IPV4	**Function:**	ARP
Reported In Release:	FI 07.2.02	**Service Request ID:**	671567

Open defects in Release 07.3.00

This section lists defects with High or Medium Technical Severity as of December 9, 2011. The presence of a defect in this list can be prompted by several different circumstances. For example, some defects may have been initially reported against an earlier release in the field. Brocade's standard process in such cases is to open defects against the current release that *might* experience the same issues, and close them only when a fix is implemented, or if it is determined that the problem does not exist with the current release.
In other cases, a fix has been developed but has not been implemented in this release because it requires particularly extensive code changes or regression testing to ensure that the fix does not create new problems. Such fixes will appear in future releases.
None of these defects have the requisite combination of probability and severity to cause significant concern to Brocade customers.
Note that when a workaround to an issue is available, it is provided; otherwise, no recommended workaround is available at this time.

Defect ID: DEFECT000379038	**Technical Severity:** Critical
Summary: High CPU condition when there are none POE devices connect to POE enabled ports	
Symptom: High CPU condition when there are none POE devices connect to POE enabled ports	
Workaround: disable legacy POE detection, by configure the following at the global configuration no legacy -inline-power <slot#>	
Probability: High	
Feature: Power over Ethernet	**Function:** Power over Ethernet
Reported In Release: FI 07.3.00	**Service Request ID:** 680137

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: 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.	
Feature: FCX L2 Forwarding	**Function**: UNDETERMINED
Probability: Medium	
Found in Release: FI 07.2.02	**Service Request ID**:

Defect ID: DEFECT000365688	**Technical Severity:** High
Summary: On ICX, if copper GBIC is used in the 10G port, sometimes the link may not come up after reboot	
Symptom: If copper GBIC is used in the 10G port, sometimes the link may not come up after reboot	
Probability: Medium	
Feature: ICX Layer1 features	**Function:** Optics
Reported In Release: FI 07.3.00	

Defect ID: DEFECT000337878	**Technical Severity:** Medium
Summary: Unable to create a VLAN using vlan-group using SSH if aaa accounting is configured.	
Symptom: When creating a vlan-group only the first VLAN was created.	
Feature: TI L2 Protocol	**Function:** VLAN GROUP
Service Request ID: 267889	
Reported In Release: FI TI 04.2.00	**Probability:** Medium